Sept. 3, 1946. M. M. LEVY 2,406,841

SECRET TRANSMISSION SYSTEM

Filed Sept. 11, 1942 3 Sheets-Sheet 1

Fig. 1.

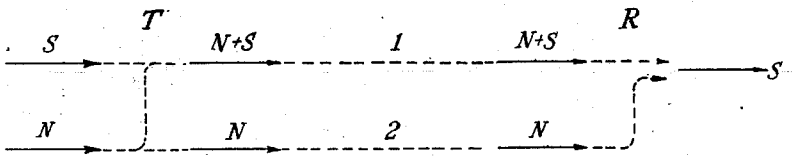


Fig. 2.

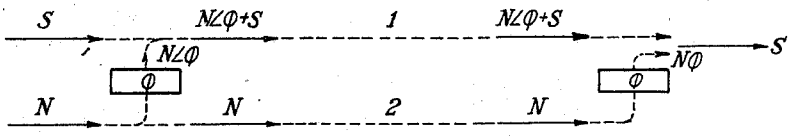


Fig. 3.

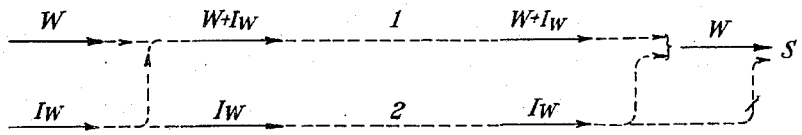


Fig. 4.

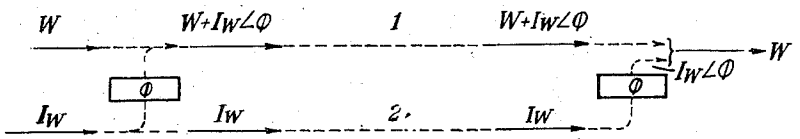
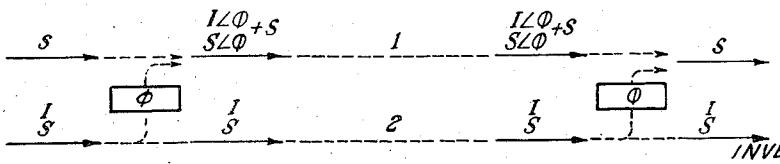


Fig. 5.



INVENTOR
M. M. Levy

BY Loyd Hall Sutton
ATTORNEY

Sept. 3, 1946. M. M. LEVY 2,406,841

SECRET TRANSMISSION SYSTEM

Filed Sept. 11, 1942 3 Sheets-Sheet 2

Fig. 6.

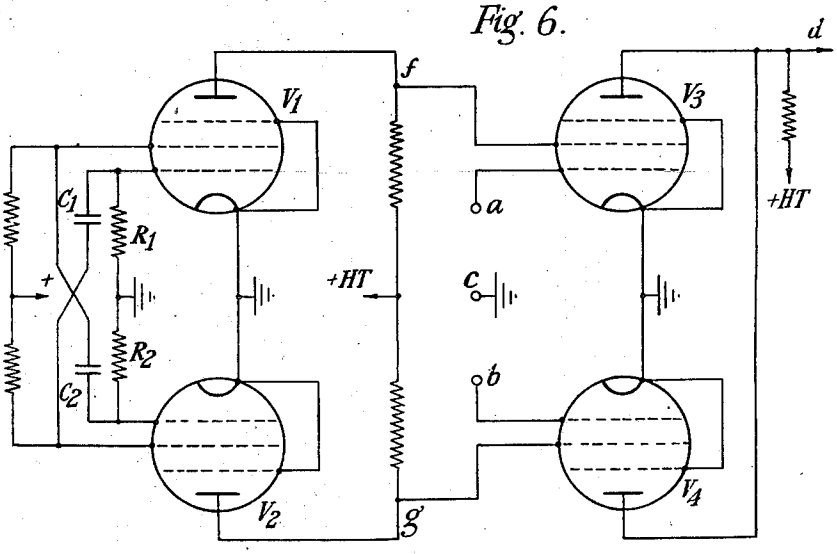


Fig. 7.

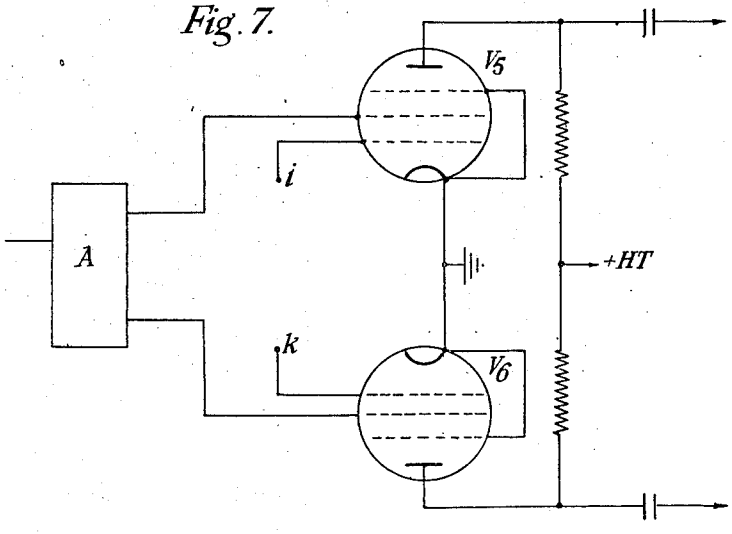
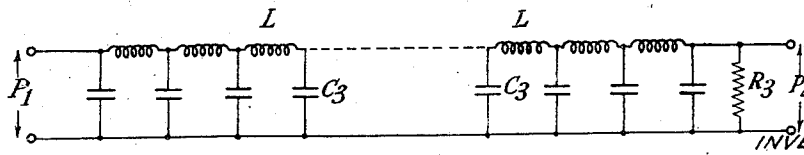


Fig. 8.



INVENTOR
M. M. Levy
BY Loyd Hall Sutton
ATTORNEY

Sept. 3, 1946. M. M. LEVY 2,406,841

SECRET TRANSMISSION SYSTEM

Filed Sept. 11, 1942 3 Sheets-Sheet 3

Fig. 9.

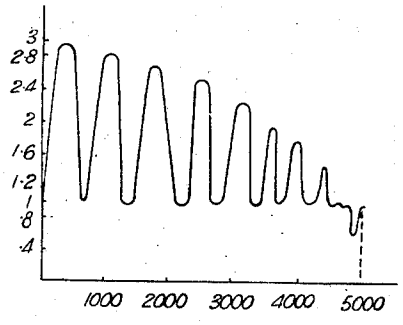


Fig. 10.

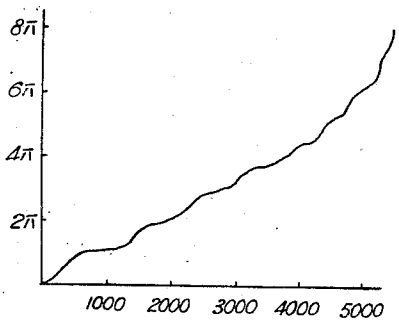


Fig. 11.

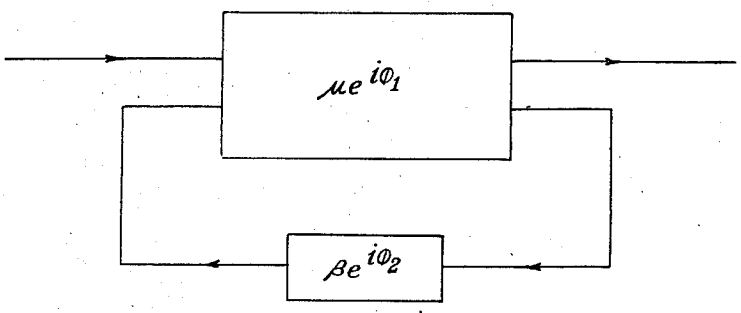
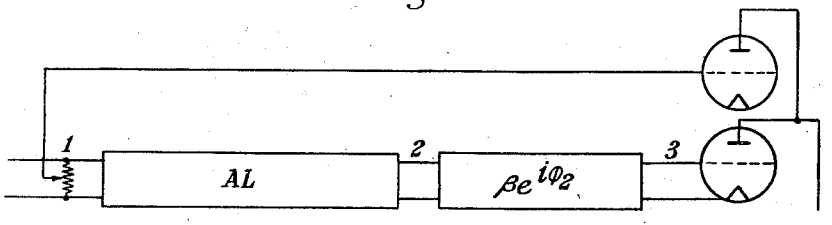


Fig. 12.



INVENTOR
M. M. Levy
BY
Loyd Hall Sutton
ATTORNEY

Patented Sept. 3, 1946

2,406,841

UNITED STATES PATENT OFFICE

2,406,841

SECRET TRANSMISSION SYSTEM

Maurice Moise Levy, London W. C. 2, England, assignor to Standard Telephones and Cables Limited, London, England, a British company

Application September 11, 1942, Serial No. 458,061
In Great Britain July 9, 1941

8 Claims. (Cl. 179—1.5)

1

This invention relates to an electric communication system in which messages are transmitted in such form as to be unintelligible to a receiver not possessing the requisite key, hereinafter called a secrecy system.

The present invention consists in its broadest aspect in such a system comprising means for transmitting two sets of signals, one on each of two separate channels, the first set of signals comprising the desired message in such form that the signals by themselves do not convey the message intelligibly, and the second set being by itself unintelligible, the two sets of signals on being combined being capable of yielding the desired message in intelligible form.

The invention is applicable to transmission both over wires and by means of electromagnetic radiation. In the case of transmission, either over wires or by means of electromagnetic radiation, by means of a carrier wave, the invention need not involve any greater band width than the transmission of one of the sets of signals alone. It is known that two separate sets of signals may be transmitted on a single carrier wave, one by frequency or phase modulation of the carrier wave and the other by amplitude modulation of the carrier wave, and that both sets of signals, whilst occupying the same band width may be separately received by two different processes of demodulation. Accordingly in performing the present invention the two sets of signals may be transmitted, the one by frequency or phase modulation and the other by amplitude modulation of a single carrier.

The invention is equivalent to transmitting an unintelligible set of signals on one channel and to transmitting on the other channel part of the key, in unintelligible form, needed to cause the first mentioned set of signals to render an intelligible message, the remainder of the key consisting in the knowledge of how to apply the second set of signals to the first. This may not in all cases yield a very high degree of secrecy but may be made to do so by means of further features of the invention. This aspect of the matter may be made clearer by means of an example.

It is well known to mask speech by means of "noise," this consisting of a random series of frequencies continually varied in different ways, the receiver being provided with a similar source of noise, and means continually varied in synchronism with the means at the transmitter. The desired message is then obtained by subtracting the local noise N at the receiver from the signals which consist of speech S or other

2

desired signals plus noise N. In applying the invention to this form of securing secrecy, the signals S+N are transmitted on one channel and the noise N alone on another channel. The signals sent along either channel are themselves unintelligible but the key needed to cause the signals S+N to yield an intelligible message is partly the signals N transmitted on the other channel and partly the knowledge that these signals N must be subtracted from the signals S+N. This by itself does not give a high degree of secrecy since the knowledge that the desired signals may be obtained by subtracting the two sets of signals is of such a nature that it can readily and simply be conveyed to an unauthorised person.

If, however, the noise currents before being mixed with desired signals to constitute one of the transmitted sets of signals, are passed through a network which alters their amplitude and phase in a manner dependent upon frequency, the result is different from the original noise and may be called N/φ. One set of signals now consists of $S+N/\varphi$ and the other of N. Both are unintelligible. The set of signals N still contains part of the key needed to obtain the desired signals from the set $S+N/\varphi$ but the desired signals S cannot be obtained by simple subtraction of the two sets of signals. The signals N must first be passed through a network at the receiver which is identical with the one used at the transmitter and the result N/φ then subtracted from the set of signals $S+N/\varphi$. The network may be of fairly simple form and yet the constitution thereof cannot be determined from either set of signals picked up by an unauthorised listener or from any combination of the two. As there is a very large number of forms that the network might take, it is highly unlikely that an unauthorised listener could find the correct form by a process of trial and error.

This process may be modified by using two networks, one at the transmitter and one at the receiver which are the inverse, one of the other. Thus the desired signals S may be combined with noise N and the set of signals S+N transmitted on one channel. The noise N is also passed through a network of the kind mentioned above to yield a set of signals N/φ which is transmitted on the other channel. Each set of signals is by itself unintelligible and the result of subtracting one from the other is equally unintelligible. If, however, the signals N/φ are at the receiver passed through a network which is the inverse of that at the transmitter so as to restore the

set of signals N/φ to N, the desired signals are obtained in intelligible form by the subtraction of the set of signals N from the set of signals S+N.

The invention may also be applied in cases in which other means than mixture with noise is used to render speech or other signals unintelligible. Thus secrecy systems are known in which a carrier frequency is continuously varied, but in known forms of such systems elaborate synchronising systems are needed to vary in synchronism the frequencies of the carrier at the transmitter and the local oscillator of a heterodyne modulator at the receiver. These difficulties are removed by means of the present invention.

Examples of such use of the present invention will now be described. It is well known that inverted speech may be obtained by causing the speech band to modulate a carrier frequency near the upper limit of the band and by selecting the lower side band. Such inverted speech is by itself unintelligible, but it is easy to render it intelligible by recombining it with the original modulating frequency, easily found by trial if it is not known, and again selecting the lower side band with suppression of the carrier. If, however, the carrier frequency used to produce the inverted speech be continuously varied in an irregular manner, it is almost impossible to obtain intelligible speech therefrom without having a local oscillator varied in synchronism with said carrier. In one example of the use of the present invention inverted speech thus produced with a continuously varied carrier is transmitted on one channel, and a mixture of the said inverted speech and the carrier used to produce it is transmitted on a second channel. At the receiver, intelligible signals can be obtained by combining the signals received on the two channels. Preferably, before combining the varying inverted speech with the varying carrier to constitute the signals sent on the second channel, the varying inverted speech is passed through a distorting network and a similar network is used at the receiver to obtain from the signals received on the second channel signals which may be combined with those received on the first channel to produce intelligible speech. In the alternative the varying inverted speech is passed through a distorting network before being transmitted on the first channel and the received signals passed through an inverse network before being combined with those received on the second channel.

In another example of the invention there is transmitted on one channel a set of signals consisting alternately of speech and inverted speech and if the intervals at which switching between the two takes place are properly chosen the result is highly unintelligible. In order to render this result intelligible the inverted speech must be reinverted, and in order to do this it is necessary to switch the received signals to such re-inverter in synchronism with the switching at the transmitter. The invention may be utilised to transmit the necessary synchronising signals and yet to prevent an unauthorised receiver making use of them to obtain intelligible signals. Thus the alternate speech and inverted speech is transmitted on a first channel and is also passed through a distorting network to produce signals which are mixed with the synchronising signals transmitted on the second channel. At the receiver the signals received on the first channel are passed through a network identical with that at the transmitter to produce signals which are subtracted from those on the second channel to obtain the synchronising signals. These synchronising signals are then applied to control a switch to obtain the inverted speech in the intervals of inversion which can be reinverted and applied in proper order with the intervals of speech to obtain the desired speech intelligibly.

The nature of the invention will be better understood from the following description taken in conjunction with the accompanying drawings in which

Figs. 1 to 5 are diagrams of systems according to the invention.

Figs. 6 and 7 are circuits which form part of the system of Fig. 5.

Fig. 8 is one form of network used in systems according to the invention.

Figs. 9 and 10 are curves relating to the network of Fig. 8, and

Figs. 11 and 12 show how a network which is the inverse of a given network may be obtained.

Referring to the drawings, Fig. 1 is a diagram illustrating one system according to the broadest aspect of the invention. Unintelligible signals are produced by mixing noise signals N with speech S to produce signals denoted N+S. These signals are sent from a transmitting station T on a channel 1, either directly or by modulation of a carrier wave to a receiving station R. The noise signals N are transmitted from station T to station R on a second channel 2. At the receiver the signals N+S and N received on channels 1 and 2 respectively, after detection if necessary, are combined together in known manner to produce the original speech S.

In the system shown in Fig. 2, noise signals N are transmitted on channel 2, as in the system of Fig. 1 but before being mixed with the speech S, these signals N are passed through a network φ which alters them in amplitude and/or phase in a manner depending upon their frequency and thus produces other signals N/φ. These latter are combined with the speech S to produce signals N/φ+S which are transmitted on channel 1. At the receiver the signals received over channel 2 are passed through a network φ which is an exact counterpart of that at the transmitter to produce signals N/φ which are thereupon combined with the signals N/φ+S received over channel 1 to give the original speech signals S.

In the system shown in Fig. 3 inverted speech is produced at the transmitter but the frequency of the oscillator used is changed at the rate of a few cycles a second between limits a few hundred cycles apart. The inverted speech thus formed is denoted Iw. The signals Iw are sent on channel 2, either directly or as modulations of a high frequency carrier. The signals Iw are mixed with the varying carrier frequency W and the mixture W+Iw sent over channel 1 either directly or as modulations of a high frequency carrier of frequency different from that of channel 2, or the high frequency carrier of channels 1 and 2 may be the same and channel 1 constituted by phase or frequency modulation and channel 2 by amplitude modulation of this carrier or vice versa.

At the receiver, the signals from channel 2 are combined with those from channel 1, and the result, which is the varying carrier frequency, applied to a demodulator to which the varying frequency band Iw of inverted speech is also applied. The result is to re-invert the signals Iw and to cancel out the variations in frequency to yield intelligible speech S.

Fig. 4 shows the arrangement of Fig. 3 modified by the addition of a distorting network φ. The varying frequency inverted speech is transmitted on channel 2, but before being combined with the varying carrier W, it is passed through a distorting network φ, and the combined signals $W+Iw/\varphi$ transmitted on channel 1. At the receiver the signals Iw received on channel 2 must be passed through a network φ identical with that at the transmitter before the varying carrier wave W can be obtained, which latter is necessary for obtaining intelligible speech from the signals Iw.

The carrier frequency being outside the transmitted inverse speech frequency range, an unauthorised listener may filter it out with a convenient band-pass filter. It is preferable therefore to send on channel 1, instead of the carrier frequency itself, a sub-harmonic of the carrier frequency within the inverse speech frequency range mixed with the varying inverted speech. After separation from the varying inverted speech at the receiver, in the manner described above, this sub-harmonic may then be made to yield the required variable carrier frequency by frequency multiplication.

The arrangements shown in Figs. 2 and 4 may be modified by placing the network φ in the path of the signals N or Iw before they are transmitted over the channel 2 instead of in the position shown. At the receiver a network is used in the position shown for φ in Fig. 2 or 4, which is the inverse of the network at the transmitter. Two networks are defined to be inverse the one of the other when a signal wave passed through both networks in series appears in unaltered form.

Still another system according to the invention is shown diagrammatically in Fig. 5. Electronic switching means is used to connect to a transmission channel speech signals S and speech signals inverted I, the alternate signals transmitted being denoted

$$\frac{I}{S}$$

These signals are unintelligible unless subjected to a switching means acting in synchronism with that at the transmitter. Synchronising signals for controlling the actuation of such switching means are denoted as s. The signals

$$\frac{I}{S}$$

are transmitted on channel 2 and are also passed through a distorting network φ to produce signals

$$\frac{I\varphi}{S\varphi}$$

which are mixed with the synchronising signals s and transmitted on channel 1. At the receiver the signals

$$\frac{I}{S}$$

received in channel 2 are passed through a distorting network φ identical with that at the transmitter and the synchronising signals s are obtained by subtracting the result from the signals received over channel 1. These synchronising signals are then applied to the signals

$$\frac{I}{S}$$

received over channel 2 to cause the speech to be reinverted during intervals corresponding to those during which it was inverted at the transmitter.

Fig. 6 shows an arrangement by means of which the signals

$$\frac{I}{S}$$

of Fig. 5 may be produced. The two pentode tubes V_1 and V_2 are connected in such a manner as to constitute a multi-vibrator. A point in the anode circuit of tube V_1 is connected to the screen grid of tube V_3 and a corresponding point in the anode circuit of tube V_2 is connected to the screen grid of tube V_4. Speech potentials are applied between the terminals a and c in the input circuit of tube V_3 and inverted speech between the terminals b and c in the input circuit of tube V_4. The anodes of tubes V_3 and V_4 are connected together. The tubes V_1 and V_2 are conducting alternately for intervals determined by the values of the condensers C_1 and C_2 and the resistances R_1 and R_2 of the multivibrator circuit. The potentials which appear at the point f and which are applied to the screen grid of tube V_3 may be considered as the synchronising signals s of Fig. 5. When this point f is positive, tube V_3 is conducting and passes speech signals into the common output circuit. When point f is negative, tube V_3 is non-conducting, but point g is positive and tube V_4 is conducting and passes inverted speech to the common output circuit. The signals appearing at point d are thus the signals

$$\frac{I}{S}$$

of Fig. 5.

Fig. 7 shows part of the arrangements at the receiver of Fig. 5. After separation of the synchronising signals s from the signals

$$\frac{I}{S}$$

the synchronising signals s are applied to a push pull amplifier A, and opposed points in the output are connected to the screen grids of two pentode tubes V_5 and V_6. The control grids are connected in opposition to terminals i, k, to which the signals

$$\frac{I}{S}$$

are applied. When the synchronising signals are positive, the tube V_5 is conducting and speech S appears in its output circuit. When the synchronising signals are negative, tube V_6 is conducting and inverted speed I appears in its output circuit.

Fig. 8 shows one example of a network, which can be used as the network φ shown in Figs. 2 to 5. This is in the form of a low-pass filter terminated by a resistance R_3 which is different from the characteristic impedance of the filter. If this network consists of ten sections, the inductances L being 0.5 henry and the capacities C_3 of 0.06 microfarad, the characteristic impedance is of the order of 1000 ohms. If the network be terminated in a resistance R_3 of 3,000 ohms, Fig. 9 shows the relation between the ratio of the voltages P_1 and P_2 at the output and input respectively as a function of frequency, whilst Fig. 10 shows the phase change produced as a function of frequency.

If instead of constituting the network of like sections, unlike sections are used, still more complex curves will be obtained.

If it is desired to produce two inverse networks the following method may be used:

Referring to Fig. 11, let $\mu e^{i\varphi_1}$ be the propagation constant of an amplifier and $\beta e^{i\varphi_2}$ the

propagation constant of the feedback path.

The propagation constant of the feedback amplifier is:

$$\frac{\mu e^{i\varphi_1}}{1+\mu\beta e^{i(\varphi_1+\varphi_2)}}=\frac{1}{\frac{1}{\mu}e^{-i\varphi_1}+\beta e^{i\varphi_2}}$$

If this circuit is considered as a network, the inverse network must have a propagation constant equal to:

$$\frac{1}{\mu}e^{-i\varphi_1}+\beta e^{i\varphi_2}$$

It is assumed that μ is practically constant throughout the frequency range and that the phase shift φ_1 produced by the amplifier is proportional to frequency throughout the frequency range. This means that if a signal is applied to the input of the amplifier, it will appear at the output after a short time, called "retardation time" and will have the same form as the applied signal. Such amplifiers are very frequently used in television.

With these hypotheses,

$$\frac{1}{\mu}$$

is a constant generally less than unity and $e^{-1\varphi_1}$ means that the network having a propagation constant

$$\frac{1}{\mu}e^{-i\varphi_1}$$

has a negative retardation time, i. e. the signal at the output appears a short time before the signal is applied.

Consider now the circuit of Fig. 12 it comprises an artificial line AL producing a phase-shift equal to φ_1, in series with a network identical with the feedback path of Fig. 11.

If a signal is applied at the input **1** of the line, the signal will appear at the output **2** of the line after a short time and will be undistorted.

Let V_1, V_2, V_3 be the voltages at a given frequency at terminals **1**, **2** and **3**.

Between V_1 and V_2 there is the relation:

$$V_2=V_1e^{i\varphi_1} \tag{1}$$

or:

$$V_1=V_2e^{i\varphi_1}$$

and between V_2 and V_3 there is the relation:

$$V_3=V_2\beta e^{i\varphi_1} \tag{2}$$

Let V_1' be a fraction $\frac{1}{\mu}$ of the voltage V_1; Equation 1 becomes:

$$V_1'=V_2\frac{1}{\mu}e^{-i\varphi_1}$$

If voltage

$$V_1'$$

is applied on the grid of a valve and V_3 on the grid of a second valve, and if the plates of the valves are in parallel, on the plates we have or voltage proportional to:

$$V_1'+V_3=V_2\left[\frac{1}{\mu}e^{-i\varphi_1}+\beta e^{i\varphi_2}\right]$$

If voltage V_2 is applied at the input of a network having a propagation constant equal to

$$\frac{1}{\mu}e^{-i\varphi_1}+\beta e^{i\varphi_2}$$

at the output we will obtain a voltage equal to

$$V_1'+V_3$$

On the other hand as the signal at terminals **2** has the same form as the signal applied at terminals **1**, one sees that the circuit of Fig. 12 is the inverse network of the circuit of Fig. 11.

What is claimed is:

1. Secrecy system comprising separate first and second signal channels, a transmitting station, means at said transmitting station for transmitting over said first channel a first set of unintelligible signals, means for transmitting over said second channel a second set of different unintelligible signals, at least one of said sets of signals containing all wave components from which a desired message signal is derivable, a receiving station, means at said receiving station for combining said two sets of signals, and means for utilizing the resultant of the combined signals to derive the desired message.

2. Secrecy system comprising separate first and second signal channels, a transmitting station, means at said transmitting station for producing noise signals consisting of a random series of frequencies continually varied, means for transmitting said noise signals over said first channel, means at said transmitting station for combining said noise signals with message signals and for transmitting the combined signals over said second signal channel, a receiving station, and means at said receiving station for combining the two sets of signals received over said two signal channels to derive the desired message.

3. Secrecy system comprising separate first and second signal channels, a transmitting station, a source of carrier frequency waves thereat, means for modulating a message signal with said carrier frequency waves to produce a band of waves in which all the signal frequencies are inverted, means for transmitting said inverted band as a first set of signals over one of said signal channels, means at said transmitting station for combining said inverted band and said carrier frequency waves to constitute a second set of signals and for transmitting said second set of signals over the other of said signal channels, a receiving station, means at said receiving station for receiving separately said two sets of signals, means for combining said two sets of signals to derive said carrier frequency wave, and means for combining said carrier frequency wave with said inverted band to derive the message signals.

4. Secrecy system according to claim 3 wherein said source of carrier frequency waves comprises a source the frequency of which is continuously varied.

5. Secrecy system comprising separate first and second signal channels, a transmitting station having means for producing noise signals consisting of a random series of frequencies continually varied, means for transmitting said signals on the first channel as a first set of signals, a first wave distorting network, means for passing said noise signals through said distorting network and combining the distorted signals with message signals to produce a second set of signals, means for transmitting said second set of signals on said second channel, a receiving station means at said receiving station for receiving separately both said sets of signals, a second wave distorting network identical with that at the transmitting station, means for passing said first set of signals through said second distorting network, and means for combining the resultant distorted signals with said second set of signals to yield the said message signals.

6. Secrecy system comprising separate first and second signal channels, a transmitting station, a source of carrier waves of varying frequency means for producing from message signals and said carrier waves a first set of signals comprising a band of signals the frequencies of which are inverted and vary continuously with respect to those of the message signals, means for transmitting said first set of signals over said first channel, a first wave distorting network, means for passing said first set of signals through said distorting network and for combining the distorted band of signals with said varying frequency carrier waves to produce a second set of signals means for transmitting the said second set of signals over said second channel, a receiving station means at said receiving station for receiving separately both said first and second sets of signals, a second wave distorting network identical with that at the transmitter, means for passing said first set of signals through said second distorting network, and means for combining the said distorted signals with said second set of signals to yield said message signals.

7. Secrecy system comprising separate first and second signal channels, a transmitting station having means for inverting a band of frequencies representing message signals, means for

producing signals consisting in successive intervals of said message signals and inverted message signals to form a first set of signals, means for transmitting said first set of signals over said first channel, a first wave distorting network, means for passing said signals through said distorting network, means for combining the resultant waves with signals for synchronising said successive intervals, means for transmitting the combined signals as a second set of signals over said second channel, a receiving station, means at said receiving station for receiving separately said first and second sets of signals, second wave distorting network identical with that at the transmitter, means for passing said first set of signals through said second network, means for combining the wave with said second set of signals to obtain said synchronising signals and means for applying said synchronising signals to said first set of signals to yield the message signals.

8. Secrecy system as claimed in claim 1 in which said separate channels are constituted, the one by frequency or phase modulation, and the other by amplitude modulation of the same carrier wave.

MAURICE MOISE LEVY.