Cryptologia, 36:295–340, 2012

ISSN: 0161-1194 print
DOI: 10.1080/01611194.2012.713803

Taylor & Francis
Taylor & Francis Group

Report on Speech Secrecy System DELILAH, a Technical Description Compiled by A. M. Turing and Lieutenant D. Bayley REME, 1945–1946

ALAN M. TURING AND D. BAYLEY

PART I: THEORY

1. The One-Time Pad Subtractor Cipher

When using a subtractor cipher, the plain language is first converted into a series of figures or "book groups." Each word or phrase is looked up in a kind of dictionary or "book," and against it is found a series of four (say) figures—the "book group" corresponding to that word. The words are replaced by the book groups:

Plain language.	YOUR	MESSAGE	UNINTELLIGIBLE	·	REPEAT	(1.1)
Book groups	1409	3511	6707	1333	8654	(1.2)

The book groups themselves might be used as a form of cipher, but this is rather insecure, so that some further process or "recipher" is usually applied. From the point of view of this reciphering, it is natural to regard the book groups as virtually plain language. Moreover, the division into groups is now of little real interest; it is useful to relieve the eye, but that is all. Let us run the groups together and call the result "P/L figures":

P/L figures	14093511670713338654	(1.3)

The one-time pad (O.T.P.) is one such system of recipherment.

If this is being used, then the encipherer and decipherer of the message have identical "pads," on each sheet of which is a random series of figures (actually broken into groups, but we ignore this). Each sheet is used once only and in the following manner.

Each message bears a reference to the page of the pad used. The originator writes the P/L figures under the figures of the pad and "subtracts":

Government Code and Cypher School: Cryptographic Studies, HW 25/36. This report was released to the British National Archives in 2009 but has never before been published. It was retyped by Craig Bauer to appear here.

The accompanying figures were too large to be reasonably included with the report here.

A short list of abbreviations, provided by John Harper, has been added just prior to the appendices.

Key (on pad)	37176019330372129001	(1.4)
P/L figures	14093511670713338654	(1.5)
Cipher	23183508760669891457	(1.6)

The "subtraction" used has not been the ordinary subtraction of mathematics, but something a little different, called "non-carrying" subtraction. One can think of this as meaning that one applies ordinary subtraction but forgets when one has "borrowed," or better, one can think of the calculation of each digit as being carried out independently, by an ordinary subtraction followed by the addition of 10 whenever a negative result is obtained:

3	7	1	7	6	0	1	9	3	3	...	(1.7)
1	4	0	9	3	5	1	1	6	7	...	(1.8)
2	3	1	-2	3	-5	0	8	-3	-4		(1.9)
0	0	0	10	0	10	0	0	10	10		(1.10)
2	3	1	8	3	5	0	8	7	6		(1.11)

In deciphering, exactly the same process is applied; the cipher is subtracted from the key, giving the P/L figures. That the process is the same is important from our point of view as it enables scrambling and descrambling to be done with the same apparatus.

The cipher obtained in this way has theoretically perfect security, that is to say that knowledge of the cipher text does not give the cryptographer any information about the P/L beyond what was previously available to him except that it does tell him the length of the message. This theoretical perfection is bound up with three facts about the O.T.P. cipher system:

a) given any cipher message and any P/L of the right length, there is one and only one series of key figures which will make the cipher yield the given P/L;
b) all series of figures are equally likely to appear on a pad; i.e., the pads are constructed by a truly random process;
c) each page of the pad is used only once.

The proof that the system has this unbreakable quality is contained in Appendix A. It is worthwhile to notice that condition a) would fail if our system depended on ordinary subtraction done figure by figure, instead of non-carrying subtraction; i.e., if instead of using (1.11) as a cipher, we used (1.9). Our condition a) does not then hold. To demonstrate that there is a weakness in this system, let us take the extreme case of the cipher 9999999999999999. Now 9 can only arise by subtracting 0 from 9, so that the P/L is completely determined as 00000000000000; this particular message can be completely broken. In the case of telegraphic messages one would not be tempted to use (1.9) rather than (1.11), but with the telephonic problem, one might, as it would be much easier to produce (1.9) than (1.11); the temptation must be resisted since the weakness involved is very great, much greater than might be supposed from the rather academic nature of the above example.

2. Application to Speech Scrambling

There is a fundamental difference between the nature of the information to be transmitted in telegraphy and that transmitted in telephony. The telegraphic information is specified by a finite sequence of symbols, each capable of only a finite number of values, e.g., of 2,000 modulation elements, each mark or space, or 400 characters each capable of 32 values. The telephonic message is specified by a voltage (say) which is given at every instant throughout a period of a minute (say) and is restricted to the frequency band 0–3,000 cycles (say); at any instant within the period the voltage may have any value within reason. If the subtractor principle is to be applied to telephonic material one might first consider simply adding a random voltage to the signal voltage. However, this does not work, as the speech energy is concentrated in comparatively few frequencies, and these frequencies will still have many times more energy in them than the other frequencies in the band after adding the random signal, so that a Fourier analysis should enable the speech to be recovered. Actually, it is much easier than this; the human ear works on a Fourier analysis basis, and if one listens to the combination of speech and random signal, one can easily pick out the speech. This experiment can be set up in very few minutes in any electrical laboratory. The weakness in this system is fundamentally the same as was described on page 2. One could try to avoid this particular difficulty by doing addition on the non-carrying principle, modifying it in the obvious way to allow for the fact that the voltages are not restricted to discrete values. This again fails, owing to the fact that the voltage corresponding to (1.10) is necessarily discontinuous, and that its discontinuities will be revealed in the cipher, enabling (1.9) to be recovered and the listening-through method applied. If the key had a very great bandwidth, it might not be possible to distinguish these latter discontinuities from the discontinuities of the key itself. However, in all practical cases, the bandwidth of the key is seriously limited. The cause of failure of this method may be detected by referring to the conditions under which the O.T.P. system is unbreakable; condition b) is not satisfied. The key is continuous and is therefore not random. Now although a continuous key defined at all times cannot be random, its values taken at discrete times can be. In fact it is shown in Appendix B that "random noise" restricted to a bandwidth 0 to B cycles has independent values at times equally spaced at intervals of $1/2B$. This suggests that we take a key with adequate bandwidth, select the values at appropriate discrete moments, combine these by non-carrying addition with the speech values at the same moments, and transmit the result. From this it is possible to recover the speech values at these chosen moments. If the time interval between the known speech values is less than a certain critical time interval determined by the bandwidth of the original speech it is possible to reconstitute this speech. The conditions for this and the proof of their validity are given in Appendix C. It is not really desirable to transmit the discrete cipher values as pulses, owing to the large bandwidth involved. A carefully designed smoothing filter enables a continuous function to be produced whose values at the discrete points are the appropriate cipher values at earlier points, without occupying much more bandwidth than that of the original speech.

3. "Delilah" Fundamental Block Diagram (Figure 1)

The system described at the end of the last section is essentially that adopted in "Delilah." In this section, we shall describe in broad outline the methods by which this result is attained.

The system requires the speech values to be limited to a certain voltage range, corresponding to the 10 possible values available for each figure in the O.T.P. cipher. This is accomplished in a simple limiter stage. The speech is also required to be confined to a certain definite frequency band. This has been chosen to be the band 0–2 kc/s, and the speech is therefore passed through an appropriate low-pass filter. On emerging from the filter, the speech is combined in a resistance network with the key. We may describe this combination of speech and key as $k(t) - s(t)$, where $k(t)$ is the key, and $s(t)$ is the speech ($t =$ time). The negative sign has been chosen to complete the analogy with the O.T.P.; there is no harm in doing so since a change in the polarity of speech is not distinguishable by the ear. The range of variation of $k(t)$ will be unity. By this, we do not mean that it is one volt, but rather that we are choosing our units for the measurement of voltage at this point of the circuit so that this is so. Actually, owing to the gains of the various stages we ought to define a new unit at each point of the circuit considered, but we shall omit to do this, leaving it to the reader to determine what unit is appropriate at each stage, if he so desires. The range of variation of $s(t)$ may be taken to be 0.7. It is permissible for it to be anything up to unity, but the trouble caused by its taking values outside the unit range makes the smaller range preferable. The mean values of $k(t)$ and $s(t)$ may be taken to be zero, both being fed through blocking condensers. The combination $k(t) - s(t)$ is now used to modulate a pulse, or in other words, the instantaneous values $k(n) - s(n)$ are picked out. We have adopted as the unit of time the interval between pulses. With a speech cut-off frequency of 2 kc/s the pulse frequency is 4 kc/s, so that the time unit is 250 μs. This process of pulse modulation is carried out by adding $k(t) - s(t)$ to a pulse, and applying the whole to a pentode which is normally biased beyond cut-off. No current flows through the valve except when the pulse is present, and the total charge which flows during a pulse depends on the value of $k(t) - s(t)$ at the time $t/(=n)$ of the pulse. We shall assume that the charge is a linear function of the signal (and, in fact, we take precautions to see that this is so), so that the charge or modulated pulse (MP) size may be written $h + k(n) - s(n)$, with h being the normal unmodulated pulse size. We have next to apply a process analogous to the addition of (1.10) to (1.9); this process is called Remainder Calculation.[1]

The Remainder Calculating process is carried out by a circuit controlled by the modulated pulses. This stage produces another pulse whenever the modulated pulses (M.P.) exceeds the critical size h. This "Remainder Calculator (R.C.) pulse" is then subtracted from the M.P., giving $h + k(n) - s(n) - 1$ if $k(n) - s(n) > 0$ but giving $h + k(n) - s(n)$ if $k(n) - s(n) < 0$. We may write the value of the resulting pulse as $h - \frac{1}{2} + R(k(n) - s(n))$, where $R(x) = x - \frac{1}{2}$ if $x > 0$, $R(x) = x + \frac{1}{2}$ if $x < 0$. This form of expression is convenient, since $R(k(n) - s(n))$ has the mean value 0. The process this far is illustrated in Figure 2.

[1]The significance of the term may be seen from what would have to be done if the key values in (1.7) were not restricted to the range of 0 to 9, e.g., if they were permitted to take the values 0 to 99. In this case, the figures in (1.9) could take values +99 to −9, and the figures (1.10) would then be multiples of 10 from −90 to +10, chosen in such a way that the figures in (1.11) all belong to the set 0,1,...,9. The process of obtaining (1.11) from (1.9) may then be described as "taking the remainder on division by 10." This calculation of remainder is not electronically convenient when the key is allowed to take such a wide range of values, owing to the variety of values required in (1.10), and we therefore arrange for the key to be restricted to a "unit" voltage range corresponding to the above range of 10. In order that condition b) may be satisfied, the key should take all values in the allowed range equally frequently.

The pulses $h - \frac{1}{2} + R(k(n) - s(n))$ are now fed into the filter. We will consider this filter chiefly in terms of indicial response rather than frequency response. Let the response of the filter at time t to a "unit pulse" at time o be $g(t)$. Then the response to the sequence of pulses $h - \frac{1}{2} + R(k(n) - s(n)) = p(n)$ is $\sum_{n=-\infty}^{\infty} p(n)g(t-n) = c(t)$. Of course $g(t)$ will be zero for negative t so that the terms for $n > t$ may be omitted. The filter is chosen so that $g(m_o) = 1$, $g(m) = 0$ for all integers other than m_o. Then $c(n) = p(n - m_o)$, all integers n. The signal $c(t)$ is sent out as the cipher version.

The function $g(t)$ should be considered in connection with the results in Appendix C. Items 2) and 3) of this appendix show that the function $c(t)$ will in general occupy a bandwidth of at least $\frac{1}{2}$ cycle (with our time unit, or with our practical values 2 kc/s). Item 4) also shows that if we are to realize this minimum bandwidth the function $g(t)$ must be of the form $g(t) = \frac{\sin \pi(t-m_o)}{c(t-m_o)}$. Such a $g(t)$ is, strictly speaking, impossible, with finite m_o, being inconsistent with the condition that it be zero for negative t. However, with moderate values of m_o it is possible to restrict the output very nearly to the theoretical minimum band. Actually the present unit uses $m_o = 1$. Three forms of $g(t)$ are shown in Figure 3. In Figure 3a we have approximated the form $\frac{\sin c(t-m_o)}{\pi(t-m_o)}$ very closely, with $m_o = 5$. In Figure 3b is shown a form of curve, which gives about as sharp a low-frequency cut-off as is possible with $m_o = 1$. Figure 3c shows essentially the form used in the present apparatus. The frequency characteristic is not especially good, but certain other features are more important. The fact that the curve is virtually zero from t just below 2 to infinity, and that its derivative is small at $t = 1$ tend to make the apparatus less sensitive to small changes of setting or component values.

If we put $R(k(n) - s(n)) = q(n)$ so that $p(n) = h - \frac{1}{2} + q(n)$, then $c(t) = \sum_{n=-\infty}^{\infty} q(n)g(t-n) + u(t)$. Here $u(t) = \left(h - \frac{1}{2}\right) \sum_{-\infty}^{\infty} g(t-n)$ represents a certain unwanted signal. It contains only D.C. and frequencies which are multiples of 1 cycle per time unit. In practice, we try to make the A.C. component of this signal small. The values $c(n)$ are those which are of importance in reception. We have $c(n) = q(n - m_o) + \beta$, where $\beta = \mu(0)$.

When the apparatus is switched to the receive condition the incoming cipher is subtracted from the key and the combination passed to the pulse modulator. The key in this case is delayed (in a manner described later) by m_o, and, by means of blocking and a difference in the receive and transmit biases, a constant signal $+ \beta$ is added so that the final signal reaching the pulse modulator grid is: $k(t - m_o) - c(t) + \beta$; i.e., at time n, $k(n - m_o) - q(n - m_o)$. The sizes of the modulated pulses are now given by $h + k(n - m_o) - q(n - m_o)$, and when the Remainder Calculator pulses are subtracted, we get $h - \frac{1}{2} + R(k(n - m_o) - q(n - m_o))$; that is to say $h - \frac{1}{2} + R(k(n - m_o) - R(k(n - m_o) - s(n - m_o)))$, and this is equal to $h - \frac{1}{2} + s(n - m_o)$, as follows from the fact that due to limiting $|s(n - m_o)| < \frac{1}{2}$ and from the equation $R(a - R(a - b)) - b$, which is valid if $|b| < \frac{1}{2}$.

The result 4) of Appendix C, shows that we can recover the speech from these pulses by putting them through a filter whose indicial response is $\frac{\sin \pi t}{\pi t}$, i.e., by putting them through an ideal low-pass filter with cut-off frequency $\frac{1}{2}$. By an ideal low-pass filter we mean one which causes no change of amplitude or phase within the pass band, but clearly we do not need to specify so much since the ear is not sensitive to phase distortion. It is sufficient to pass the pulses through a low pass filter with a fairly sharp cut-off at $\frac{1}{2}$ (i.e., at 2 kc/s). The filter used in the transmit condition has not a sufficiently sharp cut-off, but a simple switching arrangement enables it to be converted into a more suitable one and to deliver the output at an appropriate level to a pair of phones.

It is important to note the limitation $|s(n)| < \frac{1}{2}$. If it is not satisfied, we are liable to find that the output pulses are of size either $h - (3/2) + s(n - m_o)$ or $h + \frac{1}{2} + s(n - m_o)$ instead of $h - \frac{1}{2} + s(n - m_o)$. Each time that we get a pulse which is wrong in this way, there is added to the speech a pulse of form $\frac{\sin ct}{\pi t}$ (in the ideal form of theory), producing a sudden crack, like a rifle shot.

The above theory may perhaps be made clearer by giving a numerical example. For this purpose, we will only specify the instantaneous values $k(n)$, $s(n)$ instead of the complete functions $k(t)$, $s(t)$, owing to the difficulty of specifying the latter and the fact that we really only need the former. In the following table an example is given showing the various stages passed through by four pulses of speech. Three of the speech values are correctly reconstituted, but one is not, because it had not been properly limited originally.

$k(n)$	0.350	−0.142	−0.014	0.4111	
$s(n)$	0.204	−0.278	0.238	0.602	
$k(n) - s(n)$	0.146	0.136	−0.252	−0.191	
Modulated pulses ($h = 2$)	2.146	2.136	−1.748	1.809	
R.C. pulses	1	1	0	0	
M.P. with R.C. combination	1.146	1.136	1.748	1.809	
$(= h - \frac{1}{2} + R(k(n) - s(n)))$					
$h - \frac{1}{2}$	1.5	1.5	1.5	1.5	
$q(n)$	−0.354	−0.364	0.248	0.309	
$q(n - m_o) = c(n) -$ $(m_o = 1)$		−0.354	−0.364	0.248	0.309
$k(n - m_o)$		0.350	−0.142	−0.014	0.411
$k(n - m_o) - c(n) +$		0.704	0.222	−0.262	0.102
Receive M.P.		2.704	2.222	1.738	2.102
Receive R.C pulse		1	1	0	1
Receive M.P. and R.C. combination		1.704	1.222	1.738	1.102
		1.5	1.5	1.5	1.5
Reconstituted speech values $s(n - m_o)$		0.204	−0.278	0.238	−0.398
					$(= -1 + 0.602)$

PART II: GENERAL DESCRIPTION AND CIRCUIT DETAILS

4. General Description

The equipment has been built in three units, these are

(a) the COMBINING UNIT in which the scrambling and descrambling process described in § are carried out
(b) the KEY UNIT, which provides the voltage $k(t)$ required by the combining unit; and
(c) the POWER PACK, which supplies H.T. and heater current to both of the above units.

A table of the sizes, weights, and power consumptions of these units will be found below, and photographs are included at the end of the report.

The combining unit operates as either scrambler or descrambler, and the function is changed by relays in the unit operated by the microphone pressel or a key on the key unit. Apart from this switch (and a button labelled "Synch Test," which is no longer used), there are only four controls on the unit, and these have to be operated only when the apparatus is descrambling. A switch on the combining unit panel serves to cut out the scrambling facility, enabling the apparatus to receive or transmit clear speech; pilot lamps indicate which of the facilities is being used. In addition to the fundamental circuits, the combiner contains circuits for synchronising the key unit for "switching on" its output at appropriate times.

The key unit contains electronic circuits for producing the voltage $k(t)$ together with an adapted cypher machine and a plug board, both of which are used to alter the character of $k(t)$. The plug board is altered daily, while the cypher machine is reset at the end of every conversation. The only control on the key unit (apart from the H.T. switch) is a key which rotates the cypher machine when the ends of the transmission path interchange their functions. This key is coupled to the key mentioned in the above paragraph so that the relays are automatically energized immediately after the code is changed.

Full details of the circuits of these units are given in the later sections of this Part.

The apparatus has two major disadvantages. Firstly, it is essential for the receiver and transmitter to be accurately synchronised and to remain so. Thus, the system has all the snags of any synchronous system, plus the important one that once the receiver has slipped out of synchronism (through fading of the synch, signal, or mishandling the controls), the receive key wave differs from the transmit one and contact with the transmitter is lost and can only be regained by a rather tedious procedure. Secondly, it is essential that the cypher arriving at the receiver shall be identical in waveshape to the cypher leaving the transmitter. This implies that the transmission shall have a level amplitude characteristic from 0 to 4 kc/s and a linear phase characteristic over the same range. This means that transmission may not be by ordinary P.O. lines or by any radio path involving the use of sky wave. These requirements, of course, place a serious limitation on the usefulness of the apparatus. However, it is thought that operation should be quite easy over short range on U.H.F., and it is proposed to carry out tests using an F.M. transmitter working on 30 Mc/s. The present experimental system is worked four wires, but it should be quite possible to work two wire with suitable external circuits:

Unit	Weight	Size	Power requirement
Combiner	19 lb.	$14'' \times 10'' \times 8''$	(4.5 A. @ 6.3 v.) (65 m.a. @ 350 v.) (5 m.a. @ -450 v.)
Key	44 lb.	$14'' \times 18'' \times 8\frac{1}{2}''$	(4.0 A. @ 6.3 v.) (35 m.a. @ 350 v.) (2 m.a. @ -450 v.)
Power	23 lb.	$7\frac{1}{4}'' \times 8'' \times 7\frac{1}{2}''$	(1.0 A. @ 230 v. 50 $\sim$)

5. Complete Block Schematic (Figure 4)

In this section, we shall describe in outline the operation of those parts of the circuit which were not considered sufficiently fundamental to warrant description in

section 3, but that are nevertheless necessary for the working of the apparatus. These may be grouped under the following headings:

a) Pulse Generator and Synchronisation,
b) Biasing of pulse Modulator, and
c) Key Switching and Delaying.

(a) Pulse Generator and Synchronisation

An essential feature of the system was that there should be a 4 kc/s pulse in both the receiver and transmitter and that these should be accurately synchronised. The pulse is provided in both by the Pulse Generator stage together with the Pulse Squarer stage. The pulse generator is a 4 kc/s multivibrator and the pulse squarer is simply an overloaded amplifier to which is applied the differentiated O/P of the multivibrator. The multivibrator is locked, both on receive and transmit, by a 4 kc/s sine wave. In the transmit condition the sine wave is provided by the Synch Oscillator and the same sine wave is added to the cipher at an appropriate level. In the receive condition the synch oscillator becomes the Receive Cathode Follower, and the tuned circuit in it picks out the added 4 kc/s component from the in coming cipher and uses it to lock the multivibrator. It may be added that in order that this system should be satisfactory the cipher proper should be very free from frequencies in the neighbourhood of 4 kc/s. This is a consideration in the design of the Filter.

Although both receive and transmit pulse generators may be locked with the sine wave there may well be a difference of phase between them. This phase difference will depend, amongst other things, on the natural frequencies of the multivibrators. It can be made zero by suitable adjusting the frequency of the receive multivibrator. A control labeled "Synch" is provided for this purpose; and the "Synch. Test" circuit described below enables the receive operator to monitor this adjustment.

On pressing the "Synch. Test" button on transmit the output of the filter is fed back as modulation on the pulse, producing a 2 kc/s oscillation bearing a definite phase relation to the modulated pulse, which is transmitted to the receiver. If the button is also pressed on the receiving unit, this incoming oscillation undergoes a certain phase change and appears as modulation at the pulse modulator stage. The phase change is such that the zeros of the 2 kc/s sine wave in the receiver occur at the same times as the pulses in the transmitter (ignoring any delay in transmission). Therefore, if the receive pulses are in synchronism, the effective modulation is zero. In operation, then, the receive operator adjusts the "Synch" control until he hears no 2 kc/s signal in his phones.

(b) Biasing of Pulse Modulator

It is necessary, both for security and intelligibility, that the normal unmodulated size of the modulated pulses should be equal to the critical size of M.P. *h*, such that pulses exceeding *h* give rise to remainder calculator pulses, but smaller M.P. do not. The size of the normal M.P. is determined by the size of pulse fed to the pulse modulator stage from the pulse squarer, and on the bias on the P.M. stage. The bias is very critical, and also fairly large. In fact the normal value of bias is about 17 volts and the admissible variation in this voltage from the correct value may be taken to be 0.02 volt in the transmit condition and 0.05 in the receive condition. The symptoms of an incorrect bias are fairly obvious in the receive condition, so that it is feasible to provide a bias variable over a range of two or three volts and to allow the operator to choose the best

setting at any moment. In the transmit condition this is not possible. The correct setting is more critical, and also the operator cannot tell when it is obtained. An automatic form of biasing is therefore used, whereby the amount of bias is made to depend on the percentage of R.C. pulses and to give 17 volts of bias when there are 50% of R.C. pulses. This results in the bias stabilizing itself at the correct value.

One is naturally tempted to ask why the form of biasing should not then be used for the receive case also, relieving the operator of a slightly awkward control. The effect of this would be that the percentage of R.C. pulses in the receiver would be determined by its own bias circuit components rather than by the percentage occurring in the transmitter. Thus, if the transmitter produced an accurate 50% of R.C. pulses, but the receiver 48%, there would be a discrepancy of 2% representing 80 pulses per second, each producing a little crack in the phones.

(c) Key Switching and Delaying (Figure 5)

The key, which is produced at each end of the transmission path, is not truly random since it has a period of about 8 mins. However, by means of a standard cipher machine a very large number of different keys are available and a new one is selected semi-automatically on each change from transmit to receive and vice versa. Since the transmit and receive keys must be identical (except for a time difference of one unit; — page 7) it follows that the key must be cut off on switching from transmit to receive and only re-started at a moment decided by the transmitter. This is the function of the key switching and delaying circuit.

When a unit is on receive, the transmit bias is automatically increased by a considerable amount. On switching over to transmit, this bias begins to approach its normal value through a time constant of 300 ms. Hence the pulses being fed into the remainder calculator slowly increase in size until, after about half a second, the remainder calculator is tripped and produces a pulse. This pulse is fed to the filter, in the usual way, giving a broad negative pulse at the output. It is also fed to the Key Switch, a thyratron normally biased below cut-off, causing it to fire, and thus changing, instantaneously, the cathode voltage from a negative one to a positive one.

In the receive unit the tripping pulses is inverted in the Phase Inverter and passed on, together with pulses from the pulse squarer, to the key switch. The combination—pulse plus tripping pulse—is just sufficient to trip the thyratron. Since the maximum of the tripping pulse occurs one time unit after the remainder calculator pulse which produced it, it follows that the receive key switch will trip one time unit later than the transmit one.

The cathode voltage of the key switch is passed through the Key Bias Stabilizer (a positively biased diode) which stabilizes the bias when it is positive and on to a cathode follower (Key Bias Cathode Follower) to reduce the output impedance. The Key Switch Indicator (LPI) associated with this latter circuit is simply a neon which fires whenever the bias is positive and thus indicates that the key unit bias has been raised.

Switching from receive to transmit and back is done by means of a relay energized from the HT supply. During operation of this relay large transients are produced at the filter. To prevent these having any effect at the distant unit an Output Suppressor circuit is provided. This stage consists of a cathode follower which is cut off on receive and slowly begins to function about 100 ms. after switching to transmit. It is important that this circuit should be in operation before the tripping remainder calculator pulse occurs in order that the receiver shall then be in synchronism.

The key unit must be synchronised with the combining unit, and negative locking pulses at a low impedance are provided for this purpose by the Pulse Cathode-Follower.

6. Stage-By-Stage Circuit Details

(a) Synchronised Oscillator and Receive Cathode Follower (Figure 6)

This circuit is primarily intended to lower the output impedance of the cipher coming in on receive. The tuned circuit, consisting of C5 and L1 across the cathode load, provides voltage amplification for the Synch, which drives the multivibrator. In the transmit condition the output undergoes a slight phase change (delay of about 60°) in R7 and C3 and is then fed back to the grid, where it appears in an appropriate phase to maintain the oscillations. Whilst on transmit, the cipher input has the leak R1, which prevents any sudden change of bias on switching.

The amplitude of the oscillations is limited chiefly by the H.T. If full H.T. is applied very large voltages (e.g., 500 volts peak to peak) will be found at the junction of C5 and L1. The high resistance dropper R6 (50 K) limits the amplitude to about 100 volts peak to peak at this junction and about 30 volts p-p at the cathode. A certain amount of distortion naturally arises due to the valve cutting off. This distortion appears in the form of the top of the sine wave being turned over, as shown in Figure 24c. This may be explained by the series-tuned circuit still trying to maintain its normal current, and so causing a reverse current in the cathode load. The extent of this may be controlled by the resistor R7. Too high a resistance entails no oscillation; too low a resistance gives too much distortion.

(b) Pulse Generator, Pulse Squarer, and Pulse Cathode Follower (Figure 7)

The pulse generator is a multivibrator with one short and one long leg, the short time constant being given by a grid leak of 15 K and grid condenser of 75 pf and the long time constant being given by a leak of 2 M and condenser of 330 pF (product 600 μS) (multiplying up to 1.125 μs). The output is taken from the anode appropriate for giving negative pulses, and this also gives a comparatively low output impedance. The locking sine wave is fed to the long time constant grid through 40 pf and a resistance. If the resistance is omitted the locking is more effective, but the condenser has a more deadening effect on the pulse shape. In the transmit condition the sine wave is attenuated and changed in phase by C7 and R8, the values of which were fixed experimentally to obtain optimum synchronisation, before being fed to the grid, and the grid leak is made a fixed one in place of the variable used for the controlling phase in the receive condition.

In spite of the short-leg time constant being only 1.125 μs (or perhaps about 2 μs if we allow for the anode load) the width of the pulse was about 25 μs. Moreover its amplitude was inadequate, its shape insufficiently square, and its polarity wrong. It is therefore "differentiated" with C13 and R18 and the resulting narrow pulse amplified and squared off in the pulse squarer.

A previous design has no pulse squarer and took the pulse from the common cathode of the two triodes of the multivibrator.

The pulse cathode follower provides locking pulses at a very low impedance for the use of the key unit. The polarity is reversed by means of a small Rhometal core

transformer T1. This transformer also has a step down, the turns ratio being rather less than 2.1.

Approximate amplitudes of pulses are

From pulse generator, 150 volts
From pulse generator, differentiated, 30 volts
From pulse squarer, 130 volts
At key lock, 45 volts.

(c) Key Switch, Key Bias Stabilizer, and Key Bias Cathode Follower (Figure 8)

The key switch valve is a gas tetrode which is tripped by pulses on the grid and extinguished by connecting the anode to a negative potential. R91 and R92 form a potentiometer from the −450 volt line to earth such that their junction is normally at about −230 volts. To this point is connected the cathode of the gas tetrode and (via R90) the grid of the key bias cathode follower. Hence the cathode of this valve is at the same potential as the cathode of the gas tetrode but with a much lower output impedance. A suitable bias for the gas tetrode is produced by returning its grid through grid leak R87 to the slider of R76 in the cathode of the cathode follower. The anode resistor R89, the switch contact B1, the condensers C52 and C53 and resistors R93 and R94 provide the extinguishing arrangements.

On receive, pulses are applied to the grid of the gas tetrode via R84. The bias is adjusted, however, so that these pulses are insufficient to trip the valve. When a wide tripping pulse (produced by the first remainder calculator pulse in the transmitter) is added to these pulses by the phase inverter, the thyratron is tripped by the pulse which occurs near the maximum of the tripping pulse. Figure 5 illustrates the waveforms involved, and it is obvious that the key switch is tripped one time unit (250 μsecs) after the first remainder calculator pulse has been produced in the transmitter. When the gas tetrode fires, the potential of the cathode rises to about +250 volts. The grid of the bias cathode follower also rises but is stabilized at +50 volts by the key bias stabilizer, a diode which has its cathode voltage maintained at about +50 volts by the potentiometer R100. In the fired condition, the cathode of the cathode follower has a potential of about +50 volts and is adjusted to the accurate value of 50 volts required for the Key Unit by the potentiometer R100.

While on receive, C53 has been charged up to −450 volts through resistor R94. Now, on going over to transmit, the anode is connected to this negative voltage. C53 begins to discharge through the anode load R89 (time constant 20 ms), so that the anode begins to rise to its final value of about 320 volts. However, the anode does remain quite negative for several millisecs, and, since the grid is still negative, the gas tetrode is extinguished. After 40 or 50 ms, the anode is again sufficiently positive for the valve to fire if the grid is tripped. The extinguishing action on switching from transmit to receive is identical with the above.

On transmit, remainder calculator pulses only are applied to the thyratron grid and they are of sufficient amplitude to trip the valve. Hence, it follows that the first remainder calculator pulse to be produced after switching will trigger the key switch. A long time const. in the pulse modulator biasing circuit (c.v.) ensures that the first pulse does not occur until 300 ms or so after the switching has taken place. This same pulse is fed to the output filter and appears in the output smoothed, delayed by one time unit, and inverted. This pulse, reverted and amplified in the phase inverter, is the tripping pulse which is fed to the grid of the gas tetrode in the receiver as explained above. The

300 ms delay is necessary to ensure that the receive unit is correctly synchronised before the tripping pulse arrives.

Visual indication that the key switch has fired is afforded by the key switch indicator. This is a Tuneon (LPI), one pole of which is tied to a potential of about −230 volts (mid-point of R74 and R75); the other pole is joined to the cathode of the cathode follower. It is obvious, then, that when the key switch fires and this cathode goes to a potential of 60 volts positive, the neon will glow.

The rather unusual biasing arrangements on the key switch circuit were found necessary to make the circuit stable. When current flows in the Thyratron, the amounts that flow in R91 and R92 are unequal, so these resistors are unequally heated, producing a change in their values. On extinguishing the valve, then, the cathode potential will have a different value from the one it originally had. If the grid bias is obtained from a pot, between −450 volts and earth, it will remain fixed, so that the grid-cathode potential will depend on past history. Since this voltage is critical to about one volt, the circuit would be unreliable. This is overcome in the present circuit by deriving the grid bias potential from the cathode potential of the Thyratron.

It will be observed that the heater cathode potential of the gas tetrode is rather high. It was found, in practice, that a valve having a completely shielded mode (e.g., R.C.A. 2050) functioned quite satisfactorily under these conditions. Another type which had an incompletely shielded anode was found to flash-over outside the shield and, in consequence, the extinguishing circuit did not function reliably.

(d) Limiter and Speech Filter

The limiter consists of two Westinghouse Selenium rectifiers type H3 connected "head to tail." Over the operating range of these rectifiers, their characteristics may be approximately expressed by the formula:

$$I = \text{O.11}\ E.^{3.6}$$

where I is in amps and E is in volts.

This formula applies for a single rectifier when the voltage is applied in the sense appropriate to make it conduct. It may also be used for a pair of "head-and-tail" rectifiers if E and I are interpreted as the absolute magnitudes of the voltage and current, respectively. Clearly the range of variation of E is much smaller than that of I; thus a two-to-one change in I causes only a 22% change in E. Consequently, so long as the polarity of I remains unchanged the magnitude of E varies only slightly, although a change of polarity of I involves a change of polarity of E. Then if the input signal is proportional to I and the output signal to E we get the limiting effect we require (see page 8). If the current is to be proportional to the speech signal, the impedance presented by the microphone circuit to the rectifiers should be high.

The speech filter is a simple low-pass filter cutting off fairly sharply at 2 kc/s and serves to restrict the speech to the band of frequencies 0 to 2 kc/s as discussed on page 3. The filter has to follow the limiter in order to remove any harmonics above 2 kc/s introduced by the rectifiers. This will, to some extent, worsen the limiting, but the effect is not thought to be serious.

The speech was originally provided by a carbon microphone with an energizing battery and transformer in an external box. However, this arrangement was very

unsatisfactory, and at present a crystal microphone and external compressing amplifier are used. Even this arrangement leaves much to be desired, and it is felt that further work is needed on this part of the problem.

(e) Output Suppressor (Figure 9)

This stage, which acts as a cathode follower on transmit, is cut off on receive and prevents clear speech from being fed back into the line. In receive condition, H.T. is taken off the valve at switch contact B2, and the anode is connected to −450 volts via R119; this very effectively prevents the valve from conducting. During switching from receive to transmit, large transients appear in the main circuit, and it is the primary function of the Output Suppressor to prevent these getting to the line and operating the receive key switch. On going to transmit, the anode voltage begins to rise with a time const. determined by R111 and C59 (about 20 ms). Thus the anode remains negative for several ms., and the valve does not begin to operate as a cathode follower until all the transients are over. C65 in the grid circuit by-passes these transients to earth and prevents their being developed directly across the cathode load. The time during which this stage is cut off after switching is critical in that it must be long enough to prevent any transients from being transmitted but must be short enough to allow the synch to pass for about 100 ms. before the first remainder calculator pulse is produced (see page 16).

This circuit was introduced largely for bench tests over a short four-wire line. When the equipment is used with a radio link it is essential for the transmitter output to build up fairly slowly on switching from receive to transmit to avoid the possibility of transients in the receiver tripping the key switch. Since a time constant would have to be provided in the transmitter for this purpose it would render the output suppressor in the combiner redundant.

(f) Phase Inverter (Figure 10)

This stage performs two important functions: it ensures that the key and cypher are combined in the correct polarity on receive, and, since it may have high impedances in the grid circuit, it makes it possible to render the "Key Vol." and "Cypher Vol." controls independent.

On transmit, the speech from the speech filter is combined with the key in the pot. R22 and R26. The voltage at the junction is developed across R104 and applied to the grid of the phase inverter. The output of this stage is used for two purposes. For one purpose (key switch) the full output is required; this is fully discussed below. For the other purpose the gain of the stage is not required and this gain (about 9) is nullified by the attenuator R31 and R30, so that the final voltage across R30 is a little less than the input voltage and is inverted. The output is taken without a D.C. blocker to avoid distortion. The voltage across R30 is fed to the pulse modulator grid as described elsewhere.

Tracing through the main circuit (block diagram Figure 4) we see that from speech input to final output there are three inversions of phase. These occur in the phase inverter, the pulse modulator, and the output filter. Hence to Subtract the key at the receive and we need to combine with the key of the same polarity as that in the transmitter. This is done in the grid circuit of the phase inverter on receive.

The key is taken from the slider of R27 (key Vol.) and combined with the cypher from the input cathode follower in the potentiometer R25 and R101. These impedances are made high so that altering Key Vol. will have no effect on the cypher volume; i.e., this control and Cypher Vol. are made independent. The combined voltage is fed through C 57 to R102 cypher vol, the slider of which is connected to the grid of the phase inverter. The voltage appearing at the grid of this stage is thus of the form $a(-C+bK)$, where C and K are the cypher and key, and a and b depend on the setting of the Cypher Vol. control and Key Vol., respectively. As will be evident in the section on operation a control of this form is very convenient. The output of the phase inverter is fed to the grid of the pulse modulator via the same components as on transmit.

Bias in both conditions of operation is obtained from potentiometer R107 and R106 from −450 volts to earth.

The tripping pulse for the Thyratron is taken from the anode of the phase inverter through C50 and R83. The time const. of these components together with that of C51 and R87 in the Thyratron grid circuit are chosen so that these four components shall form a high-pass filter to the slow voltage rise which occurs as the anode of the output suppressor in the transmitter goes positive from having any effect at the key switch grid. Since the tripping pulse is taken from the anode direct, it is amplified with respect to the input of the unit and, in consequence, allows a larger tolerance on the Thyratron grid bias.

(g) Pulse Modulator (Figure 11)

The purpose of the circuit is to give an output consisting of pulses of a size varying with the modulating signal. It is desired that over the working range the area of the pulse (as seen on a C.R.O.) should be a linear function of the modulating voltage. This effect is obtained by working a 6AC7 (pentode) class C. The voltage applied to the grid is pulse combined with modulating signal in what is essentially a potentiometer arrangement, viz., R30, R31, R28, and C18 (C18 will be discussed later). The appropriate bias is applied through R32 or R33, according to the position of the transmit–receive switch. The purpose of R34 is described under (c) and (j). The screen of the 6AC7 is taken direct to the decoupled H.T. This tends to improve the linearity of the pulse area against the modulating voltage curve, due to screen current reducing anode current. The anode load is split to provide attenuated output to drive the remainder calculator. The condenser C18 enables the pulse shape at the output of this stage to be improved by a compensating predistortion.

(h) Remainder Calculator (Figure 12)

The remainder calculator is required to produce positive output pulses when the pulses from the pulse modulator exceed a certain critical value, actually about 120 volts. The size and timing of the remainder calculator pulse should not depend on the size of the tripping pulse nor on past history. The width of an remainder calculator pulse should not exceed 30 μs say, but its shape is not very critical. Any small constant error in the time of the remainder calculator pulse can be corrected by means of the condenser C29.

The circuit is essentially a form of Kipp relay. It is, in fact, a multivibrator biased so as to have a stable state. This biasing is done by returning one grid leak (R47) to a voltage negative with respect to cathode. Either of these precautions by itself would

probably suffice for this purpose, but the actual arrangement shown is convenient in view of the fact that we do not want small pulses to disturb the stable state. The tripping pulses are fed through C24 into the first grid, which is normally passing grid current. These pulses are amplified in spite of the grid current and appear on the second grid. Only when they are sufficiently large to raise this grid above cut-off is there any cumulative effect raising the first grid by way of C24. When this occurs the system becomes unstable and the second tube becomes conducting instead of the first. However, the new condition does not persist for very long. The first grid soon returns above cut-off and the stable state is resumed.

The feed from pulse modulator to remainder calculator may be either through a resistance or a capacity. The latter has been chosen as it gives a more stable timing of the R.C. pulse.

(i) Output Filter (Figure 13)

It is rather difficult to give a really satisfactory account of the output filter circuit. The circuit actually used was arrived at by calculations of a trial-and-error nature. Most of the considerations involved were of too vague and confused a nature to be worth recording here, but the more definite of them will be mentioned shortly, and the ideal aimed at will also be described.

As was mentioned on page 7, the ideal form of indicial response approximates $\frac{\sin \pi t}{\pi t}$ as in Figure 3a. The earlier experiments were done with a form similar to 3b, but it was found very difficult to make the curve vanish at all the points required, and therefore it was decided to use an indicial response of the form in 3c, which would be less touchy. The main points of this form are

(i) $g(t)$ virtually 0 from $t = 3$ onwards,
(ii) $g(2) = 0$ and $g'(2)$ small,
(iii) $g'(1)$ small,
(iv) several derivatives 0 at $t = 0$.

The reason for requiring (i) and (ii) is the stability mentioned above. The reason for (iii) is largely that it makes variations in timing of remainder calculator pulses of less importance. (iv) effectively means that high frequencies will be absent, and is a good thing both from the point of view of bandwidth and of security (the latter because it prevents the detection of R.C. pulse by studying transients). Besides these requirements for the indicial response the output filter is required to have the following frequency properties if possible:

(v) Very low response at 4 kc/s
(vi) Low response at high frequencies (of (iv))
(vii) Fairly level response up to 2 kc/s.

(v) is required in order that there should be no output at frequencies near to 4 kc/s, which might upset the synchronisation.
(vi) is of secondary importance: it is useful if the output is to be fed straight to the phones on receive.

The response on any linear network with lumped constants to an input signal e^{pt} is of the form $G(p)\, e^{pt}$, where $G(p)$ is a rational function (ratio of two polynomials). The method used for designing the output filter was to split the problem into two

parts. First, an appropriate function $G(p)$ was chosen, and then an attempt was made to design a network to realize it. The function eventually chosen was

$$G(p) = \frac{p^2 + 4\pi^2}{(p+\pi)(p+2\pi)(p+(0.8+i)\pi)(p+(0.8-i)\pi)\ (p+(0.8+1.6i)\pi)\ (p+(0.8-1.6i)\pi)}$$

The corresponding indicial response $\int_{-i\infty}^{i\infty} G(p)e^{pt}dp$, and the frequency response are shown in Figure 14.

In order to realize the frequency response $G(p)$ above, we have somehow to bring in the factor $p^2 + 4\pi^2$ of the numerator, which effectively eliminates all 4 kc/s. This is done by means of the feedback circuit L4, C35, L3, C32, C34, R52. The reason for doing it in this way is that it is desirable to remove the 4 kc/s before the signal reaches the grid of V1B in order to reduce grid swing. However, impedance in the grid circuit are too high to allow more conventional methods, such as a shunt series-tuned circuit. The higher harmonics of the pulse have already been largely removed by the condensors C33 and C36. It was intended that the factors $p + 0.8\pi \pm 1.6i\pi$ of the denominator should be brought in by the feedback circuit also and the factors $p + \pi$ and $p + 2\ \pi$ by the grid circuit. The remaining factors $p + 0.8 \pm i\pi$ were to be brought in by the tuned circuit L5, C40. This way of looking at the circuit is only an approximation, but is certainly helpful.

The response of the actual circuit was calculated on the following assumptions.

(i) All components to the input side of C33 to be replaced by a series resistor of 170 K. The equivalent voltage applied to the input side of this resistor to be a combination of attenuated modulated pulse and R.C. pulse. This assumption consists mainly in ignoring C29.
(ii) The anode impedance of the valve (6J5) is 7 K, and its amplification factor 20. The grid-anode capacity is assumed to be 4pf; it is taken into account from the point of view that the anode volts influence the grid volts, but the influence of grid volts on anode volts is ignored.
(iii) The components R52, C34 are ignored from the point of view of their influence on the voltage at the junction of L3, C32.

The result of this calculation is to give the response as

$$4.5\alpha^4 \frac{1.06\alpha^3 + 0.198\alpha^2 p + 0.1675\alpha p^2 + .0255p^3}{19.61\alpha^7 + 48.0\alpha^6 p + 53.16\alpha^5 p^2 + 34.47\alpha^4 p^3 + 13.80\alpha^3 p^4, +3.51\alpha^2 p^5 + 0.478\alpha p^6 + .0319p^7}$$

where $\alpha = 10{,}000\ \text{sec}^{-1}$.

The zeros of the numerator are approximately -6.4α, $(-0.9 \pm 2.56i)\alpha$, and those of the denominator are

$(-4.48 \pm 3.96i)\alpha$
$(-1.03 \pm 1.30i)\alpha$
$(-1.39 \pm 1.90i)\alpha$
-1.25α

Our standard unit of time being 250 μs, we have $\alpha = 0.85$, and therefore these roots become

Numerator	
$-5.12\pi,\ (-0.072 \pm 2.05i)\pi$	$\pm 2i\pi$
Denominator	
$(-3.6 \pm 3.18i)\pi$	-2π
$(-0.83 \pm 1.04i)\pi$	$(-0.8 \pm i)\pi$
$(-1.12 \pm 1.52i)\pi$	$(-0.8 \pm 1.61i)\pi$
$-\pi$	$-\pi$

In the right-hand column have been shown the figures which were aimed at. It should be realized that it was extremely difficult to do any calculations at all, and it was certainly not worthwhile to try and get more accurate roots before trying the circuit out. It will also be noticed that the actual circuit response has one more factor in numerator and denominator than the one aimed at. In effect, we may consider the factor $\frac{p+5.12\pi}{p^2+7.25p+20.1\pi^2}$ in the actual circuit as replacing $\frac{1}{p+2\pi}$ in the desired response. In effect, this means the unwanted factor hard to read, which tends to bring the maximum of the indicial response rather earlier than desired. It could have been corrected, but this was not actually done.

The output is understood to be taken at the junction of L5, C40. The actual experimental indicial response curve is shown in Figure 24. The corresponding calculation was never made.

In the receive condition the phones are connected to the junction L5, R66. This point is chosen in order that the tuned circuit L5, C40 may lower the response at 2.3 kc/s and so help to remove inverted speech.

As has been mentioned elsewhere, the purpose of the condenser C29 is to delay the modulated pulse relative to the R.C. pulse, which normally occurs somewhat later. Except for high frequencies the condenser can be considered as giving a delay of 84 K. C29. With C29 = 150 pf this amounts to 12.6 μs.

(j) Transmit Bias Circuit (Figure 15)

If fixed bias is used for the pulse modulator the value of the bias voltage is very critical. The bias required is of the order of 17 volts, and a difference in this of 0.05 volt has an appreciable effect on the tripping percentage. A difference of about a volt suffices for a change from 0% to 100%. To get over this difficulty the bias is made to depend on the tripping percentage, a small change in tripping percentage having a considerable effect on the bias. This results in the bias and tripping percentage both settling down to an equilibrium value. This equilibrium value of tripping percentage is, of course, also dependent on component values, but it is not very sensitive.

In the receive condition this form of bias is not possible, owing to the fact that both circuits cannot be adjusted to give exactly 50% tripping percentage. With automatic bias as described above the receiver will produce its characteristic proportion of R.C. pulses regardless of the proportion produced by the transmitter, and if these do not add up to 100%, any discrepancy will result in errors, producing a noise like the crackle of rifle fire.

The mathematical theory of the bias circuit is not difficult. The input circuit C54, 55, R98 to the diode has such a short time constant (27.5 μs) that we can assume the condenser quite uncharged just before each remainder calculator pulse. Owing to the large size of the condenser C56, we may take the anode potential of the diode as a constant $-B$. On the peak of a remainder calculated pulse (which is negative as applied to this circuit) the cathode voltage will equal the anode voltage, so that the two sides of the condenser C are at $-E$ and $-B$, and the charge on it is $C(E - B)$. This charge must have flowed through the diode. Consequently if T is the average time between R.C. pulses, the D.C. current through the diode is $C(E - B)/T$. In the case that we are on receive, this is zero so that $E = B$. On transmit the current flows through $R32 + R34 = R$ say, so that $\frac{CR(E-B)}{T} = B$. Solving for B gives $B = \frac{E}{(1+T/CR)}$. Putting in actual values $C = 125$ pf, $R = 2$ M, and $T = 250\alpha^{-1}$ μs where 100α is the tripping percentage $B = \frac{E}{1+\alpha^{-1}}$. E is normally about 55 volts, and of course α should be $\frac{1}{2}$. $\frac{3}{4}B$ is available as actual bias.

The time required for the bias to reach its normal transmit value after switching is of importance in connection with the key-switch circuit. It may be assumed that there are no R.C. pulses in this period (since there is too much bias for them to occur), and therefore no current through the diode. Initially the anode voltage is equal to $-E$, and we wish to know when it will reach $E/3$. The time required will be C56 $(R32 + R34) \log_e 3 = 440$ ms.

(k) Send Receive Switch

This is done by means of two relays, one "A" relay, having six changeovers, and the other "B" relay, having two. Both relays are normal 3000 types, but the "B" relay has heavy-duty contacts since it has to switch voltages of the order of 700. The operating current is taken from the H.T. supply via R19 and R20, the relays being energized simultaneously on connecting the point "*A*" to ground either by pressing the pressel or operating the T/R switch on the Key Unit. The hold-on current for the relays is rather less than the current to operate; to save H.T. current by taking advantage of this fact C17 is connected across R20 to provide an initial surge on operation.

If the output suppressor and key switch are to operate satisfactorily, it is essential for the two relays to operate within 20 milliseconds of each other. The "B" relay has a much lighter spring load than the "A" relay and tends to operate first; to prevent this, it is slugged with resistor R21.

(l) Cypher Clear Switching

The cypher-clear switch is a D.P.D.T. switch mounted on the front panel between two indicator windows, one green and the other red. In normal operation this switch is put in circuit by connecting the wander lead in the cathode of the remainder calculator to the socket "S". With the switch in the "cypher" position, R51 in the remainder calculator cathode circuit is short circuited, and the Combiner scrambles normally. In addition, the junction of LP2 and R39 is made earthy by the other pole of the switch and LP2 lights and illuminates a green window, indicating that it is safe to carry on a secret conversation.

On putting the switch to "Clear," the junction of R51 and R52 in the remainder calculator cathode is put to ground and R51 is no longer short circuited; at the same time the earth is taken from the junction of LP2 and R39 and applied to the live side

of the "Key Input" jack. Thus, there is no key fed to the pulse modulator, and no remainder calculator pulses are fed into the output filter (although they are fed into the bias circuit in the usual way). In consequence, the output of the filter will be clear speech; in the lamp circuit, current flows through LP2, R39, and LP3; the resistance of this circuit is now so high that the current is only 60 m.a., which is sufficient to light up LP3 but does not affect LP2, hence the red window is illuminated. The supply to the indicator lamps is taken from the combiner heater supply so that one lamp will always be alight if the supply to the combiner is "on."

(m) Power Supply

Power for the whole equipment is provided by a small power pack of almost conventional type, the main points being the separate heater supply and the bias producing circuit.

The positive H.T. supply circuit is a full wave condenser input circuit with one section of smoothing and gives 120 m.a. at 350 volts with about 0.5% ripple.

The negative H.T. supply comes from a half wave condenser input circuit driven from one-half of the H.T. transformer secondary. The smoothing filter is a two-section resistance–capacity one which cuts down the ripple to negligible proportions. The high output impedance it produces is unimportant since the load on this part of the circuit is small and constant. The extra loading on one side of the mains transformer may also be neglected since the output current of the bias circuit is only about 5 m.a. The bias rectifier is at present a 6×5 valve, which is, of course, running well below its rating. It was used because it was the lowest rated rectifier available at the time of design; it is thought that some economy would be afforded by the use of a metal rectifier such as a Westinghouse 5 D 73.

The supplies are brought out on three sockets connected in parallel, one being a spare for the connection of any of the pieces of test gear mentioned in Part III.

(n) Testing Arrangements

For setting up and testing the apparatus, a cathode-ray oscillograph is essential, and a double-beam type is preferred. Two jacks are provided on the front panel of the combiner to facilitate the use of the C.R.O. If these jacks are used the C.R.O. should be fitted with a screened load of about 100 p.f. capacity and a plug 201.

The jack labeled "Monitor" is connected to the anode of the pulse modulator through 55 pf and enables the modulated pulses to be viewed; this jack is connected in such a way that its live side is put to earth through 100 p.f. when the plug is removed; this is to avoid the C.R.O. lead causing any extra loading when it is plugged in.

The jack labeled "Scope" connects to a wandering lead through either one or two condensers or directly, giving a choice of effective C.R.O. impedances. It should be remembered when using a condenser that the voltage appearing across the C.R.O. terminals has been attenuated due to this capacity and the capacity of the C.R.O. lead forming an A.C. potentiometer.

Sub-chassis in the combiner, there are three sets of test sockets and wander plugs which are used in the test procedure described in § 10.

The wander lead in the anode circuit of the pulse modulator short circuits R53 in the "normal" position or earths its junction with R54 in the "test" position. Thus, in the "test" position pulses are fed to the remainder calculators but not into the output filter.

The one in the cathode circuit of the remainder calculators operates in a similar way and prevents remainder calculators pulses from feeding into the output filter in the "test" position. In the position marked "S" this facility is transferred to the Cypher–Clear switch as explained in section (l); this is its position during operation.

The test sockets associated with R108 render it possible to prevent the synchronising sine wave from being fed to the cypher output jack.

In a combiner from which the Synch-Test circuit has been omitted it would be very useful to install a switch inside the chassis to take the place of Slb and to be used for setting up transmit bias.

(o) Key Unit Block Schematic

As described in the section on the combiner block schematic, the system requires a random voltage ($k(t)$) to be produced simultaneously at each end of the transmission path. This problem presents formidable difficulties. Of the possible solutions, the two that received most serious consideration are (a) recording random noise on discs or tape and using those recordings simultaneously at the ends of the transmission path and (b) generating identical voltages at each end. The first has the advantage that the keys are truly random and identical but has the disadvantage that the mechanical difficulties of starting and maintaining the keys in synchronism are large and, furthermore, the number of discs or reels of tape required becomes prohibitive. The second scheme is the one that has been tried in practice and has the following disadvantage. In the first place, the keys have to be produced to some prearranged plan and in synchronism with the rest of the apparatus so that they are not truly random; and in the second place, it is quite difficult to make the keys at the two ends identical. However, two units have been produced which have outputs sufficiently random for all practical purposes and which have the advantage of being simple, small and self-contained. The difficulty due to component differences and component instability has not been entirely overcome, with the result that the signal-to-noise ratio of the reconstituted speech is rather lower than is desirable. The purpose of this section is to describe, in outline, how the key is produced.

Six multivibrators are locked with the pulse from the combiner and their outputs taken to networks which serve both to isolate individual multivibrators and to differentiate the outputs (so as to strengthen, relatively, the higher harmonics). The fundamental frequency of each multivibrator is some exact sub-multiple of the combiner pulse frequency, the various sub-multiples being 5, 7, 8, 9, 23, and 31. (A special technique is needed to provide a multivibrator which will count down by as large a sub-multiple as 23 and still be stable; this technique is described in Section 8.) The outputs of these networks (26 in all) pass through the cypher machine and are combined at the output end to form seven inputs to seven distorting networks. The distorting networks have differing phase characteristics, so that the two outputs which are produced by combining their seven outputs at the plugboard depend enormously on what frequencies were fed into the various networks, i.e., on the setting of the cypher machine and the plugboard.

Up to this point the two outputs each contain a large number of frequencies, but the frequency spectrum is still very far from being the continuous one associated with random noise. A non-linear device in the form of a modulator is introduced and it intermodulates the two inputs to give sum and difference frequencies. The output of

the modulator thus has an enormous number of frequencies and is almost indistinguishable by ear from random noise. It may be recalled from the general theory that the requirements of an ideal key are the following:

a) The key values at the moments when the sampling pulses occur take all values between $-\frac{1}{2}$ and $+\frac{1}{2}$ with equal frequency and take no values outside this range
b) The key values at the times of the sampling pulses are independent.

The condition a) may be obtained by appropriate limiting arrangements, but actually it is not very critical and is probably sufficiently nearly fulfilled in the present unit which gives a rather better approximation to the ideal than obtains with the normal distribution as expected with unlimited random noise.

Some results concerning condition b) are mentioned in Appendix B. They show that if we have random noise with an energy density $P(f)$ at frequency f, where $\sum_{n=-\infty}^{\infty} P(f+n) = Q(f)$ is constant, and limit it approximately for a), we shall satisfy our requirements. The actual form of $P(f)$ is somewhat as shown in Figure 21 and satisfies the conditions fairly well. Strictly speaking, the measurement of $P(f)$ should be made before limiting, but this is not actually possible as there is no place in the key unit where such a signal exists. It is not thought that this makes any appreciable difference.

The multivibrators start simultaneously, and since they have fundamental frequencies which are prime to one another it follows that they will arrive back at the starting position after a time $5 \times 7 \times 8 \times 9 \times 23 \times 31$ times the period of the locking pulse. That is, the key will repeat after $1{,}785{,}600 \times 250\,\mu\text{sec} = 7.48$ mins. Provided, then, that we change the cypher machine setting at least every 7 min. We are assured of producing a non-repeating key. In actual operation this means that one person may speak continuously for only 7 min. before transferring control to the distant end of the link. This may be looked on as a limitation, but it is felt that 7 mins. is an adequate allowance.

The security would be enhanced if the various multivibrators did not all start up together but had variable and interchangeable delays of one, two, or three time units. A scheme has been proposed for providing those delays, but the extra complication was not thought justifiable in the First Model.[2]

8. Stage-by-Stage Key Unit Circuit Details

(a) The Multivibrator

The multivibrators in the key unit must provide accurate frequency division and must be stable over long periods. This is fairly easy to achieve on ones that count down by factors less than 10, but a multivibrator counting down by large primes such as 23 is not a practicable proposition and the circuit described later was devised for this purpose.

The first problem was to choose a suitable valve. For reasons of space economy a double triode was considered essential and it was desirable to use a valve which required the minimum of heater current. A valve satisfying these requirements is the 6C8G and this type was standardized throughout the key unit. Since then a new type has been brought to the notice of the authors. This is the 6J6, a miniature

[2]It has been assumed above that the reader is familiar with the cypher machine used. Should that not be the case, it will be sufficient to understand that the machine is a device enabling 26 contacts to be connected to 26 others in a pre-determined random manner and that the mode of connection may be changed by pressing a key.

double triode, which has the additional advantage of having a low anode impedance; with this valve the multivibrator mechanical design could be considerably simplified.

The anode loads and H.T. feed arrangements were next fixed to suit the valve working conditions.

To make the circuit more stable with respect to random voltage pick up it was decided to return the grids to a positive potential and, so that too large a locking pulse would not be needed, the fairly low value of 50 volts was chosen. The locking pulse from the combiner was arranged for before the key unit was designed and had a maximum amplitude of dome 40 volts. The locking pulse amplitude was standardized at 37 volts.

Various methods of feeding the locking pulse on to the multivibrator were tried and it was found that the best results were obtained when negative pulses were fed to the anodes. The pulse feeds through the grid coupling condenser and on to the grid of the other triode. If that triode is conducting then, in spite of grid current, the pulses appear inverted and amplified at the anode, from whence they are fed to the grid of the other (cut-off) triode, which will begin to conduct when some pulse raises the grid above cut-off.

The chief objectives to be attained in the design of a multivibrator are that the circuit should remain locked even if the components are appreciably different from their rated values, and the waveforms should vary little with component values. In the case that locking pulses of known size can be applied to the grids, the first problem can be treated mathematically quite conveniently. Two main facts emerge from the analysis and are such as might be expected from common sense considerations. The pulses must be of sufficient amplitude that, on the grid voltage curve, the peak of one pulse should rise above the foot of the next. This need only apply for the pulse which locks and the immediately preceding one. The second fact is that the ratio

$$\frac{\text{Maximum time constant for locking}}{\text{Minimum time constant for locking}} = \frac{N}{N-1},$$

where N is the number of locking-pulse periods during which the grid in question should be below cut-off.

From this it follows that, to obtain the maximum tolerance and to ensure that identical multivibrators have identical waveshapes, the multivibrators should be locked on both grids and each valve should be cut off for intervals of time which differ by, at most, one locking pulse period. This in effect means that the tolerance on the time constant is $100/(2N-1)\%$. If we know the pulse size we can calculate the nominal value of time constant. In practice, however, when we are providing the locking pulses via the other valve their amplitude becomes a rather doubtful quantity. Grid current makes it difficult to calculate their amplitude. Attempts to estimate them were eventually abandoned. However, even with unknown pulse amplitudes theory gives us some indications. The condition that the pulses must "overlap" as described above and this fact combined with knowledge of the voltages involved (cut-off volts, grid-leak return volts, initial volts) leads to the conclusion that the nominal time constant must not be less than a certain calculable minimum. If the condenser has already been chosen, this in effect means that there is a "minimum grid leak" for each order of division. In practice it is best not to exceed this minimum by very much, otherwise the tolerances of the components controlling the pulse amplitude may become too significant. Roughly speaking, the effect of an error in pulse amplitude of $p\%$ is

equivalent to an error of $p/N - 1\%$ in time constant, when the pulse is of minimum size (and therefore the grid leak a minimum also), but for larger pulses we should multiply this by the ratio of the actual pulse to the minimum.

The procedure actually adopted in designing the multivibrators was first to choose appropriate condenser values. These condensers were standardized at 300 pf. for all multivibrators, since this is a preferred value which is small enough to allow the associated anode to rise fairly sharply when the valve starts to conduct and yet which is not so small as to necessitate very large values of grid leaks. The minimum grid leaks were then calculated, and convenient values for actual grid leaks were chosen about 10% higher and in preferred values if possible. The pulse feeding components were then adjusted until the multivibrator was in the centre of its tolerance range. The tolerance range was determined by varying not the grid leaks but the frequency of the locking pulses; when this method is employed it is important to ensure that the shape and amplitude of the locking pulses do not depend on the frequency.

As mentioned in Section 5 the key output has to be switched on at moments decided by the transmitter. A bias is provided by the combiner for this purpose.

One grid of each multivibrator is returned to a potential of 50 volts produced by a potentiometer in the key chassis. The other grids are commoned and connected to the "Bias" jack, which, in turn connects with the Bias cathode follower in the combiner. When the key switch in the combiner is not fired the bias voltage is -210, and since each multivibrator has one grid held at this potential there is no output from the key unit. The instant the key switch fires, the bias voltage rises to $+50$ volts and each multivibrator grid begins to rise exponentially in the normal way and the multivibrators will oscillate as long as the bias remains at this high value.

The value of the negative bias was chosen to be -210 because this is the voltage to which the grid falls during normal operation, and ensures that the multivibrator behaves normally during the first half cycle.

The 2.47 megaohm resistor in the key untit joining "Bias" to the 50 volt potentiometer provides a current drain from the 50 volt supply when the bias is negative equal to the drain due to the grids when the multivibrators are running. This prevents the 50 volt supply changing when the bias becomes positive.

To simplify the key chassis design and to simplify maintenance it was decided to make each multivibrator a plug-in unit. A set of spares is provided and in the event of any multivibrator failing it is a simple matter to remove it and insert another. The small diagrams show the final multivibrator designs, while the main circuit diagram shows only the sockets in the key chassis which take the multivibrators.

The grid leaks and pulse feed resistors in the first models were carefully selected, but 10% tolerance components were used for the other parts of the circuit. After manufacture each multivibrator was tested for tolerance by fixing the working conditions and varying the pulse frequency about 4 kc/s. It was found necessary to trim the grid condensers to obtain reasonable tolerances, and it is thought that closer tolerance components should be used throughout to make the circuit more stable with respect to variations of the various voltages. In use, the units have been very satisfactory and far less trouble has been experienced than was anticipated.

(b) High Order Frequency Division Circuits (Figure 17)

A single multivibrator is not suitable for frequency division where the order of division is more than about 10, owing to the very narrow tolerances in component

values and voltages which would be necessary. Large orders of division may be obtained by locking one multivibrator with the pulse frequency and deriving a pulse from it to drive another lower frequency multivibrator. For example, we may divide by 24 by dividing down from the pulse by 6 and so producing a frequency of 666.6 c/s. This square wave may now be differentiated to produce pulses of this frequency which are used to lock a multivibrator whose natural frequency is about 166 c/s. For our present purpose we need to count down by large prime numbers and it is obvious that the above method, as it stands, is not applicable. However, we may modify it to count down by large primes which are nearer to the product of two integers. Thus $23 = 24 - 1 = 6 \times 4 - 1$, and, by modifying the above circuit, we can achieve the desired result.

The divide by 6 circuits is normal and is locked on both grids. The tripping circuit has a frequency approximately one quarter of that of the divide by six, but one grid circuit has a time constant of only 500 μsec or so while the other grid circuit has a long time constant. The "short leg" grid is fed with normal locking pulses and is raised above cut off by the second pulse after the valve becomes non-conducting (grid 4, Figure 18). The output of one anode of the divide by 6 is differentiated and applied to grid 3 of the trip circuit (Figure 18), causing that grid to be raised above cut off on the fourth pulse. Grid 3 is returned below cut off again after 500 μsec due to the effect of the locking pulse on grid 4. The resulting wave form of the tripping circuit is shown at anode 4 in Figure 18. This output is differentiated and applied back to the divide by 6 circuit causing it to trip one time unit sooner than normal so that the process illustrated at grid 3 may repeat.

In the above it must be appreciated that locking is done by feeding the various voltages on to the anodes as described in the previous section.

The high orders of division used in the key unit are 23 and 31. The latter being obtained by using a tripping circuit in conjunction with a standard divide by 8. In each case a total of four outputs is taken from the multivibrator itself and two from the tripping circuit.

(c) Multivibrator Output Networks (Figure 19)

Since the outputs of several multivibrators get connected together when they reach the distorting networks it is necessary to ensure that they do not influence one another through this interconnection. It is necessary, therefore, to provide attenuation between the multivibrators and the cipher machine. It is also desirable to attenuate the lower frequencies more than the high, in order to provide a more uniform energy spectrum at the networks; this is affected by using a small blocking condenser (470 pf). A small delaying condenser (200 pf) is also provided in order that any remaining interaction between the multivibrators may be delayed so as not to coincide with locking pulses, and therefore so as to be very unlikely to disturb the locking. From each anode either one or two outputs are taken; in the case that only one output is taken, the 200 K resistor is omitted.

The output networks described above and shown in Figure 19a are a conservative design, and probably unnecessarily elaborate. It is suggested that the networks shown in Figure 19b would probably be quite adequate, and should be tried.

Another criticism of the present output networks concerns the levels of the outputs from the various multivibrators. Owing to the differentiating effect of the output networks, there is a tendency for the higher frequency multivibrators to deliver more power than the lower frequency ones. This is particularly noticeable in the case of the

"divide by 5" multivibrator and it might perhaps be advisable to decrease its output by 2 dB (say) by modification of the output networks associated with it.

(d) Distorting Networks

The distorting networks were chosen to give very differing phase characteristics. On the whole they were also desired to have fairly level response up to 2 kc/s and little response at high frequencies, but this was at most a guiding principle. Another important requirement concerned the output level from the networks. They should give equal output power when the inputs have equal power and have the typical energy spectrum to be expected from the multivibrators. This requirement is necessary in order to guard against the possibility of the output from one network dominating all the rest, thus facilitating the breaking of the system.

(e) Modulator (Figure 20)

The modulator is intended to give an output which is essentially the product of the two inputs. There is no need for it to be an exact product, but it should at least have the right sign, and it is of course very desirable that the output be reliable, i.e., that two different modulators made to the same design, and fed with the same in out voltages should not give appreciable different output due to component differences; it is thought that the present design is capable of improvement in this respect.

The modulator contains two double triodes and two double diodes. The first double triode, a 6SC7, is simply a high gain voltage amplifier for each of the inputs. The second double triode 6C8G is used as a phase inverter for each of the amplified inputs. It is important that the anode and cathode loads (5 K) of these should be accurately equal. Taking these stages for granted, the circuit reduces itself to that shown in Figure 20a. I shall follow out the theory of the circuit assuming in effect zero output impedance for inputs S_1 and S_2 and also ignoring the load. In this case we can replace the circuit by that of Figure 20b and assume zero total current through all the diodes.

A preliminary argument based on symmetry is of interest. Let the output voltage be $F(S_1, S_2)$. Let us try to calculate $F(S_1, -S_2)$. The circuit required to produce this may be seen to be derived from that which yields $F(S_1, S_2)$ by changing the signs of the inputs and the directions of the diodes. It therefore yields $-F(S_1, S_2)$. In other words, we have

$$F(S_1, -S_2) = F(S_1, S_2)$$

and similarly

$$F(-S_1, -S_2) = -F(S_1, S_2).$$

Combining these two equations with

$$F(S_1, S_2) = F(S_2, S_1),$$

we may write

$$F(S_1, S_2) = S_1 S_2 G(S_1^2 + S_2^2 + S_1^2 S_2^2).$$

This argument is of interest as it shows how far we can get without making any assumptions about the diode characteristic, and such arguments are of very general application to circuits of this nature.

To obtain a more complete theory we must assume something about the diodes, and we shall assume that they are always either short circuit or open circuit, changing over at zero anode voltage. Putting x for the output voltage, we have for the current through all the diodes,

$$\frac{2}{R}[(q-x)H(q-x)+(-q-x)H(-q-x)+(p-x)H(-p+x)+(-p-x)H(p+x)]=0,$$

where

$$H(t)=\begin{cases}1 & t>0\\ 0 & t<0\end{cases},$$

so that

$$H(t)=\frac{1}{2}+\frac{1}{2}sgn\ t$$

and

$$tH(t)=\frac{1}{2}t+\frac{1}{2}|t|.$$

Then

$$4x=|q-x|+|q+x|-|p-x|-|p+x|,$$
$$x=\frac{1}{2}\mathrm{Max}(|q|,|x|)-\frac{1}{2}\mathrm{Max}(|p|,|x|);$$

i.e.,

$$x=\frac{|c|-|p|}{2}\qquad \text{if } |x|\leq \mathrm{Min}(|p|,|q|),$$

i.e., if

$$\frac{\mathrm{Max}(|p|,|q|)}{\mathrm{Min}(|p|,|q|)}\geq 3,$$
$$x=\frac{|q|-|x|}{2}\qquad \text{if } |q|\geq|x|\geq|p|,$$
$$x=\frac{|x|-|p|}{2}\qquad \text{if } |p|\geq|x|\geq|q|,$$

i.e.,

$$x=\frac{1}{3}\ \mathrm{Max}(|p|,|q|)\ sgn(|q|-|p|)\quad \text{if}\quad \frac{\mathrm{Max}(|p|,|q|)}{\mathrm{Min}(|p|,|q|)}\leq 3.$$

Putting

$$p = \frac{S_1 + S_2}{2}, \qquad q = \frac{S_1 + S_2}{2},$$

this becomes

$$x = \frac{1}{2}\,\frac{|q|^2 - |P|^2}{|q| + |p|} = -\frac{1}{2}\frac{S_1 S_2}{\mathrm{Max}(|S_1|, |S_2|)} \qquad \text{if Max } \left(\left|\frac{S_1}{S_2}\right|, \left|\frac{S_2}{S_1}\right|\right) \geq 2;$$

$$x = -\frac{1}{6}\,(|S_1| + |S_2|)\ sgn\ S_1 S_2 \qquad \text{otherwise.}$$

An approximation to x which is rather better than (const) $\times\ S_1 S_2$

$$x = \frac{S_1 S_2}{2\sqrt{S_1^2 + S_2^2}}.$$

This gives the right sign and has an error in magnitude of at most 10%.

An output of this kind will have an effect similar to $S_1 S_2$ from the point of view of having a great variety of frequencies. The output $S_1 S_2$ originally suggested was only an indication of what was desired. The purpose of the 0.01 μF condenser on the output is to eliminate the higher frequencies to some extent.

(f) Testing Arrangements

The testing facilities are provided on the rear panel of the units. There is a row of test sockets for measuring the critical voltages and a Yaxley switch and jack to check that the multivibrators are locking satisfactorily. The use of the voltage test points needs no further comment, but the multivibrator test point requires a little explanation.

The Yaxley has eight positions: *N*, 5, 7, 8, 9, 23, 31, *L*. Under the Yaxley and to the left is a test jack, and to the right is a toggle switch. With the Yaxley at "*N*" and the toggle switch pointing to the jack marked "Output," the key unit is operating in its normal condition. With the toggle switch in the other position, various voltages may be selected by the Yaxley and fed to the test jack. These voltages are the outputs of the various multivibrators and the locking pulse. To avoid the use of C.R.O. amplifiers, these voltages are amplified inside the Key Unit by switching the grid of the first amplifying valve in the modulator. For monitoring the multivibrators, it is convenient to use headphones when checking locking, but the C.R.O. must be used when checking that similar multivibrators in two chassis are starting in phase when the key switch fires; the oscillogram Figure 24b was taken in this way.

PART III: OPERATION AND MAINTENANCE

9. Test Gear

(a) Noise Generator (Figure 22)

It is convenient to be able to test combiners independently of the key units so as to track down the source of any loss of intelligibility. To do this, we use, as key in the

transmitter, random noise from some such source as a gas triode, a radio receiver, or a saturated diode. The necessary 250 μsec delay at the receiver is obtained by passing the same random noise through an artificial line. This paragraph describes the noise generator used during development.

The noise source in this case was a radio receiver (H.R.O.) without aerial but with the B.F.O. switched on. The noise generator has an input transformer to match into the output stage of the H.R.O., followed by a resistor to increase the impedance presented to the rectifiers which are connected "back to back" to limit the noise in the same way as the speech is limited. A filter is now inserted to remove all frequencies above 2 kc/s. The final stage is a 6AC7 working class "A" and giving an output of up to 10 volts peak to peak at an impedance of 10 K.

(b) Delay Line (Figure 23)

A small piece of equipment was made to enable two combiners to be used with receiver noise for the key instead of a key from key units. When this is done, it is necessary to delay the key provided for the receiver by one time unit (250 μs). A straightforward delay line was used together with simplifying stages. The delay line consisted of 30 series inductances of 1 mH nominal and 30 shunt condensers of 0.1 μF. These figures were arrived at as follows. It seems necessary, to avoid distortion, to have at least 20 sections, although this might have been reduced if some correcting networks were used. The only inductances available quickly in large quantity were 1 mH, and the condensers available were 0.01, 0.05, 0.1, and 0.5. This determined the condenser as 0.1 μF and the number of sections about 25. It was thought advisable to include the 30 sections and to make the delay variable by switching. A fine delay control was also incorporated in a resistance capacity section. The values of the inductance and capacity elements being now fixed, the characteristic impedance of the line is found to be 90 ohms. The line was therefore terminated in this resistance. In view of the finite resistance of the chokes, it was necessary to put resistors in parallel with the condensers to make the line more nearly distortionless.

In view of the low characteristic impedance of the line, it was necessary to have the input to the line at a low impedance. This was provided by an amplification stage consisting of half a 6SN7 working into 7:1 step-down transformer, giving an output impedance of about 120 ohms. The exact characteristics of this first stage, including the transformer, fortunately do not matter, as they are common to the transmitter and receiver circuits, and may be considered as part of the original noise generator. In particular the exact value of the output impedence of the transformer is insignificant from the point of view of the relation between the waveforms provided at the two outputs; one may even consider the output impedance of the transformer to be zero, provided that the corresponding E.M.F. is taken to be the actual voltage which appears across the secondary in operation. Adopting this attitude, a series resistor of 90 ohms is put in series with the delay line between it and the transformer, and the output for the transmitter is taken direct from the transformer. Between the end of the delay line and the output for the receiver there are two stages of amplification to give sufficient power and the correct polarity. There is a changeover switch to enable the delay line outputs to be interchanged when the transmitting combiner is changed.

(c) Indicial Response Test Set

This device, as its name suggests, is used primarily to check the response of the output filter. A single pulse fed into the filter will produce a voltage at the output as shown in Figure 3c. However, to view this curve on a C.R.O., we need to make it recurrent. It is not sufficient to feed in unmodulated pulses from the pulse modulator since the outputs due to consecutive pulses would interfere on the C.R.O. To get a satisfactory picture on the screen we feed in pulses having a period of eight times as long as that of the modulated pulses. It is easy to produce these pulses from the remainder calculator if modulation is applied to the pulse modulator so as to produce one pulse larger than standard sine in every eight pulses. The test set produces this modulating voltage.

The first stage is a multivibrator driven from the locking pulse and dividing by eight. In the circuit diagram this is shown as a built-in multivibrator, but it could well be a standard plug-in type as used in the Key Unit. The output of this stage is applied via a grid stopper to a pentode of which the cathode is returned to a variable positive potential. At the anode of the pentode a square wave-form is produced with a negative going voltage which is variable in time over a small range. This can easily be seen to be so if it is remembered that the anode voltage of the multivibrator does not rise sharply. This square wave is differentiated and applied to a diode which shorts the positive pulse to ground. We are now left with a sharp negative pulse variable in time. A Kipp relay is triggered with this pulse and produces at its cathode a positive pulse of about 100 μsec wide and variable in time. In order to square up and invert this pulse, it is applied to another pentode, giving as the final output a negative pulse of 100 μsec duration, variable in time over a small range, at a frequency exactly one eighth of the locking frequency and with an impedance of 10 K. The time delay on the output pulse is provided to enable it to be adjusted so that its centre coincides with a modulated pulse in the combiner.

A circuit diagram is included with the report and a description of the use of the apparatus is given in the next section.

10. Setting Up and Routine Checks

Connect both combiner and key unit to the power pack, switch on and allow 10 mins. to warm up.

Check that the H.T. is 350 volts ±5 volts. The load is fixed so there is no trouble due to pack regulation, but mains voltage variations have been found to be a source of trouble in the first model and it may be necessary to feed the power pack through a constant voltage transformer.

Switch to transmit and check the frequency of the mod. Pulses (scope jacked to the "Monitor") against a B.F.O. or other frequency standard. Adjust the frequency with the insulated trimming tool to within a few cycles of 4 kc/s.

Shape the mod. Pulses by adjusting C18 until they have the shape shown in Figure 24a.

Adjust the remainder calculator feed trimmer C24 until the mod. Pulses as seen on the scope measures 122 volts. Next, plug a pair of phones into "Cypher Out" press "Synch Test" and adjust the bias condenser C55 until a clean 2 kc/s tone is heard in the phones. If "Synch Test" is to be omitted from the circuit, the switch Slb should be provided for the purpose of setting up this bias (see circuit diagram). C24 will now need re-adjustment, and then C55 will need to be trimmed again. These two trimmers should be adjusted by successive approximation until the pulse has the

correct amplitude and the clean tone is heard at the output; the adjustment is not at all difficult. The pulse amplitude has been fixed to be 122 volts to ensure that the pulse modulator is worked on the linear part of its characteristic. The 2 kc/s tone indicates that the remainder calculator is producing exactly 50% of remainder calculator pulses and hence that the transmit bias is correct.

Connect "Lock" "Key Bias" and "Key Input" to the appropriate jacks on the key unit. Plug the, scope into "Scope" and connect the wander lead to the "Lock" jack; adjust the resistor R78 ("Pulse") until the amplitude is 37 volts.

Now adjust R100 until the voltage (as read on the 400 volt range of an A.V.O. model 7) at the test point B on the key unit is 50 volts.

Adjust the potentiometer marked "+60" at the rear of the key unit until the voltage (read on the 400 volt range of the A.V.O.) at test point 60 is 50 volts.

Key switch bias should now be adjusted. With the combiner on receive, turn the potentiometer on the front panel until the key switch indicator just lights. Now turn a few degrees clockwise and the indicator should go out when the combiner is switched from transmit to receive. Check that the neon lights after a delay of about one second on switching from receive to transmit. (If the receive bias potentiometer is incorrectly set, the neon may strike immediately on switching.) Adjust the key switch bias potentiometer until the indicator remains out on receive but lights after a slight delay on changing to transmit. This adjustment will usually be sufficient, but further trimming may be needed when a complete link is set up.

This completes the setting of the present controls and the equipment is ready for use. The adjustment of the front panel manual controls is described under the section on operation. The rest of this section is devoted to the method of using the test gear described in section 9.

To check indicial response of the output filter, the following procedure should be adopted. Run the combiner alone and adjust the voltage to 350. Feed lock to the indicial response test set and feed its output to the key input jack of the combiner. Switch to transmit and connect a crocodile clip to the key input jack of the combiner. Switch to transmit and connect a crocodile clip from the slider of R96 to the junction of C56 and R32; this enables the receive bias potentiometer R96 to control the bias on the pulse modulator in spite of the combiner's being on transmit. Short circuit the mod. Pulse to ground at the junction of R53 and R54, and short circuit the synchronising wave at the junction of R108 and R112 with the test plugs provided. Plug the oscilloscope into the "Cypher Out" jack (amplifiers may be needed since the voltage will be of the order of 3) and adjust the receive bias control and 'scope time base until a clean picture as shown in Figure 24b is obtained.

The receive bias control reduces all mod. Pulses until only the large ones due to the modulation of the test set are of sufficient amplitude to effect the remainder calculator, and it is this pulse feeding into the output filter which produces the desired waveform. It is convenient to display mod. Pulses on the second beam of the, scope to serve as timing markers. Examination of the photographs in Figures 24b to 24d will show that the response is not quite zero two time units after the initiating pulse. It was found experimentally that a response of this form at the output of the combiner was better than one having the theoretical one of Figure 3c. The method of adjustment during design was to have two combiners working with the delay line and random receiver noise as described below and to adjust R66 in the transmitting combiner until noise due to uncancelled remainder calculator pulses was a minimum. It was then found that the ideal response originally set up had degenerated to the one

shown in the Figure 24. It is thought that the circuit of the combiner up to the grid of the pulse modulator has a small compensating effect.

The indicial response can also be observed by grounding the remainder calculator pulses at their test socket and allowing the mod. Pulses to pass into the filter. However, care is needed in interpreting the result since the response is complicated by the 4 kc/s and harmonics due to the pulses. It is necessary to use this method to check that the output due to standard modulation (37 volts at the anode of the pulse modulator) on the pulse is the same as the output due to one remainder calculator pulse.

During test and to assist fault finding it is useful to be able to use combiners independently of key units. Two combiners are set up as for normal operation except that the key units are omitted and instead, the key used is random noise from a receiver or other noise source. The 250 μsec delay for the receiver is obtained by passing its key through a delay line. A switch on the delay line chassis enables the functions of the two output jacks to be interchanged when one combiner is switched to transmit and the other to receive. With the delay line the receive and transmit keys are much more nearly identical than with the key units and a good degree of cancellation is possible. The photograph Figure 25d was taken under these conditions and shows the mod. Pulse at the receiver. The mod. Pulse, it will be seen, has only two amplitudes (depending on whether the transmit remainder calculator has fired or not) showing that the key modulation had been successfully cancelled off (there was, of course, no speech modulaton at the transmitter while this photograph was taken).

11. Operation

This section attempts to give some idea of the method of operation indicated by tests in the laboratory. Up to the present, it has not been possible to carry out any field trials, but it is proposed to do so at the earliest opportunity so as to gain experience to serve as a basis for future improvement.

The combiner has four knob controls, one switch, and three pilot lamps, while the key unit has two keys which may or may not be worked independently and one pilot lamp. It will be convenient to first consider the function of all these controls separately.

The switch on the combiner is largely self-explanatory. In one position the combiner is operating as a scrambler and a green pilot lamp lights; in the other position the combiner will receive or transmit clear speech and a red warning lamp lights.

The four knob controls are operative only on receive.

- "Key Vol." controls the amplitude of key voltage which is added to the incoming cypher; in correct adjustment, the smooth noise due to uncancelled key is at a minimum.
- "Cypher Vol." controls the amount of cypher plus key which is applied as modulation to the pulse modulator.
- "Bias" adjusts the amount of bias on the pulse modulator; when incorrectly set a noise of loud crackles is heard in the phones.
- "Synch" varies the phase of the pulse generator with respect to the incoming synch, sine waves and hence with the transmit mod. Pulses.

The remaining pilot lamp is the key switch indicator which, when lit, shows that the key unit is running. The key unit manual keys rotate the cypher machine and change the combiner from transmit to receive and vice versa. The keys are really independent, the one marked "code change" rotating the cypher machine and the one

marked "T/R" operating the combiner relays. When "code change" is pressed the cypher machine is rotated and the spring returns both keys to the normal position, and an arm on "T/R" changes over two small switches; one switch operates the combiner relays and the other operates an opal pilot lamp on the key chassis. The switches are such that they make and break on alternate operating strokes and are ganged so that the pilot lamp lights only when the combiner is on transmit. The combiner may be changed from receive to transmit or transmit to receive without alteration of the cypher machine setting merely by pressing the "T/R" key and releasing it. The code setting may be changed without operating the combiner relays by pressing the "code change" fully, pressing in the small button to the right of the keys until it engages with the "T/R" key and then releasing "code change." "Code change" will return to normal, but the "T/R" key will remain in at the bottom of its travel and the switches will not be operated. To release the "T/R" key, press it slightly until the rotating button flies free, and then release it.

The method of operation in the Laboratory will now be explained. Two sets of equipment are set up in adjacent rooms and connected by two short lines at "cypher out" and "cypher in." The combiner is put to transmit and the other to receive, and the synch control of the receive combiner is adjusted while listening in the phones. A region will be found on the potentiometer over which the noise in the phones is fairly low and which has boundaries defined by a high-pitched buzzing noise. Over this region the receive combiner is working at the same frequency as the transmit combiner, and if the control is set to the centre of the range the receive apparatus will be very nearly synchronised. Now the direction of transmission is changed over and the other combiner synchronised.

Put both combiners to receive and, by flipping the T/R key of the one which is to be used as receiver, get it to the receive position with the key switch indicator extinguished. Check that the cypher machine settings are identical and press the T/R key at the transmit end. The key switch indicator should go out and light up again after about 300 ms. and at the same time the key switch indicator at the receive end should light up. Now listening in telephone at the receive and adjust key vol. for a minimum and adjust bias to the centre of the range defined by the loud crackles, then adjust cypher vol. for minimum noise. These three controls should be adjusted until the minimum of noise remains in the phones; the various controls have different effects on the quality of the background noise and a little experience soon indicates how to obtain the best results.

Some improvement may be obtained by adjusting the synch control, but great care is needed since, if the combiner slips out of lock the key will also slip out of lock, and the receive and transmit keys will no longer be identical even when synchronism is regained. Speech may now be fed into the transmit combiner as "Mic," and the controls re-adjusted to obtain the maximum intelligibility.

The T R switch on the transmit combiner should now be pressed to put it to receive (the key switch indicator will extinguish) and then the receiver T/R switch should be pressed. Having successfully changed the direction of transmission in this way adjust what is now the receive combiner in the same way as before.

Most of the work in the laboratory has been done with speech taken from a recording, but a conversation can be carried on between the two sets if the following points are observed. The transmit apparatus must be changed to receive before the receive is changed to transmit, and the change should be effected by pressing the "code change" key so as to change the code as well as the direction of transmission (this is not essential, but it is the way the apparatus is intended to be used).

To the right of the cypher machine in the key unit there is a slip of paper protected by a sheet of celluloid; this is used in setting codes on the cypher machine. On the paper are five columns of letters, each of which is a complete alphabet arranged in random order. Any letter in this table may be specified by two co-ordinates, the first giving the column and the second the row. The letters are required in sets of five and since there must always be one letter from each column, the column co-ordinates is omitted but is contained in the order of the row co-ordinate. That is to say, in a series of five letters is specified by five numbers in the range 1 to 26, the first number *n* indicates the *n*th letter in the first column, the second number *m* is the *m*th letter in the second column, etc. In addition, the numbers of the columns refer to the wheels of the cypher machine reading from left to right. For example, if the sequence of numbers is 6 8 11 3 22, the left-hand wheel of the cypher machine is set to the letter in the sixth row of the first column, the next wheel of the machine is set to the letter in the eighth row of the second column and so on. Fresh paper slips are provided each day together with information giving the arrangement of the wheels in the cypher machine and the plugs in the plug board.

The following procedure has been suggested for making contact on an R/T link. It has not been tried under such conditions but has been found satisfactory over a short line, although it is then more complicated than is necessary due to there being no need to report signal strength.

We take account of only two stations; one is called "Control" for the sake of clarity, though normal R/T procedure should be adopted fact. Both sets are normally on clear and receive. During preliminary conversation to establish the link, both operators take the opportunity to adjust the synchronisation. (This is facilitated by calibration on the synch control because the operator will know from previous experience the approximate position of the control.)

Control: Hello BOLO, are you receiving me?, over.
Out Stn: Hello Control, I hear you R 4, report my signals, over
Control: Hello BOLO, R5. I have a message for you:- Figs 2 18 5 8 14 Over.
Out Stn: Hello Control, message received Figs:- Figs 2 18 5 8 14 over.
Control: Message correct, wait.
(Both stations now work out cypher machine setting and set up machine: when done Control continues)
Hello BOLO, figs set, over.[3]
Out Stn: Hello Control, figs set, over to green and over to you.
(Out station. changes to cypher and presses code change; Control changes to cypher, presses code change and continues.)
Control: Hello BOLO, hello BOLO are you receiving me?..... etc.
(for five seconds or so to allow BOLO to adjust controls)... are you receiving me? over.
(presses code change)
Out Stn: Hello Control, I hear you R 4.... Etc. (for five secs. To allow Control to adjust his set)... over.

[3]Up to this point "T/R" switch only is pressed; after this point "code change" is always pressed.

Control: Hello BOLO I have a message for you . . . (secret conversation continues).
(After all conversation has been finished both ends go to clear and receive).

Communication will break down if either end mishandles the synch control or if the cypher machines fall out of step. Should this happen, the out station should go to receive and clear; control should go to transmit and clear and try to make contact again. When contact has been made on clear the starting up procedure should be repeated.

12. Some Suggestions for Future Developments

A small and compact speech privacy equipment has been devised and constructed. The system offers very high security, but before it can be put to field use considerable further refinement is essential, and even then the sphere of application is bound to be limited. The following comments are intended to serve as a guide to further development.

The combiner as a whole is fairly satisfactory as can be shown by operating it with the same key at receive and transmit ends. However, the articulation could probably be improved if the speech bandwidth was increased to 2.5 kc/s. This would entail an increase in total bandwidth of 1 kc/s, but this is not a serious objection since it would not affect operation over a radio link and the present 4 kc/s bandwidth is, in any case, too wide for an ordinary line. The speech input and limiting arrangements at present leave much to be desired and a more suitable microphone amplifier could be built into the combiner to replace the present external one. A consideration of the pulse modulator stage with a view to improving its linearity should yield better quality speech. The main operating difficulty with the combiner is due to the ease with which the receive combiner can be slipped out of lock when adjusting the synch control, and it is felt that the synchronising system could be improved from this point of view. Two valves (V4A and V6A) are working under conditions which over-load the heater-cathode insulation by 150%. The valves have shown no signs of distress, but their lives may be considerably shortened.

The existing key units have been matched by trimming components, but for production models it would be necessary to use more stable and closer tolerance components if the signal/noise ratio is to be improved. The multivibrator mechanical design could be improved by using an octal plug which could be securely bolted to the sub-chassis and by the provision of some quick-release clamping arrangement to hold the multivibrator in the key chassis.

At one stage of the development it was found that mains voltage variations altered the power pack voltage to the extent the multivibrators would not remain stably locked. The trouble seems to have disappeared, but it may be found necessary to stabilize the power pack voltage to ± 10 volts if the equipment is to be used in regions of poor mains voltage regulation unless great care is taken in setting the multivibrators to the centre of their tolerance ranges during production.

With these improvements, together with others which are bound to become evident as experience is gained with the system, it should be possible to provide a reliable and compact high-security speech privacy system for application in a limited field.

ABBREVIATION	DESCRIPTION	COMMENT
A.V.O.		The trade name of a portable test meter widely used in the 1940s
B.F.O.	Beat Frequency Oscillator	Standard test equipment at the time
C.R.O.	Cathode Ray Oscilloscope	Standard test equipment at the time
D.P.D.T.	Double Pole Double Throw	Standard electrical component
E.M.F.	Electro Magnetic Field	Standard electrical term
H.R.O.	National HRO	WWII—popular professional radio receiver (see http://en.wikipedia.org/wiki/National_HRO)
H.T.	High Tension	Standard electrical term
M.P.	Modulated Pulse	
O/P	Output	
O.T.P.	One Time Pad	
P.U.P.	Percentage of Unwanted Power	
P.M.	Pulse Modulator	
P.O.	Post Office	
pot.	Potentiometer	Standard electrical component
R.C.	Remainder Counter	This could be confusing. R.C. is often used in electrical terms to describe a Resistor Capacitor combination giving a time constant

Appendix A. Theoretically Perfect Security of One-Time Pad System

We shall show that if the Conditions a), b), and c) from page 2 are satisfied, then denoting by $P(C, L)$ the probability of the cipher C having decode L, we have $P(C_1, L) = P(C_2, L)$ for all L and all C_1, C_2 of equal length.

Let us consider the following method of determining the probabilities $P(C, L)$. We make a list of all the possibilities, i.e., of all the possible combinations of P/L and of key; we may suppose that we confine ourselves to P/L and key of appropriate length. If N is the number of possible keys (or messages) of this length, then the probability of the choice of key being K and the P/L being L is c_L/N, where c_L is the a priori probability of the P/L being L, since the probability of any key is $1/N$.

Now if we know the cipher to be C we may strike out as impossible any entries which do not combine to give C. The probabilities of the remaining entries are in

proportion to their original probabilities; let the factor of proportionality be b. Then the final list consists of all pairs K, L which combine to give C, each with probability bc_L/N. Now since there is just one K which will so combine with each L, the total probability of L is bqL/N, i.e., $P(C, L) = bq_L/N$. Now the total probability of all possible values of L is unity, which determines b to be N, i.e., $P(C, L) = c_L$ all C, L of the appropriate length.

Appendix B. A Property of Random Noise

It is proposed to prove that the voltage values at integer moments of a random noise limited to the frequency band 0–$\frac{1}{2}$, and having a uniform spectrum within this band, are independent, and that each one is distributed according to the normal error law. It is understood that we have selected a suitable time unit for the purpose of the band concerned.

If we are to avoid a detailed discussion of the nature of random noise we shall have to take certain of its properties for granted. I shall assume the following, which is proved in "Mathematical Analysis of Random Noise" (S. O. Rice B. S. T. J. Vol. 23, 1944).

Let $k(t)$ be a random noise defined in the time interval $-\frac{1}{2} - N$ to $\frac{1}{2} + N$. We may express it as a Fourier series in this interval:

$$k(t) = \sum_{t=1}^{\infty} x_{2t+1} \sin\frac{2\pi + t}{2N+1} + \sum_{t=1}^{\infty} x_{2t}\cos\frac{2\pi + t}{2N+1} + \frac{1}{2}x_0. \tag{B1}$$

Then the relative probabilities of the various possible random noises may be expressed by saying that the probability of obtaining a noise whose first $2N+1$ Fourier components lie in the $2N+1$ dimensional region D is

$$P(D) = \left(\frac{\gamma}{\sqrt{2\pi}}\right)^{2N+1} \int_{x_0} \dots \int_{x_{2N}} e^{-\frac{1}{2\gamma^2}\sum_{t=0}^{2N} x_t^2}\, dx_0 \dots dx_{2N}, \quad (x_0, \dots, x_{2N}) \text{ in } D. \tag{B2}$$

The constant γ determines the amplification of the noise.

The numbers $x_0, \dots, x_{2N}$ may be described as coordinates for the component of the noise in the frequency band up to half unit frequency. We shall now introduce new coordinates in this space, viz. the values $k(0), k(1), k(2), \dots, k(2N)$ of the function $k(t)$. If the coordinates $x_0, \dots, x_{2N}$ are regarded as rectangular Cartesian, then the coordinates $k(0), \dots k(2N)$ are also rectangular Cartesian, as follows from the identity

$$\sum_{s=0}^{2N} (k(s))^2 = \left(N = \frac{1}{2}\right) \sum_{t=0}^{2N} x_t^2,$$

which is valid if $x = 0$ for $r > 2N$ and is a simple consequence of the orthogonality relations of the trigonometric functions.

The assumption that the first $2N+1$ components are distributed according to (B1) and that the others are means that our noise has been first made periodic with period $2N+1$ and then passed through an ideal low-pass filter with a cut off

frequency of $\frac{1}{2}$. The effect of making the signal periodic becomes small for large N, i.e., when the interval is large. It follows from this that if we put $y_0 = k(0), \ldots$ $y_{21} = k(2N)$, then the relation between volume elements is $dx_0 \ldots dx_{2N} = (N + \frac{1}{2})^{-(N+\frac{1}{2})}\, dy_0 \ldots dy_{2N'}$ and therefore, that the Equation (B2) may be expressed in the form that the probability $q(D')$ of the new coordinates $y_0, \ldots, y_{2N}$ lying in the region D' is

$$q(D') = \left(\frac{\gamma}{\sqrt{2\pi}}\right)^{2N+1} \left(N+\frac{1}{2}\right)^{-\left(N+\frac{1}{2}\right)} \int_{y_0} \cdots \int_{y_{2N}} e^{-\frac{1}{2\gamma^2\left(N+\frac{1}{2}\right)} \sum_{s=0}^{2N} y_s^2} dy_0 \ldots dy_{2N} \qquad \text{(B3)}$$

$(y_0, \ldots, y_{2N})$ in D'.

In other words, the probability of the inequalities

$$y_0 \le k(0) \le y_0 + dy_0, \quad y_1 \le k(1) \le y_1 + dy_1, \ldots, y_{2N} \le k(2N) \le y_{2N} + dy_{2N}$$

being satisfied is

$$\left(\frac{dy_0}{\gamma\sqrt{2\pi\left(N+\frac{1}{2}\right)}} e^{-\frac{y_0^2}{2\gamma^2\left(N+\frac{1}{2}\right)}}\right)\left(\frac{dy_1}{\gamma\sqrt{2\pi\left(N+\frac{1}{2}\right)}} e^{-\frac{y_1^2}{2\gamma^2\left(N+\frac{1}{2}\right)}}\right) \cdots \left(\frac{dy_{2N}}{\gamma\sqrt{2\pi\left(N+\frac{1}{2}\right)}} e^{-\frac{y_{2N}^2}{2\gamma^2\left(N+\frac{1}{2}\right)}}\right).$$

Since this is a product of factors, each dependent on the appropriate variable, the values of the function $k(t)$ at the integer times are independent, and each one is distributed according to the normal error law with standard deviation $\gamma\sqrt{N+\frac{1}{2}}$.

In the above, we assumed a noise spectrum which was uniform up to half unit frequency and zero above. Actually, the above independence result will hold under more general conditions concerning the spectrum. These are added without proof.

Let the mean noise energy per unit bandwidth at frequency f be $P(f)$. Then the above independence result holds provided $\sum_{m=-\infty}^{\infty} P(f+m)$ is a constant. It is understood that $P(f)$ is defined for negative f as well as positive, the equation $P(-f) = P(f)$ holding.

Appendix C. The Bandwidth Theorem

We wish to determine the conditions under which a function which is limited by the conditions that it contains no frequencies above a certain cut-off can take given values at specified points at equal intervals. Our result is:-

Let c_n be a real number for all positive and negative integers, and let U denote the totality of functions which have no frequencies above f. Then

1) if $f > \frac{1}{2}$, there are an infinity of functions z in U taking the given values c_n, i.e., satisfying the equations $g(n) = c_n$ all n.
2) if $f = \frac{1}{2}$, there is one and only one function in U taking the given values.
3) if $f < \frac{1}{2}$, there are not, in general, any functions in U taking the given values; i.e., unless the sequence c_n satisfies certain special conditions, there is no such function.

4) the function whose existence is established in 2) is given by

$$g(t) = \sum_{t=-\infty}^{\infty} C_t \frac{\sin\pi(t-\frac{1}{2})}{\pi(t-\frac{1}{2})}.$$

In order to make the problem definite I will suppose that the functions 'g' concerned are all integrable square and that the series is convergent, so that Fourier integral theory will apply.

If $g(t)$ has only frequencies up to f, we can express it in the form

$$g(t) = \int_{-f}^{f} G(\omega) e^{2\pi i\omega t}\, d\omega.$$

Assuming now that $g(n) = c_n$ for all integers n, we shall have

$$c_n = \int_{-f}^{f} G(\omega) e^{2\pi i\omega n}\, d\omega.$$

If $f < \frac{1}{2}$, this may be expressed by saying that the numbers c_n are the Fourier coefficients of the function with period 1 which is equal to $G(\omega)$ in the interval $(-f, f)$ and is zero in the remainder of the interval $(-\frac{1}{2}, \frac{1}{2})$. This is a considerable restriction on the c_n and establishes 3). Now suppose that $g_1(t)$ and $g_2(t)$ are two functions both taking the given values c_n, and that $g(t) = g_1(t) - g_2(t)$, and suppose $f = \frac{1}{2}$; then

$$0 = g(n) = \int_{-\frac{1}{2}}^{\frac{1}{2}} G(\omega) e^{2\pi i\omega n}\, d\omega;$$

i.e., the Fourier coefficients of the function $G(\omega)$ expanded in the interval $(-\frac{1}{2}, \frac{1}{2})$ are all zero. The function itself is therefore everywhere zero (assuming it continuous, say) and $g(t)$ is therefore zero for all t; i.e., $g_1(t) = g_2(t)$. This means that if there is any function with the given values, then there is only one.

It is easily seen that $g(t)$ given under 4) takes the required values. Each term is also restricted to the required frequency band. Thus, we have established 2) and 4).

It remains to prove 1). That there is at least one such function follows from 2), for we are not obliged to use the whole band. It will suffice to show that we can find an infinity of functions which are zero at the integer points and are restricted to U. Any function of the form of a product of sin πt with a function which has no frequencies above $f - \frac{1}{2}$ has this property.

Appendix D. Departures from the Ideal Theory

1. Introduction

There are a number of respects in which the ideal theory described in § 3 is only approximately fulfilled. In this appendix we propose to look into the mathematical theory of the effects of these departures in order that we may know how much tolerance is permissible in connection with each. The effects of the departures are

mainly of two kinds. They may lower security, or they may deteriorate intelligibility. Each will have to be considered from both points of view.

Loss of intelligibility can be measured reasonably well by the magnitude of unwanted signal produced by the effect. That is to say that we regard the reconstituted speech as consisting of the original speech with a certain added signal, and the number of decibels by which the wanted signal is stronger than the unwanted is a measure of the goodness of the reconstituted speech. It is better, however, not to work in decibels but rather in terms of proportionate power. We may say that there is **k** unwanted signal if the power in the unwanted signal is a fraction **k**/100 of the power of the wanted signal. This method is preferable, since we can add up the percentages in the case of independent effects. This method of percentage of unwanted power (P.U.P.) is not, of course, applicable to the frequency and phase distortion in the reconstituted speech, but these forms of distortion are not our chief concern.

The theory of the magnitude of the various effects leading to loss of intelligibility will be investigated in some detail. For various reasons, however, it has been decided to give only a rather qualitative account of the questions of security.

The chief ways in which the actual apparatus may differ from the ideal are

a) Finite width of pulse modulator stage.
b) Non linearity of pulse modulator.
c) Imperfection of limiting of speech.
d) Imperfect filtering of speech.
e) Imperfect voltage distribution of key.
f) Nonrandom key.
g) Dependence of R.C. pulse amplitude on M.P. amplitude.
h) Dependence of R.C. pulse time on M.P. amplitude.
i) Dependence of R.C. pulse amplitude on previous R.C. pulses.
j) Dependence of R.C. pulse time on previous R.C. pulses.
k) Dependence of R.C. pulse critical tripping voltage on previous R.C. pulses.
l) Failure of the indicial response function g to satisfy the equations $g(n) = o(n + m_o)$ accurately.
m) Imperfection of the transmission system.
n) Differences between the key produced by the transmitting and receiving apparatus.
o) Failure of the output network to cut off at frequency $\frac{1}{2}$ in the receive condition.
p) Frequency distortion of the output network below frequency $\frac{1}{2}$ in the receive condition.
q) Difference in the time between R.C. pulse and M.P.
r) Fixed error in synchronisation.
s) Quickly varying error in synchronisation (Synch Dither).
t) Bias error on transmit.
u) Bias error on receive.
v) Incorrect setting of Cypher Vol. control.
w) Insufficient key or too much key.

We shall consider the effects of these on intelligibility. Normally, a very small unwanted signal will involve only a small loss of security. Hence in cases where we can show that the unwanted signal is very small we need not make a special investigation of loss of security.

2. Intelligibility Considerations

(a). Finite Width of M.P.

Suppose that the output voltage of the P.M. stage is $Q(x)$ for input x, that the form of unmodulated pulse is $p(t)$, and the modulating voltage $m(t)$; then by Taylor's theorem, we have for the output voltage

$$Q(p(t)+m(t)) = Q(p(t)+m(t)Q'(p(t)) + \frac{1}{2}(m(t))^2 Q''(p(t)) + \cdots$$

The first term in this series is periodic. So far as possible, it is suppressed in the output filter. The terms after the second represent a form of error discussed elsewhere. For the present we concentrate on the second term, $m(t)\ Q'\ (p(t))$. Here $Q'\ (p(t))$ represents a periodic pulse-like curve and may be expressed as a sum of separate pulses $Q'(p(t)) = \alpha \sum_{n=-\infty}^{\infty} \psi(t-n)$.

The function $\psi(t)$ is supposed to be zero except for quite small values of t and $\int \psi(t)dt = 1$. Now when the signal $\alpha\, m(t) \sum_{n=-\infty}^{\infty} \psi(t-n)$ has passed through the current filter it emerges as

$$\alpha \int_{-\infty}^{\infty} \sum_{n=-\infty}^{\infty} m(u)\psi(u-n)g(t-u)du = \alpha \sum_{n=-\infty}^{\infty} \int_{-\infty}^{\infty} m(u+n)\psi(n)g(t-n-u)du.$$

If we expand $m(u+n)\ g(t-n-u)$ in powers of u by Maclaurin's theorem, we obtain

$$\alpha \sum_{n=-\infty}^{\infty} \sum_{t=0}^{\infty} \frac{1}{\lfloor t} \left[\frac{d^t}{du^t}\{m(u+n)g(t-u-n)\}\right]_{u=0} \int_{-\infty}^{\infty} u^t \psi(u)\ du.$$

In this we may ignore the terms with $t \geq 3$, since $\int_{-\infty}^{\infty} u^t \psi(u)du$ will be very small. We may also omit the term with $t=1$ altogether. This simply means that we are taking our time origin at the centroid of a pulse. There then remains

$$\alpha \sum_{n=-\infty}^{\infty} \left[m(n)g(t-n) + \frac{1}{2}\sigma^2(m'(n)g(t-n) - 2m'(n)g'(t-n) + m(n)g'(t-n))\right].$$

where $\sigma^2 = \int_{-\infty}^{\infty} u^2\psi(u)du = (S.D.\ of\ pulse)^2$;

$$\begin{aligned} &-\alpha \sum_{n=-\infty}^{\infty} \left(m(n) + \frac{1}{2}\sigma^2 m''(n)\right)\left(g(t-n) + \frac{1}{2}\sigma^2 g''(t-n)\right) \\ &-\alpha\sigma^2 \sum_{n=-\infty}^{\infty} m'(n)g'(t-n) - \frac{\alpha G^4}{4} \sum_{n=-\infty}^{\infty} m''(n)g''(t-n) \\ &= \alpha \sum_{n=-\infty}^{\infty} m^*(n)g^*(t-n) - \alpha\sigma^2 \sum_{n=-\infty}^{\infty} m'(n)g'(t-n) \end{aligned}$$

where

$$\begin{aligned} m^*(t) &= m(t) + \frac{1}{2}\sigma^2 m''(t,) \\ g^*(t) &= g(t) + \frac{1}{2}\sigma^2 g''(t), \end{aligned}$$

and we have ignored the term in σ^4. Thus, the error consists in

(1) Slight frequency distortion of the modulation whereby $m(t)$ becomes replaced by $m^*(t)$.
(2) Slight modification of the output filter response whereby $g(t)$ becomes $g^*(t)$.
(3) The unwanted signal $-\alpha\sigma^2 \sum_{n=-\infty}^{\infty} m'(n)g'(t-n)$.

Of these, the effect of (1) may be ignored. Such a small frequency distortion on the speech is negligible. It applies equally to the transmit and receive keys, and there only remains the effect on the cipher in the receiving combiner. This last effect can be considered as modifying the transmitter indicial response, i.e., as being a further effect of form (2). The effect (2) may be allowed for in the design of the current filter. The effect (3) cannot be passed over so easily, and its magnitude must be estimated.

$$P.U.P. = \frac{\textit{Mean square unwanted signal}}{\textit{Mean square wanted signal}} = \sigma^4 \frac{(\textit{R.M.S. value of } \sum m'(n)g'(t-n))^2}{(\textit{R.M.S. value of } \sum m(n)g(t-n))}.$$

If we take the assumption that the modulation has uniform frequency spectrum up to frequency $\frac{1}{2}$ and zero above, and also that the spectrum associated with $g(t)$ has this same property, it may be shown that $P.U.P. = \frac{1}{5}\pi^4\sigma^4$. Assuming a square pulse of width d this becomes $P.U.P. = \frac{1}{720}\pi^4\alpha^4$. If we take $\alpha = 15\,\mu s = \frac{15}{250}$ we find the unwanted signal to be 57 dB down on the wanted signal.

(b). Non-Linearity of Pulse Modulator Stage

We now consider the P.M. stage as having an input of instantaneous values $k(n) - s(n)$ and giving an output of instantaneous values $\xi(k(n) - s(n))$. Strictly speaking, the ideal form of $\xi(x)$ is x, but for the purpose of the present discussion we consider $\gamma x + \delta$, with $\gamma = 1$ as ideal; the effect of the constant δ is merely to alter the amount of 4 kc/s in the output, and variations in γ may be compensated for by altering the Cypher Vol. control. Now let $\chi(u)\,du$ be the probability of a cypher value lying in the range $(u,\ u+du)$ and $\tau(u)\,du$ the probability of the combination of speech and key lying in this range. Then

$$P.U.P. = \frac{\int_{-\infty}^{\infty} \tau(u)(\xi(u) - \gamma(u) - \delta)^2 du}{\int_{-\infty}^{\infty} \chi(u)u^2 du}$$

Taking the ideal form, $\chi(u) = \frac{1}{2}\left(sgn\left(u - \frac{1}{2}\right) - sgn\left(u + \frac{1}{2}\right)\right)$, we have $\int_{-\infty}^{\infty} \chi(u)u^2 du = \frac{1}{12}$. We may put $\xi(u) - \gamma u - \delta = a + bu + cu^2 + \alpha u^3$ ignoring the higher powers. Further, we may take $a = 0$ (ignoring 4 kc/s) and $c = 0$ adjusting pulse amplitude, and the adjust b for minimum (cypher vol).

Assume $\tau(-u) = \tau(u)$,

$$P.U.P. = \min_b 12 \int_{-\infty}^{\infty} \tau(u)\left(bu + du^3\right)^2 du = 12\alpha^2\left(L_6 - \frac{L_4^2}{L_2}\right),$$

where $L_{2m} = \int_{-\infty}^{\infty} \tau(u)u^{2m}\,du$. Now the unwanted power is most serious when the speech is weak, and we may therefore put $\tau(u) = \chi(u)$, giving the P.U.P. eventually as $\frac{3}{700}d^2$. With $d = \frac{1}{10}$ this means the unwanted signal is 43 dB down on the cipher. The actual value of d is doubtful.

The above analysis does not take any account of the output filter, and therefore probably gives too large a value for P.U.P. due to the fact that the intermodulation products will largely be above 2 kc/s. Overestimate may be about 5 dB.

(c). Imperfect Limiting of Speech
The effect of this is drastic and has already been discussed in detail (page 8).

(d). Imperfect Filtering of Speech. (o) and (p) Imperfection of Receive Filter
We can see the effect of these without going into the complete ciphering process. We simply consider the effect of converting imperfectly filtered speech to pulses and back. We consider the speech signal $s(t) = \int_{-\infty}^{\infty} S(u)e^{2\pi iut}du$. We multiply this signal by a periodic pulse $\sum_{n=-\infty}^{\infty} C_n e^{2\pi int}du$ and get

$$\mathrm{S(t)} \sum_{-\infty}^{\infty} C_n e^{2\pi int} = \int_{-\infty}^{\infty} H(u)e^{2\pi iut}du$$

where $H(u) = \sum_{-\infty}^{\infty} S(u-n)C_n$; i.e., the frequency analysis of the modulated pulses is given by $H(u)$. After filtering, the frequency analysis becomes, $H(u)\ R(u)$ say, We may reasonably assume $S(u) = 0$ if $|u| \geq 1$ (in the ideal case, $S(u) = 0$ unless $|u| \leq \frac{1}{2}$) and likewise that $R(u) = 0$ unless $|u| < 1$. Then $H(u)\ R(u) = 0$, unless $|u| < 1$, in which case it is given by

$$H(u)R(u) = [C_0 S(u) + C_1 S(u-1) + C_{-1} S(u+1)]R(u),$$

the other terms in the infinite series vanishing. For narrow pulses we may put $C_0 = C_1 = C_{-1}$ (=1), say. Then, $H(u)R(u) = (S(u) = S(u-1) + S(u+1))R(u)$.

The first term represents speech which has undergone slight frequency distortion, and the other two represent speech inverted in the unit frequency (N.B., if $S(u-1)$ $R(u) \neq 0$, then $|u-1| + |u| = 1$, and if $S(u+1)\ R(\mathrm{u}) \neq 0$, then $|u-1| + |u| = 1$). In fact, we may describe the effect of these processes as being equivalent to adding speech, inverted in unit frequency (4 kc/s) and at the same level to the original speech, and then passing the whole through the receive phone filter. The P.U.P. may be calculated to be $2\int_{\frac{1}{2}}^{\infty} |R(u)|^2 du + 2\int_{\frac{1}{2}}^{\infty} |S(u)|^2 du$, but this is referred to the speech and not to the cipher, as we have done elsewhere. This fact makes a great difference, for not only is the speech weaker on the whole than the cipher, but the worst effects are when the speech is very weak. The unwanted power in this case also differs from most other cases in being limited to particular frequencies (when the speech is a vowel) and in being almost entirely in the neighborhood of frequency $\frac{1}{2}$ (2 kc/s).

(g). Dependence of R.C. Pulse Amplitude on M.P. Amplitude
We take it that the R.C. pulse amplitude is given by αx $(x < 0)$ $1 + \beta x$ $(x > 0)$, where α, β are small (and should be 0), and x is the modulation on the MP in the usual units. We may rewrite this in the form

$$\frac{\beta+\alpha}{2}x + \left(\frac{1}{2} + \frac{\beta-\alpha}{2}|\bar{x}|\right) + \frac{1}{2}sgn\ x + \frac{\beta-\alpha}{2}(|x| - |\bar{x}|).$$

The term $\frac{\beta+\alpha}{2}x$ may be absorbed in the M.P. and considered as modifying its characteristic as described in (b). The term $\frac{1}{2} + \frac{\beta-\alpha}{2}|\bar{x}|$ merely affects the 4 kc/s output. The wanted signal is $\frac{1}{2}\ sgn\ x$, and the unwanted signal, omitting the 4 kc/s, is

$$\frac{\beta-\alpha}{2}(|x| - |\bar{x}|),$$

which has a mean square value of $\frac{1}{4}|\beta-\alpha|^2\left(\bar{x}^2-|\bar{x}|^2\right)$, which with small speech modulation $\left(\bar{x}^2=\frac{1}{12}, |\bar{x}|=\frac{1}{4}\right)$, becomes $\frac{1}{192}|\beta-\alpha|^2$. Comparing with the mean square wanted signal (1/12), we get P.U.P. $\frac{1}{16}|\beta-\alpha|^2$. $|\beta-\alpha|$ is probably less than 1/25 so that the unwanted signal is at least 40 dB down.

(h). Dependence of R.C. Pulse Time on M.P. Amplitude

Let us suppose that the R.C. pulse time varies linearly with the size of the M.P., the RC pulse occurring at time εX after M.P. when the M.P. is of height $h+x$ $(x>o)$. With small ε, the unwanted signal at the output of the filter is $\varepsilon\frac{x+|x|}{2}g'(t)$. The component $\frac{1}{2}\varepsilon x g'(t)$ can be absorbed with $xg(t)$, the output from the M.P., and can be considered as altering $g(t)$ to $g(t+\frac{1}{2}\varepsilon)$. The component $\frac{1}{2}|x|\,g'(t)$ cannot be disposed of quite so easily but need only be considered at the sampling moments. It gives rise to a P.U.P. of $\frac{1}{4}\varepsilon^2\sum_{-\infty}^{\infty}|g'(n)|^2$, which is comparatively small owing to $g'(1)$ having been made small; probably $\sum_{n=-\infty}^{\infty}|g'(n)|^2=0.2$ and $\varepsilon=5\,\mu$sec is a conservative estimate with capacitative feed to R.C. This gives 47 dB.

(k). Dependence of R.C. Pulse Critical Tripping Voltage on Previous R.C. Pulses

This should have no effect on intelligibility provided that the range of variation of tripping voltage is not so large as to cause cracks.

(l). Imperfection of the Output Filter

(m). Imperfection of the Transmission System

We assume that the output filter and the transmission system introduce only frequency (& phase) distortion. They may be taken in combination, and with them may be taken any frequency distortion that occurs in the stages of the receiver before the pulse modulator: (see also (a)). The error may be described by saying that the values $g(0)$, $g(1)$, $g(2)$, $g(3)$,... of the indicial response at the integer points differ from 0, 1, 0, 0, ... Actually we need only consider two types of error in this indicial response. The first is an error in $g(2)$ or $g(3)$, and the second is an error due to using insufficiently large blocking condensors.

The P.U.P. for an error in $g(2)$ can be very easily estimated, for the unwanted signal evidently consists of the wanted signal attenuated by the factor $g(2)$ and delayed by one time unit, so that $P.U.P.=|g(2)|^2$. It is intended that the resistor R66 be adjusted at the factory to give $g(2)=0$, so that we may really be limited by $g(3)$ (to which similar considerations apply) and the accuracy and stability of the adjustment. Referring to the photographs in Figure 24, one might estimate the error from this source as 30 dB down, but this would be a mistake, as the photographs in question were taken at the output of the transmitter and do not take account of the delays in the receiver. The true value is probably 40 or 50 dB down. It should be remarked that it is also possible to get an error in $g(1)$ by altering Cypher Vol.; it may be advisable to have a slight error of this kind which may compensate errors from $g(2)$ or other causes at the frequencies to which the ear is sensitive. Changing the setting of Cypher Vol. certainly alters the character of the residual noise.

The errors due to insufficiently large blocking condensers may be treated without reference to the pulse form of the input to the filter stage, as the frequencies concerned are low in comparison with the pulse frequency. Now the effect of a resistance capacity coupling with time constant α^{-1} is to give an output of $\frac{p}{p+\alpha}e^{pt}$ for an input of e^{pt}. If there are a number of these sections at various stages, there will be a resultant distortion which may be described by the product $\prod_n\frac{p}{p+\alpha n}$, α_n^{-1} being the time constant

associated with the nth such section. Except for frequencies of the order of a few cycles per sec., we can approximate this by $\left(1+\frac{\alpha}{p}\right)^{-1}$ where $\alpha=\sum\alpha_n$. The unwanted signal with an input $e^{2\pi ift}$ *is* $\frac{\alpha}{\alpha+2\pi if}e^{2\pi ift}$ representing a P.U.P. at this frequency of $\frac{\alpha^2}{\alpha^2+4\pi^2f^2}$. The average of this over the frequencies up to $\frac{1}{2}$ gives the true P.U.P. and is $\frac{\alpha}{2}$. In the actual apparatus, α^{-1} is 5 ms, and the P.U.P. works out at 16 dB down. Actually, this very large unwanted signal gives very little trouble, owing to the poor response of the phones and the ear at these low frequencies. A correcting circuit was once used to deal with this unwanted signal, and was found very effective from the point of view of modulation observed on receive pulses, but its effect was negligible when listening.

(n). Differences Between Receive and Transmit Keys

This is liable to be the main source of residual noise. The P.U.P. is given approximately by

$$\frac{\text{power in the difference of keys}}{\text{power in the mean of keys}}$$

Strictly speaking, the P.U.P. should be calculated in terms of the key values at the times of the sampling pulses, but the above ratio is thought to be adequate. It is thought that it would be difficult to improve on 20 dB; consequently, the values of 40 dB and higher which prevail for the other forms of error may be considered entirely satisfactory.

(q). Difference in Time Between R.C. and M.P. Pulses

(j). Dependence of R.C. Pulse Time on Previous R.C. Pulses

(y). Difference in Shape Between M.P. and R.C. Pulses

(i). Dependence of R.C. Pulse Amplitude on Previous R.C. Pulses

To deal with (q), we consider the R.C. pulses as having values $\pm\frac{1}{2}$ instead of the values 0, 1; this merely affecting the 4 kc/s. The unwanted signal may be considered to consist of the actual R.C. pulse less an equal R.C. pulse at the time of the M.P. Denoting unit pulse at time 0 by the "Dirac function" $\delta(t)$[t], we may say that the unwanted signal going into the output filter is $-\frac{1}{2}\delta(t-\frac{1}{2}\varepsilon)+\frac{1}{2}\delta(t+\frac{1}{2}\varepsilon)$, where ε is the time difference of M.P. and R.C. pulse. Now $\delta(t)=\int_{-\infty}^{\infty}e^{2\pi ivt}dv$, and therefore,

$$-\frac{1}{2}\delta(t-\frac{1}{2}\varepsilon)+\frac{1}{2}\delta(t+\frac{1}{2}\varepsilon)=\delta(t)=\int_{-\infty}^{\infty}i\,\sin\pi\varepsilon v\;e^{2\pi ivt}\;dv.$$

The components below frequency $\frac{1}{2}$ of these are, respectively, $\int_{-\frac{1}{2}}^{\frac{1}{2}}e^{2\pi ivt}dv$ and $\int_{-\frac{1}{2}}^{\frac{1}{2}}i\,\sin\pi\varepsilon v\;e^{2\pi ivt}dv$. For small ε, the latter is approximately $\int_{-\frac{1}{2}}^{\frac{1}{2}}i\pi\varepsilon v\;e^{2\pi ivt}dv$. Then,

$$\frac{\text{Power in unwanted signal}}{\text{Power in signal from R.C.}}=\frac{\int_{-\frac{1}{2}}^{\frac{1}{2}}\pi^2\varepsilon^2v^2dv}{\int_{-\frac{1}{2}}^{\frac{1}{2}}\frac{1}{4}dv}=\frac{\pi^2\varepsilon^2}{3}.$$

But the power in the R.C. is three times the cipher signal; hence, $P.U.P.=\pi^2\varepsilon^2$. Probably ε is about 1 μs so that the unwanted signal is 38 dB down.

As regards differences in shape, we will only take account of differences in standard deviation of pulse, and will assume the pulses to be of Gaussian form.

One pulse we will assume of form $\frac{1}{2}\frac{1}{\sqrt{2\pi}\sigma_1}e^{-\frac{1}{2}\frac{t^2}{\sigma_1^2}}$ and the other $\frac{1}{2}\frac{1}{\sqrt{2\pi}\sigma_2}e^{-\frac{1}{2}\frac{t^2}{\sigma_2^2}}$. The difference, in Fourier integral form is

$$\frac{1}{2}\int_{-\infty}^{\infty}\left(e^{-2\pi^2\sigma_1^2\nu^2}-e^{2\pi^2\sigma_2^2\nu^2}\right)e^{2\pi i\nu t}d\nu,$$

$=\delta(t)$ is the limiting case, as $k\to\infty$ of a function, which is 0 for $T>\frac{1}{2}k$ and is k otherwise.

Assuming σ_1, σ_2 small and taking the component below frequency $\frac{1}{2}$, we get $\pi^2\left(\sigma_2^2-\sigma_1^2\right)\int_{-\frac{1}{2}}^{\frac{1}{2}}\nu^2e^{2\pi i\nu t}d\nu$, as before, P.U.P. $3\pi^4\left(\sigma_2^2-\sigma_1^2\right)^2\frac{\int_{-\frac{1}{2}}^{\frac{1}{2}}\nu^4d\nu}{\int_{-\frac{1}{2}}^{\frac{1}{2}}d\nu}=\frac{3\pi^4}{20}\left(\sigma_2^2-\sigma_1^2\right)^2$.

Typically, we might have $\sigma_1=17\,\mu s$ and the unwanted signal is 48 dB down.

It must be remembered that σ_1, σ_2 are here not the actual standard deviations of the pulses but of the pulses as modified by C29. They are best measured at the junction R56-R58 with C33 open circuited.

The error due to the dependence of R.C. pulse time on previous R.C. pulses is no greater than an error due to a fixed time error of similar magnitude. Actually, this error is negligible. Similar considerations apply to dependence of the size of the R.C. pulse on previous R.C. pulses.

(r). Fixed Error in Synchronisation

(s). Synch Dither

The effect of a fixed error in synchronisation is to replace $g(t)$ by $g(t+\varepsilon)$, where ε is the time error. It will be seen that it may be considered on the same lines as an error in the output filter, and also that an error in $g(2)$ in the output filter may be corrected by a compensating Synch. error. The small value of $g'(1)$ reduces the alteration in $g(1)$; alterations in $g(1)$ can of course also be corrected with Cypher Vol.

A rough estimate of the P.U.P. for an error of ε is given by $\varepsilon^2\sum_{n=-\infty}^{\infty}|g'(n)|^2$, which is probably about $0.2\varepsilon^2$. For an error of 5 μs, this is 41 dB down. Thus if errors as large as 10 μs occur, this may be the largest unwanted signal apart from that due to unequal keys.

Synch dither will produce trouble of the same kind as fixed synch error, and there will also be unwanted signals at the dither frequencies. Although this unwanted signal may have appreciable power, it can be ignored in practice as the frequencies are so low.

(t). Bias Error on Transmit

(u). Bias Error on Receive

The effect of bias error on transmit is more serious for security than intelligibility. It should have no effect on intelligibility which cannot be corrected with the receive bias. An error in receive bias produces loud rifle like cracks.

(v). Incorrect Setting of Cypher Vol.

(w). Incorrect Setting of Key Vol.

Assuming there are no other sources of error, the effect of an incorrect setting of either of these controls will be to bring to the phones an amount of Cypher or Key corresponding to the error in setting; e.g., if the Key Vol. is set so as to give

10% too much key there will be unwanted key in the phones 20 dB below the level of cypher (or key) at the phones (as measured, e.g., with receiver on "Clear"). Actually there will, of course, always be the other forms of error. It may be as well at this point to remember that we have been making the assumption throughout that the various unwanted signals are quite independent and, therefore, that we can add their powers. This assumption is fairly good on the whole but must not be taken too literally. It is partly due to the failure of this principle that the quality of residual noise changes as we alter the Key Vol. and Cypher Vol. controls.

3. Security Considerations

The most serious cause of insecurity is likely to be a non-random key, and this will take different forms according to the design of key unit used. With the present key unit, the greatest danger probably arises from the possibility of applying a Fourier analysis to very long stretches of key. Owing to the modulator, it would be necessary to use several seconds of key at a time, with several thousands of pulses, and the work would have to be repeated for each transmission (e.g., 30 secs. of speech); even then, it is probable that the speech masks the key to such an extent as to make the Fourier analysis impossible.

There are also some slight possibilities of working on other weaknesses than those of the key, but, owing to the considerations in § 1, these weaknesses are very much less in this system than in others using a key. It may, however, be worthwhile to mention what weaknesses there could be.

Imperfect voltage distribution of key (e) may, in extreme cases, enable the voltage distribution of speech to be inferred to some small extent; this might result in its being possible to distinguish whether a vowel or a consonant was being spoken, and this again might help a little with Fourier analysis of key. Bias error on transmit (t) has a similar effect, but the automatic bias renders this negligible. Imperfect limiting of speech (d) also has the effect, but its effect on intelligibility is so drastic that we need not fear much transmission under such circumstances. The effect of insufficient key (x) is drastic, and in extreme cases enables the scramble to be "listened through." It is better to have too much key. The chief remaining danger is the possibility that it may be possible, by some means, to distinguish whether there has been an remainder calculation pulse at a particular time or not. This would have to be done by very critical examination of the detailed waveforms at the times of the sampling pulses and the remainder calculation pulses. Since very little signal is transmitted at frequencies above 4 kc/s, this does not seem to be a practical possibility.