Dec. 21, 1965 M. R. SCHROEDER 3,225,142

PRIVACY SYSTEM

Filed Dec. 18, 1961 3 Sheets-Sheet 1

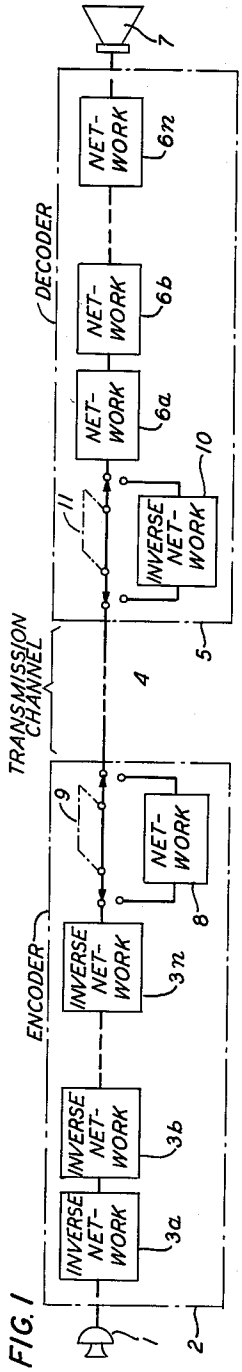


FIG. 1

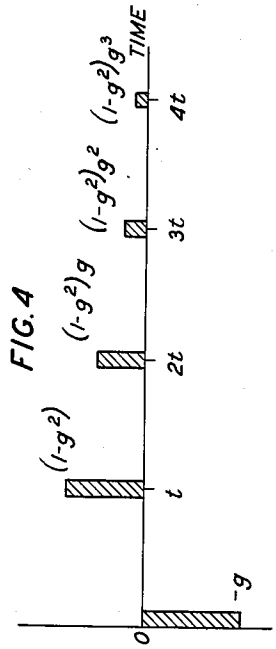


FIG. 4

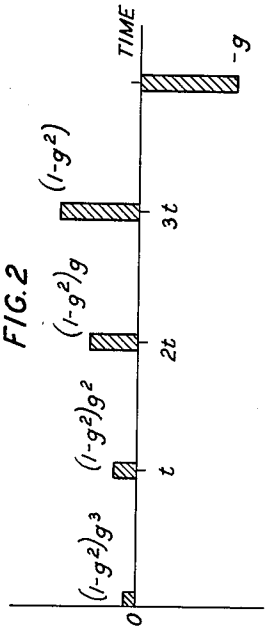


FIG. 2

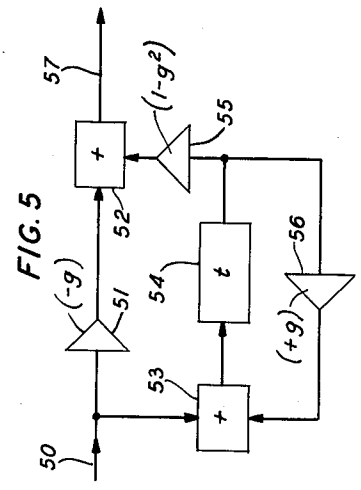


FIG. 5

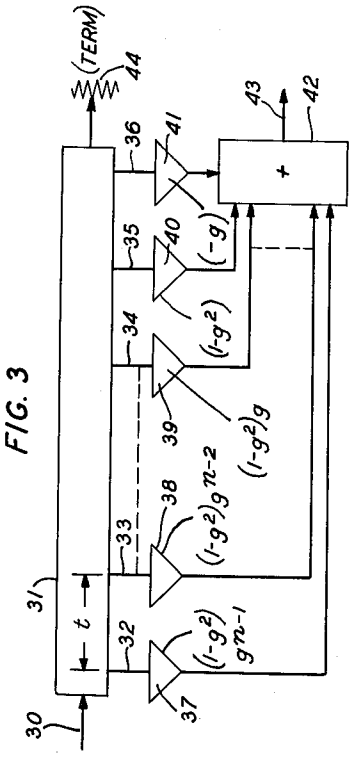


FIG. 3

INVENTOR
M. R. SCHROEDER
BY G. E. Hirsch Jr.
ATTORNEY

Dec. 21, 1965 M. R. SCHROEDER 3,225,142

PRIVACY SYSTEM

Filed Dec. 18, 1961 3 Sheets-Sheet 2

FIG. 6

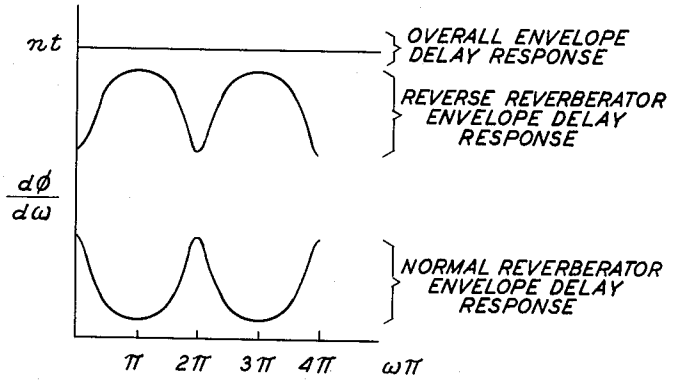
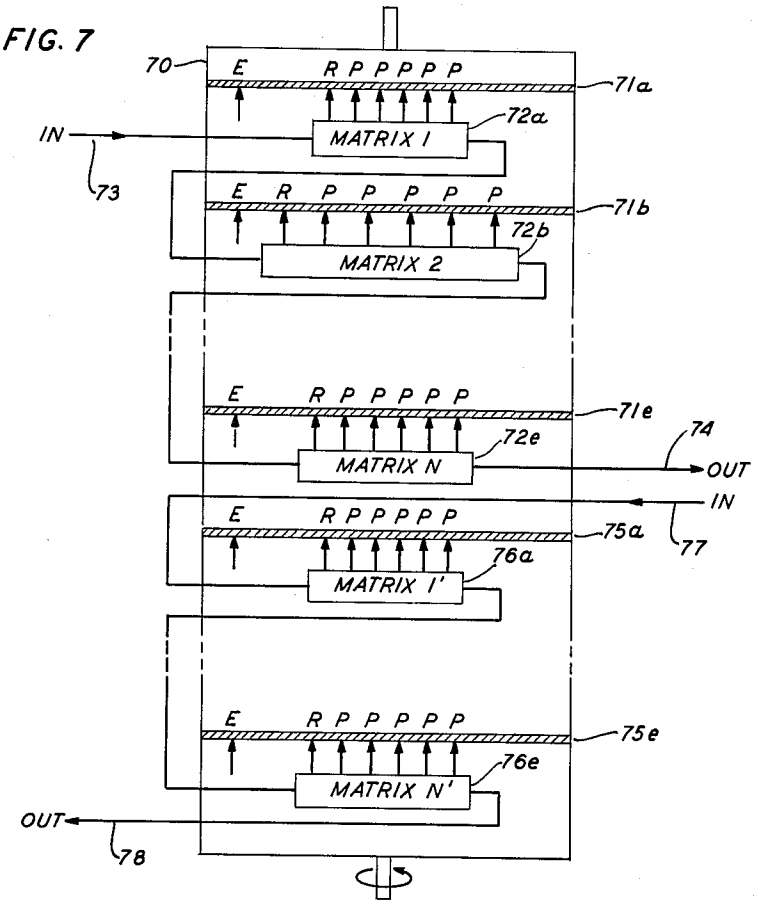


FIG. 7



INVENTOR
M. R. SCHROEDER
BY G. E. Hirsch Jr.
ATTORNEY

Dec. 21, 1965 M. R. SCHROEDER 3,225,142

PRIVACY SYSTEM

Filed Dec. 18, 1961 3 Sheets-Sheet 3

FIG. 8

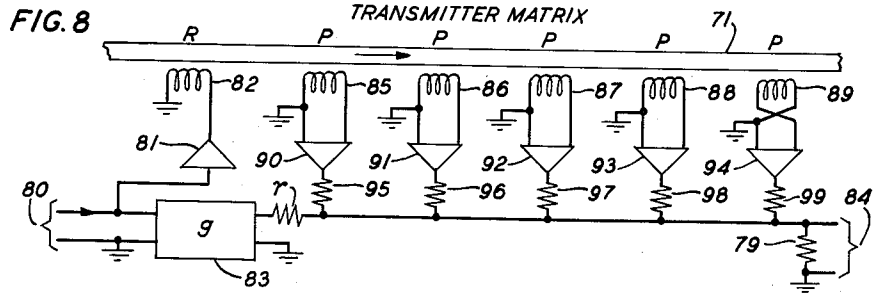


FIG. 9

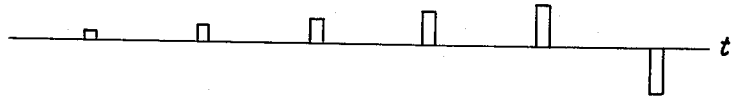


FIG. 10

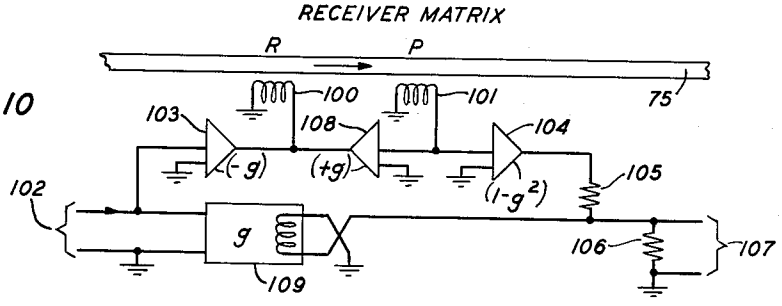


FIG. 11

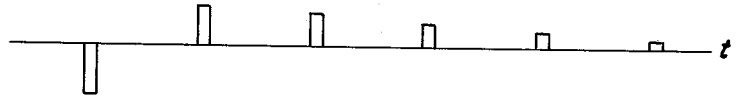


FIG. 12

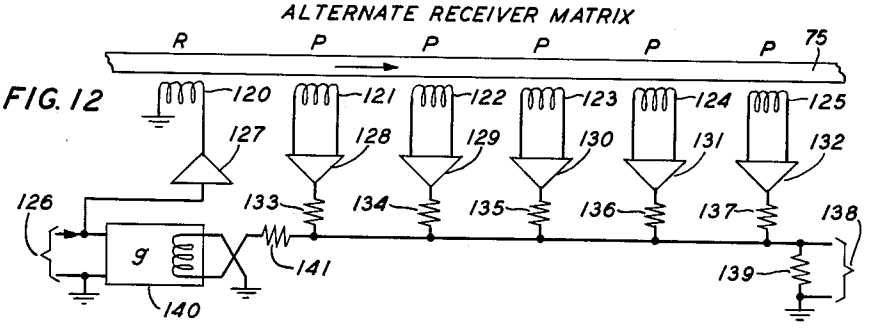
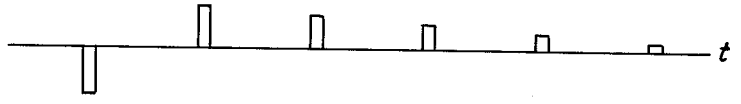


FIG. 13



INVENTOR
M. R. SCHROEDER
BY G. E. Hirsch Jr.
ATTORNEY

United States Patent Office 3,225,142 Patented Dec. 21, 1965

3,225,142

PRIVACY SYSTEM

Manfred R. Schroeder, Gillette, N.J., assignor to Bell Telephone Laboratories, Incorporated, New York, N.Y., a corporation of New York

Filed Dec. 18, 1961, Ser. No. 159,885
12 Claims. (Cl. 179—1.5)

This invention relates to systems and methods of transmission with privacy. It is applicable to wire or radio transmission and to the sending of speech messages, telegraph signals, or any other type of signals which may be transmitted from point to point by electrical means.

A general object of the invention is to increase the difficulty of unauthorized reception of a signal, message, or wave being transmitted.

A related object is to facilitate alteration of a secret signaling code with a minimum of alterations to apparatus components.

Analog communication systems have been devised in which electric signals corresponding to speech or other signals to be privately transmitted have been scrambled, garbled, or otherwise rendered more or less unintelligible in various ways. Their frequency components have been inverted with respect to a selected nominal frequency; they have been broken up into short segments which are then transmitted in alternation with corresponding short segments of another message; they have been recorded, inverted with respect to time (picked up backward) and transmitted so inverted; their transmission rate has been widely varied at a fairly high rate; and many other devices have been employed to make the relation between the electric signal as transmitted and the original message to be transmitted unobvious and therefore undecipherable. Such systems are characterized, in the main, by a perturbation or other masking effect which follows a definite and prescribed pattern, either recurring periodically in time or involving a definite numerical relation between the component frequencies of the plain message and those of the ciphered message. In general, this pattern is separate and distinct from the message to be transmitted and is unrelated to the peculiarities of the particular message, being controlled entirely by means external to portions of the apparatus or circuit which carry the message signals themselves.

In contrast to such systems, in accordance with the present invention, a correlated masking signal is utilized to transform a normal message signal into a "scrambled" signal; i.e., a signal whose characteristics differ widely from those of the plain message so that, to an unauthorized recipient, the entire message is meaningless. The invention thus provides means and methods for enciphering a message at a transmitter station and correspondingly for deciphering it at a receiver station.

Features of the present invention are that the encoded signal is produced by a process of linear filtering so that the resultant scrambled signal is amenable to analog transmission; that decoding requires only the use of a linear filter whose several parameters correspond to those of the encoder filter; that autocorrelation or power spectrum analysis of the transmitted signal will not reveal the filter parameters because of their all-pass characteristics; that linear distortion of the transmission medium does not interfere with the unscrambling process (sufficiently frequent nonlinear distortions are converted into a continuous background noise); and that frustrated decoding further scrambles the message.

Briefly stated, the invention turns to account a number of properties of message signals that affect their subjective intelligibility. It has long been known that reverberation impairs the intelligibility of message signals, especially

speech signals. Thus, it is more difficult to understand speech uttered in a highly reverberant atmosphere than that uttered in a sound studio. More importantly, it has been found that a considerable number of spaced echoes of gradually increasing amplitudes preceding a signal reduces speech intelligibility very considerably. Spaced echoes of increasing amplitudes preceding a signal may be viewed as a mirror image, on the time scale, of spaced echoes of diminishing amplitudes following a signal. The latter echoes together are generally referred to as reverberation signals, or simply "reverberation." Thus, echoes preceding a signal may conveniently be termed "reverse reverberation signals" or simply "reverse reverberation." Since time for such reverse reverberation signals is measured prior to the actual time of occurrence of the original signal, it is additionally convenient to refer to the times of occurrence of the reverse echoes in negative time. On an absolute scale, the negative times assume positive values somewhat less than those of the original signal and its normal echoes. Experiments indicate that reverse reverberation with a "negative" reverberation time in excess of two seconds renders speech virtually unintelligible. Since reverberation can be artificially produced by relatively simple apparatus involving linear filtering, it is thus entirely feasible to utilize linear filtering to make ordinary speech unintelligible.

It is in accordance with the present invention to mask or scramble a signal by passing it through a linear filter at a transmitter station in order to add reverse (time-inverted) reverberation to the signal. With a sufficient number of pre-echoes of the proper amplitude and polarity, the resulting signal, for all practical purposes, is unintelligible to unauthorized receivers. At a licensed receiver station, scrambled signals are passed through a linear filter whose transmission function is adjusted in accordance with a predetermined code to be the exact, or nearly the exact, inverse of the transmission function of the transmitter station filter. As a result, the pre-echoes are effectively removed to leave a delayed replica of the original signal.

In applying linear filtering to the scrambling and unscrambling of speech, a number of conditions must be fulfilled to insure privacy before decoding and high intelligibility after authorized decoding.

(1) Intelligibility must be near zero even for listeners trained with this particular type of filtering.

(2) The filters must have approximate inverses.

(3) The filtering process must be complex enough that privacy is assured over a considerable time interval even for expert cryptanalysts.

(4) The filtering process must have approximately an all-pass characteristic, both to avoid an increase in channel noise brought about by the inverse filtering operation and better to camouflage the parameters of the filter.

(5) The ciphering relation must be easily alterable at will.

All five conditions are met by apparatus of the present invention. In particular, an all-pass reverberation network of the type described in a copending application of B. F. Logan and M. R. Schroeder, Serial No. 59,273, filed September 29, 1960, now Patent No. 3,110,771, granted November 12, 1963, has a sufficiently satisfactory inverse so that the necessary coding and decoding operations may be attained by use of them. Although it is, of course, desirable that transmission be carried on instantaneously, the total delay of a sufficiently good scrambling all-pass reverberation network in tandem with its inverse is on the order of one second so that the entire coding-decoding process necessarily causes a delay of the reconstructed message by this amount. The delay can be avoided by employing fil-

ter networks with exact inverses of one another, for example, comb filters or the like, but it has been found that the inherent low sensitivity to channel noise of the all-pass network configurations more than compensates for the slight transmission delay involved in their use. Moreover, for satisfactory unscrambling, both networks must have an essentially flat frequency response. The all-pass reverberation networks employed in the practice of the invention are characterized by a flat frequency response; i.e., constant attenuation across the band, high echo density, and an aperiodic echo response.

The invention will be fully apprehended from the following detailed description of an illustrative embodiment thereof taken in connection with the appended drawings, in which:

FIG. 1 is a block schematic drawing of a transmission system employing the privacy features of the present invention;

FIG. 2 shows the impulse response of an (approximate) all-pass network arranged to produce reverse reverberation in accordance with the invention;

FIG. 3 shows in block schematic form an all-pass network with an inverse reverberation characteristic similar to that illustrated in FIG. 2;

FIG. 4 shows the impulse response of an (approximate) all-pass network arranged to produce normal reverberation of a signal;

FIG. 5 is an all-pass network with a normal reverberation characteristic similar to that illustrated in FIG. 4;

FIG. 6 illustrates the normal and reverse reverberator envelope delay responses and the manner by which they add algebraically to yield a constant envelope delay;

FIG. 7 shows a magnetic delay drum employing a plurality of individual magnetic bands, a number of the magnetic heads associated with the several bands and matrices connected to implement the all-pass networks employed at the encoder and decoder, respectively, of a transmission system constructed in accordance with the present invention;

FIG. 8 is a detailed schematic drawing of a transmission matrix for generating a reverse reverberation characteristic;

FIG. 9 illustrates the impulse response of the circuit of FIG. 8;

FIG. 10 is a schematic diagram of a receiver matrix used for securing a normal reverberation characteristic;

FIG. 11 illustrates the impulse response of the circuit of FIG. 10;

FIG. 12 is an alternative receiver matrix for securing a normal reverberation characteristic suitable for use in the practice of the invention; and

FIG. 13 illustrates the impulse response of the circuit of FIG. 12.

The functions and operations of the apparatus to be described are revealed in the block schematic diagram of FIG. 1 wherein a wave, originating for example in a speech source such as a microphone 1, is applied to an encoder 2. The wave is scrambled in the encoder so that its apparent significance is destroyed. Scrambling of the wave is attained by subjecting it to reverse or time-inverted reverberation in which echoes of the wave precede the direct wave. Reverse reverberation is obtained by so selecting the parameters of a linear filter that the impulse response of a normal all-pass reverberator is inverted in time. To increase the degree of privacy even further, it is preferable to employ several all-pass networks connected in series, represented by networks 3*a*, 3*b*, . . . 3*n* in encoder 2, each with different parameters. Scrambled speech is then transmitted via channel 4, which may be either wire or radio and may employ the services of wire or radio circuit terminal equipment of any desired construction, to decoder 5 at a licensed receiver station. Decoder 5 is equipped with a series of networks 6*a*, 6*b*, . . . 6*n* selected according to a private schedule to cancel the inverse reverberation and to reconstitute the clear message wave which in turn is supplied to a reproducer 7.

For an authorized listener to understand the message, an equal number of reverberator networks 6 must be used in which the several parameters closely match the corresponding parameters of the private schedule momentarily agreed upon between the sender and the receiver. As a further hinderance to an unauthorized listener who is accomplished at listening and understanding reverse speech (he could obtain reverse speech with normal reverberation by recording signals appearing on channel 4 and playing the tape backwards) normal reverberation may be added to the message wave. For this purpose an all-pass reverberation network 8 may be connected in series with the inverse networks 3 of encoder 2 by means of switch 9. The parameters of network 8 are suitably selected so that they do not interfere with, i.e., aid in decoding, the scrambled signals from filters 3. At the decoder station 5 an inverse network 10 is connected in series with reverberation networks 6 by means of switch 11 to remove normal reverberation. This refinement, of course, is not necessary since intelligibility of decoded speech is not materially reduced by the presence of a nominal amount of reverberation.

Before considering the structure and operational details of the filter networks employed in coding and decoding a message signal, it is believed helpful to consider briefly the characteristics of reverberant and reverse reverberant speech. This may best be done through a consideration of the impulse response of the all-pass networks employed in the networks of the sort described in the aforementioned Logan-Schroeder application and shown by way of example in FIG. 5. It has the impulse response shown in FIG. 4. The impulse response may be written

$$F(z)=-g+(1-g^2)z+(1-g^2)gz^2 + \ldots +(1-g^2)g^{n-1}z^n \quad (1)$$

where $z=e^{-j\omega t}$ in the delay operation for a delay of t. Since this response characterizes an all-pass network, its exact inverse will have an impulse response which is the same as (1), but which is reversed in time; i.e., is a mirror image of the normal response reflected about zero time. This requires negative delay. It is not, therefore, physically possible to build a network which will give the exact reversed impulse response, but the inverse may be closely approximated by reflecting the response in time around zero and shifting the zero point backward in time by delaying the entire operation by a selected delay nt. The negative delays then become positive and realizable (at least n of them; delays greater than nt are still negative but may be discarded). This results in a truncated impulse response for the reverse reverberator which may be expressed as follows:

$$F'(z)=(1-g^2)g^{n-1}+(1-g^2)g^{n-2}z + \ldots +(1-g^2)z^{n-1}-gz^n \quad (2)$$

The product of F(z) and F'(z), the response of the entire coding and decoding process, is (after some transformations)

$$F(z)\cdot F'(z)=-\frac{(1-g^2)g^n}{1-gz}+z^n \quad (3)$$

The quotient on the right-hand side of the equation indicates an exponentially decaying "pre-echo," which can be made as small as desired by increasing n. The term z^n represents the desired, but delayed, signal. It has been found that this procedure results in a minimum R.M.S. error approximation to a pure delay for the delay allowed. The inverted and truncated impulse response for $n=4$ is shown in FIG. 2.

An impulse response of this sort can be realized by using a transversal filter whose taps are spaced at t intervals and whose coefficients are selected in accordance

with the Equation 2. A suitable inverse network is shown in block schematic form in FIG. 3. Message waves applied to terminal **30** are directed through a delay line **31** which has spaced along its length a series of taps **32**, **33** . . . **34**, **35**, and **36**. To produce the impulse response shown in FIG. 2, successive pulses are evenly spaced apart from one another with a delay t between pulses, i.e., the taps on delay line **31** are evenly spaced at t intervals. It is to be understood, however, that it is in accordance with the invention to alter the spacing between the several taps, i.e., adjust, the interval t, in accordance with the selected private schedule. Energy from each of the taps is adjusted in amplitude by a series of amplifiers **37**, **38** . . . **39**, **40**, and **41** and summed in an adder network **42**. The several amplifiers are adjusted to provide the appropriate amplitude and polarity for the corresponding impulse in the response diagram of FIG. 2. Thus, amplifier **37** has a gain of $(1-g^2)g^{n-1}$, amplifier **38** has a gain of $(1-g^2)g^{n-2}$ and so on through amplifier **41** which has a gain of $(-g)$. It is evident of course that the signal provided by amplifier **41** is delayed by the total delay period nt of line **31**.

A suitable all-pass reverberation network which produces an impulse response, shown in FIG. 4, which is the inverse of that shown in FIG. 2 and is thus suitable for use in the decoder of the apparatus of FIG. 1, may employ a transversal network similar in many respects to that shown in FIG. 3. However, it is entirely satisfactory to use an all-pass network of the type described in the aforementioned Logan-Schroeder application. Such a network is shown in FIG. 5. Signals applied at terminal **50** are passed by way of amplifier **51** whose gain is $(-g)$ to an adder **52** and by a second path directly to adder **53**. Signals from adder **53** are transferred by way of delay line **54** with a delay interval of t seconds, to adder **52**, by way of an amplifier **55** whose gain is adjusted to $(1-g^2)$, and are returned to adder **53** by way of amplifier **56** whose gain is adjusted to $(+g)$. The gain and polarity of the several impulses in the response characteristic may be adjusted as required by the code schedule by altering the delay interval of element **54** and the gain (polarity) of amplifier **56**. Details of operation of the circuit are more fully discussed in the aforementioned Logan-Schroeder application. In short, signals developed at output terminal **57** have the characteristic shown in FIG. 4 and represent a normally reverberated signal. With a proper selection of parameters, the impulse response of the network may be made to have substantially the inverse characteristic of the network of FIG. 3.

For reverberation time $T=2$ seconds, and a loop gain of $1/\sqrt{2}$, the loop delay t must be 0.1 second. Thus, for $n=10$, the total delay for scrambling and unscrambling is approximately one second.

In practice, it is preferable to use several all-pass sections connected in series to increase the difficulty of unscrambling for an unlicensed recipient. Here the minimum R.M.S. error inverse is again a filter whose impulse response is that of a forward reverberator reversed in time, delayed, and truncated for negative times. The result is, in general, a very complex impulse response. It is therefore more convenient to use as an approximate total inverse, the series connection of the approximate inverses of the individual all-pass sections. Individual inverting of the several sections results in echo powers of the over-all response which apparently are only slightly greater than the true minimum R.M.S. error inversion of the multisection filter.

Thus, it has been found to be entirely satisfactory to connect five or more of the reverse reverberation network of FIG. 3 in tandem at the encoder **2** and to employ an equal number of normal reverberation networks of the sort shown in FIG. 5 connected in tandem at the decoder **5**. With such an arrangement, signals transferred by transmission channel **4** are totally unintelligible to unauthorized recipients, and yet, after decoding by a licensed receiver, are delayed by no more than five seconds. While a delay of this sort somewhat impairs the spontaneous character of normal speech, the privacy afforded transmitted signals in most cases more than justifies the delay. In a tandem arrangement, it is customary to adjust the delay intervals t for each reverberator in accordance with the agreed upon schedule. Thus, the several delays of each reverberator and corresponding reverse reverberator are the same but, of course, the delays are different for each pair of corresponding units.

Unscrambling of the message is thus attained merely by using an equal number of normal reverberators at the decoder station, each with parameters closely matched to the corresponding parameters of the encoder filters. Anyone wishing to intercept the message must also use an equal number of normal reverberators, and must closely match the parameters of the scrambling filters. It is important therefore to know how closely the parameters must be matched for marginal intelligibility. Essentially, two parameters must be matched for unscrambling, namely, the gain g and the delay t.

The effect of mismatching the gain and delay of a filter network pair cannot be determined merely by considering amplitude variations since the networks are (ideally) all-pass. However, the phase characteristic shows a periodicity and thus is helpful. From a summation of a selected number of terms of Equation 1, taken as an infinite geometric series, one may obtain expressions for phase lag and for the derivative of phase with respect to ω. The latter expression denotes envelope delay. The result of these algebraic steps yields an expression for the envelope delay response of the normal reverberator (impulse response of FIG. 4) as follows:

$$\frac{d\varphi(\omega)}{d\omega}=\frac{1-g^2}{1+g^2-2g\cos\omega t}t \tag{4}$$

This expression exhibits a comb like frequency response as shown in the lower portion of FIG. 6. The envelope delay response of the inverted reverberator, shown in the middle portion of FIG. 6, has similar characteristics; it is inverted as compared with the normal reverberator envelope delay characteristic and is displaced by a constant nt from it. Thus, when the gains and delays of the network pair are matched, the envelope-delay characteristics add to give the constant delay nt as shown at the top of FIG. 6.

It is apparent that the effect of a small change in t will cause the peaks of the envelope delay to shift in frequency. The frequencies at which the envelope delay exhibits peaks may be written

$$\omega_n=\frac{2\pi n}{t}n=0,\ 1,\ 2\ \ldots \tag{5}$$

Then, for a small change in t, viz: Δt,

$$\omega_n+\Delta\omega_n=\frac{2\pi n}{t+\Delta t} \tag{6}$$

Solving 6 for $\Delta\omega_n$ and making the assumption that Δt is small compared to t, it follows that:

$$\Delta\omega_n=-\frac{\Delta t}{t}\frac{2\pi n}{t}=-\frac{\Delta t}{t}\omega_n \tag{7}$$

For small values of n (corresponding to very low frequencies) the shift of peaks, $\Delta\omega_n$, will be small and the effect of mismatching will be small. The worst effect, namely, additional scrambling, will occur at those frequencies for which

$$\Delta\omega_n=\pm\frac{\pi}{t}$$

Using this relation in 7, the values of frequency f_p for which this occurs are:

$$f_p=\frac{p}{2\Delta t},\ p=1, 2 \ldots \quad (8)$$

It is expected that the scrambling will be twice as much at these frequencies, inasmuch as the peaks in envelope delay curves interleave instead of canceling. Since most of the signal power in a speech signal is contained in frequencies below 5000 c.p.s., matching to within $\Delta t=0.1$ ms. should be sufficient for unscrambling (the signal may, if desired, be band-limited to 3000 c.p.s.). Similarly, for $\Delta t=1$ ms., the first double scrambling occurs at 500 c.p.s. and the message will not be unscrambled since a 500 c.p.s. band is narrower than required for speech intelligibility.

It is difficult to set exact limits on how closely the delay interval t must be matched because intelligibility depends on the message ensemble, the rate of speech production, and other factors. Furthermore, when there are multiple sections to be matched, there are many combinations of mismatched conditions that can occur. Consider, for example, a case in which five scrambling network sections are connected in series at the encoder, and in which an equal number of unscrambling networks are serially connected at the decoder. It has been determined that, for matched gains, if four out of the five delays are matched, and if $\Delta t=0.2$ ms. for the fifth section, some messages over the system may be intelligible. Experiments indicate, however, that if each of the five unscrambling networks are mismatched by approximately 0.2 ms., it is quite unlikely that any message will be intelligible. From these considerations, it is conservatively estimated that the delays must be matched to better than 0.2 ms. if the message is to be intercepted.

Changing the gain of the networks at either of the two stations has the effect of changing the height of the peaks of the envelope delay curve. However, tests reveal that substantial mismatching in the magnitudes of the network coefficients (g) has little effect in maintaining secrecy, all other parameters being properly matched. However, the same tests confirm mathematical findings that the polarity (sign) of the coefficients must be equal at the two stations. If the coefficient polarities are not equal, the decoded speech becomes even less intelligible than the scrambled speech, i.e., improper decoding further encodes the signal. As a general rule then, only the algebraic sign of the coefficients g are significant in the private schedule.

To unscramble the message, an eavesdropper thus must have the following information, assuming of course that he is familiar with the encoding method:

(1) The number of network sections in the encoder.

(2) A rough idea of the gain of each network section.

(3)The algebraic sign of each impulse in the impulse response for each network in the encoder network.

(4) The delay of each network section to better than 0.2 millisecond to have marginal intelligibility.

It will be appreciated that if there are as many as five network sections in the encoder, each employing t's on the order of 100 ms., it is virtually impossible for one to construct a suitable decoder by a trial and error method. Nor do autocorrelation or power spectrum analyses of the transmitted signal help in ascertaining the several parameters.

From the noise and distortion standpoint, an important feature of the privacy transmission system of the present invention resides in the remarkable insensitivity of the system to the effects of linear and nonlinear distortions arising in the terminal equipment, in the transmission channel, or in both. Since linear filters are used both at the encoder and at the decoder, linear distortion of the transmission medium does not interfere with the decoding process. Further, it has been demonstrated that nonlinear distortion, in many cases, has a subjectively smaller effect on signals scrambled by the apparatus of the invention than it does on normal non-private transmissions. In the encoder, the amplitudes of the various hamonics are not affected, but their phases are altered so that a message is "spread-out" in time. The unscrambling networks of the decoder then mix the phases of the scrambled message in precisely the right manner to reconstruct the original message. This also involves spreading out in time. Any nonlinear distortion, such as clipping, applied to the scrambled speech will likewise be spread out when unscrambled and thus will not be associated with any part of the original speech. If this distortion occurs sufficiently often, it is heard as a continuous background noise which, subjectively, may be less annoying than distortion. In essence, nonlinear distortion applied to a scrambed signal is not correlated with the original message after scrambling. Further, frequency shifts encountered during the course of signal-sideband transmission over a carrier system are not harmful. Such shifts are similar to equivalent frequency shifts in the original signal. Doppler frequency shifts in transmission systems using a carrier plus sidebands similarly go unnoticed so long as the received signal is monitored and the receiver is properly tuned.

Turning now to a consideration of the apparatus by which the various encoding and decoding operations discussed above are carried out, conventional electronic components, e.g., acoustic delay lines, amplifiers, and adders may be interconnected in the configurations of FIGS. 3 and 5, and several of the configurations may be connected in tandem as shown in FIG. 1, to encode and decode, respectively, applied message signals. In practice, the necessary delays and means for conveniently altering the delays required to maintain a fresh code schedule are realized with a rotating magnetic drum provided with a plurality of independent tracks and a number of associated magnetic transducers, i.e., read, write, and erase heads. FIG. 7 illustrates a preferred arrangement. Delay elements for both the coding and decoding networks are contained on a single drum **70** which is rotated at a constant speed in the indicated direction by any suitable means, not shown. In the example, N separated, circumferential tracks, e.g., five tracks labeled **71***a* . . . *e*, are shown along the upper portion of the drum interconnected with N matrices **72***a* . . . *e* to provide an N stage encoder. Applied signals enter the tandemly connected networks at terminal **73** and, after passing through N networks, emerge at terminal **74**. Similarly, N separated circumferential tracks **75***a* . . . *e* spaced along the lower portion of drum **70** and the associated matrices **76***a* . . . *e* constitute the decoder. Signals entering at terminal **77** pass through N, e.g., five network stages, and emerge at terminal **78**. An erase head E, a single write head R, and n pick up heads P are juxtaposed with each track so that a fresh recording is made for each revolution of drum **70** and n replicas are available at t intervals in the connecting matrices.

In practice, the magnetic transducers along each of the several tracks of the rotating drum are supported in holders attached to a stationary annular ring juxtaposed with the magnetic track so that they may be easily moved about the circumference of the drum to yield any desired delay intervals.

FIGS. 8, 10, and 12 illustrate various ways in which the magnetic transducers and matrices are interconnected to develop networks whose impulse characteristics are those shown, respectively, in FIGS. 9, 11, and 13. It will be appreciated that FIG. 8 represents a network for developing reverse reverberation signals that is, in many respects, similar to that shown in FIG. 3. In the apparatus of FIG. 8, signals applied at input terminal **80** follow two paths: one leading to record head **82** via amplifier **81** and the other leading to output terminal **84** via buffer amplifier **83**. Signals recorded on magnetic track **71** (traveling in the indicated direction) are picked up in succession by

pick up heads **85** through **89**, adjusted in signal strength, according to the weighting coefficients set forth in Equation 2, in amplifiers **90** through **94** and supplied by way of resistors **95** through **99** to output terminal **84** wherein a composite output signal is developed across summing resistor **79**. The exact position of the several pick up heads is, of course, determined by the intervals t required in the selected code schedule. With the proper gain characteristics of the amplifiers **81** and **90** through **94**, and with a phase reversal in the circuit of pick up head **89**, obtained either as shown by reversing the connecting terminals of pick up head **89** or in amplifier **94**, the overall network of FIG. 8 gives rise to the impulse characteristic shown in FIG. 9. This is, of course, the reverse reverberation characteristic defined in Equation 2 above.

FIG. 10 illustrates a magnetic drum version of the normal reverberator shown in block form in FIG. 5. It requires one write head **100** and one pick up head **101**. Signals applied to terminal **102** are passed by way of amplifier **103**, adjusted to have gain $(-g)$, and recorded via head **100** on magnetic track **75**. At a time t seconds later, the signal is passed by way of read head **101** to amplifier **104**, whose gain is $(1-g^2)$, to adder network **105–106** and appears at output terminal **107**. Delayed signals from head **101** are also fed back by way of amplifier **108**, adjusted for gain $(+g)$, to record head **100** wherein they are rerecorded, eventually to be recovered by pick up head **101** in the fashion previously described. Signals applied at terminal **102** are also passed by way of buffer device **109**, which is arranged to invert the signals in polarity, to adder **105–106**. With the pick up and record heads adjusted to provide a delay interval of t seconds, the impulse characteristic shown in FIG. 11 is produced which, as before, is substantially that of a normally reverberated signal.

FIG. 12 illustrates an alternative decoder arrangement which has an impulse response, shown in FIG. 13, substantially identical to the normal reverberation response of FIG. 11. It utilizes, instead of the feedback loop of the apparatus of FIG. 10, a record head **120** and a plurality of pick up heads **121** through **125**. Signals applied at input terminal **126** are adjusted in gain in amplifier **127** and applied directly to write head **120** for recording on magnetic track **75**. At intervals t seconds apart the signals are recovered in the pick up heads, adjusted in gain in amplifiers **128** through **132** according to the coefficients of Equation 2, and supplied via resistors **133** through **137** to adder resistor **139** and output terminal **138**. Signals from input terminal **126** are supplied by way of buffer **140** which, as before, is arranged to invert the polarity of the direct signal component and to supply it via resistor **141** to the adder network at output terminal **138**. Advantageously, with the apparatus of FIG. 12 the individual delay periods may be individually adjusted by moving the pick up heads physically, and the polarity of the individual impulse response elements may be easily adjusted by reversing the terminals on selected pick up heads or by inverting the developed signals in the amplifiers **128** through **132**.

It is not necessary that the rotating magnetic drum **70** used at a transmitter station by synchronized with its counterpart at a receiver station. Since the code schedule, known at both stations, indicates the individual delay intervals, the approximate gain, the exact polarity of each impulse in the network response, and the number of interconnected all-pass networks, it is possible to position the magnetic heads about the drum to duplicate exactly the networks of the encoder station. Moreover, after the magnetic drums at the several stations in the transmission network have been calibrated, for example, in terms of head position versus time delay or the like, it is an easy matter to change the cipher code quickly in order to prevent code detection.

The above-described arrangements are, of course, merely illustrative of the application of the principles of the invention. Although the networks used in the practice of the invention have been described for the most part in terms of transversal filter theory and illustrated by means of delay lines, either acoustic or magnetic, amplifiers, adders and the like, the various networks may also, of course, be realized with conventional wave filters or transmission networks of any well known sort. Numerous other arrangements may be devised by those skilled in the art without departing from the spirit and scope of the invention.

What is claimed is

1. Apparatus for scrambling a message signal to render it unintelligible to an unauthorized recipient which comprises,

means at a transmitter station for adding a sequence of variously delayed replicas of a message signal to the message signal to form a composite signal

means for transmitting said composite signal in analog form to a receiver station,

and at the receiver station,

means for canceling the delay replicas of the received composite signal to reconstitute said message signal.

2. Apparatus for scrambling a message signal to render it unintelligible to an unauthorized recipient which comprises,

means at a transmitter station for adding reverse reverberation to a message signal before transmission,

means for transmitting said message signal and its additions in analog form to a receiver station,

and at the receiver station,

means for canceling the reverse reverberation to reconstitute said message signal.

3. In a signaling system,

means at a transmitter station for translating an input message signal into a signal composed of the message signal and a considerable number of spaced echoes of the signal,

means for transmitting said message signal and said echoes together to a receiver station,

and at said receiver station,

means for canceling said echoes to leave only said message signal.

4. In combination, means for linearly filtering a communication signal to produce a sequence of echoes of said signal, means for adding said sequences of echoes to said signal to produce a composite signal,

means for transmitting said composite signal to a receiver station,

and at said receiver station,

means for linearly filtering the received composite signal to produce a sequence of echoes of said communication signal inverse to said sequence of echoes produced at said transmitting station,

means for subtracting said sequence of inverse echoes from said received composite signal to produce a replica of said communication signal.

5. Scrambling apparatus for encoding message signals for analog transmission to a licensed receiver station which comprises,

means for masking applied message signals with a selected number of pre-signal echoes of the message signal,

said pre-signal echoes being evenly spaced apart in time and of gradually increasing amplitudes,

said masking means comprising a first network including at least one all-pass network,

means for supplying message signals to said first network,

means for individually adjusting the parameters of said first network according to a private code schedule to establish for said first network an impulse response substantially the inverse of normal signal reverberation, and

means for supplying masked message signals derived from said first network to a transmission circuit.

6. Scrambling apparatus as defined in claim 5, in combination with means for adding a selected number of post-echoes to the message signal,

said means comprising a second network connected in series with said first network which includes at least one all-pass network, and

means for adjusting the parameters of said second network to establish for said second network an impulse response of normal post-signal reverberation.

7. Unscrambling apparatus for decoding analog message signals received from a transmitter station masked by the addition of reverse reverberation in the form of pre-signal echoes,

comprising a first network including at least one all-pass network,

means for supplying received signals to said first network,

means for individually adjusting the parameters of said first network according to a private code schedule to establish for said first network an impulse response of normal signal reverberation which is substantially the inverse of the impulse response of the reverse reverberation added to the message signals at said transmitter station, and

means for supplying unscrambled message signals derived from said first network to a utilization device.

8. Unscrambling apparatus as defined in claim 7 in combination with means for removing post-echoes added to said received signal,

said means comprising a second network connected in series with said first network which includes at least one all-pass network, and

means for adjusting the parameters of said second network to establish for said second network an impulse response substantially the inverse of normal signal reverberation.

9. In a privacy system, a first station,

a transmission circuit and a second station,

means at said first station for substantially reducing the intelligibility of applied message signals,

said means including a linear filter,

means for so selecting the parameters of said linear filter that its impulse response resembles that of an all-pass network, and

means for supplying message signals to said linear filter,

means for transmitting signals derived from said filter to a second station,

means at said second station for restoring the intelligibility of signals received from said first station,

said means including a linear filter,

means for so selecting the parameters of said linear filter that its impulse response is substantially the inverse of the impulse response of said linear filter at said first station, and

means for supplying said recovered signals to a utilization circuit.

10. In a privacy system, a first station,

a transmission circuit and a second station,

means at said first station for imparting reverse reverberation to applied signals,

said means including a plurality of interconnected all-pass networks,

means for adjusting said networks individually to alter the impulse responses thereof,

and means for supplying altered signals to said transmission circuit,

means at said second station for removing said reverse reverberation from signals received from said transmission circuit,

said means including a plurality of interconnected all-pass networks whose impulse responses together are adjusted to be substantially the inverse of those of said interconnected all-pass networks at said first station, and

means for supplying said recovered signals to a utilization circuit.

11. In a privacy system which includes a first station, a transmission circuit and a second station,

encoder apparatus at said first station for destroying the apparent meaning of applied signals,

said encoder apparatus including a plurality of interconnected all-pass networks,

means for adjusting each one of said networks to alter the impulse response thereof in accordance with a preassigned schedule,

means for supplying message signals to said encoder apparatus,

and means for supplying encoded signals from said encoder apparatus to said transmission circuit,

decoder apparatus at said second station for restoring apparent meaning to received signals,

said decoder apparatus including a plurality of interconnected all-pass networks,

means for adjusting each one of said networks in accordance with said preassigned schedule to alter the impulse response thereof to substantially the inverse of the impulse response of the corresponding network at said first station,

means for supplying received signals to said decoder apparatus, and

means for supplying restored signals from said decoder apparatus to a utilization circuit.

12. The method of private signal transmission which comprises masking a message signal by passing it through a linear filter at a transmitter station in order to develop a number of echoes of said signal,

transmitting the signal together with a selected number of echoes of selected amplitude, polarity, and separation to a receiver station,

and at the receiver station,

passing the signals through a linear filter whose transmission function is adjusted in accordance with a predetermined code to be substantially the inverse of the transmission function of the transmitter station filter.

References Cited by the Examiner

UNITED STATES PATENTS

2,312,897	3/1943	Guanella	179—1.5
2,406,841	9/1946	Levy	179—1.5
2,935,604	5/1960	DiToro	325—44
2,953,643	9/1960	Koenig	179—1.5
3,012,100	12/1961	Mitchell	179—1.5

ROBERT H. ROSE, *Primary Examiner.*

STEPHEN W. CAPELLI, *Examiner.*