United States Patent [19]

Reynolds

[11] **3,808,536**

[45] **Apr. 30, 1974**

[54] **COMMUNICATION SCRAMBLER SYSTEM**

[75] Inventor: **John Spackman Reynolds,** Portsmouth, England

[73] Assignee: **The General Electric Company Limited,** London, England

[22] Filed: **Apr. 12, 1972**

[21] Appl. No.: **243,281**

[52] **U.S. Cl.** .... **325/32,** 178/22, 179/1.5 R, 179/1.5 S

[51] **Int. Cl.** **H04k 1/02**

[58] **Field of Search** .... 325/32, 42, 44; 179/1.5 R; 178/22

[56] **References Cited**

UNITED STATES PATENTS

3,560,659	2/1971	Greefkes et al.	325/42
3,123,672	3/1964	Ross	179/1.5 R
3,696,207	10/1972	Lundin et al.	179/1.5 S
3,659,046	4/1972	Angeleri et al.	325/32
3,614,316	10/1971	Andrews, Jr. et al	178/22

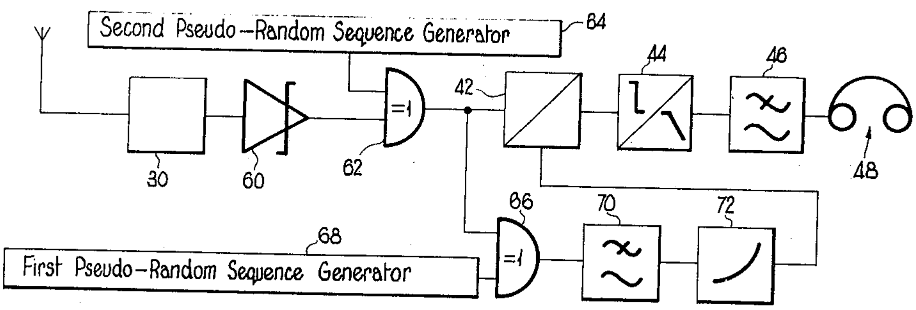
Primary Examiner—Maynard R. Wilbur
Assistant Examiner—H. A. Birmiel
Attorney, Agent, or Firm—Kirschstein, Kirschstein Ottinger & Frank

[57] **ABSTRACT**

A scrambler system in which amplitude zero-crossings in speech are encrypted at a transmitter by combination with a pseudo-random digital sequence, the reverse process occurring at the receiver. The amplitude envelope need not be encrypted, but if desired, can be encrypted by combination with a further pseudo-random digital sequence. A higher level of scrambling can be achieved in the transmitted signal by using the conjugate of the amplitude envelope.

With a sequence bit rate of about two kilobits per second, there is no increase in bandwidth requirements compared to the transmission of unscrambled speech. Thus standard transceivers can be employed, and pre-existing ones readily modified for scrambling and unscrambling.

20 Claims, 4 Drawing Figures



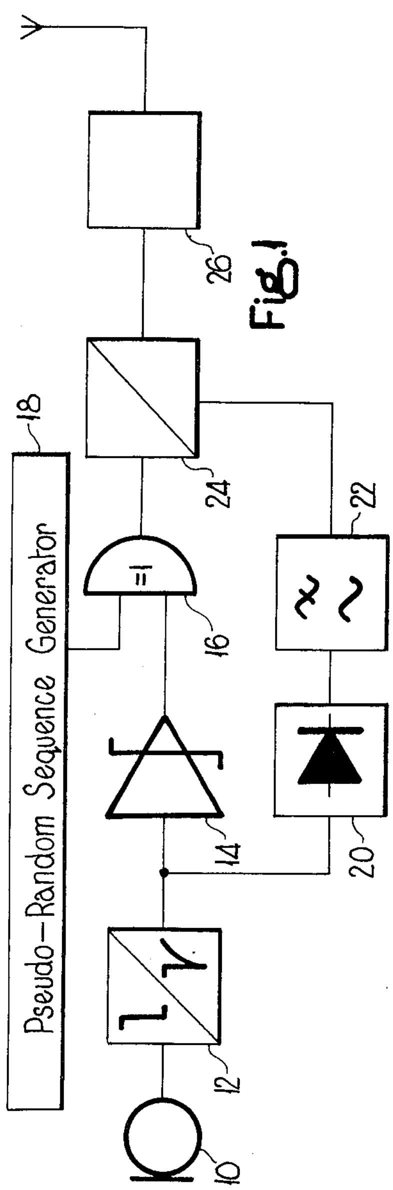

Pseudo-Random Sequence Generator
10
12
14
16
18
20
22
24
26

Fig.1

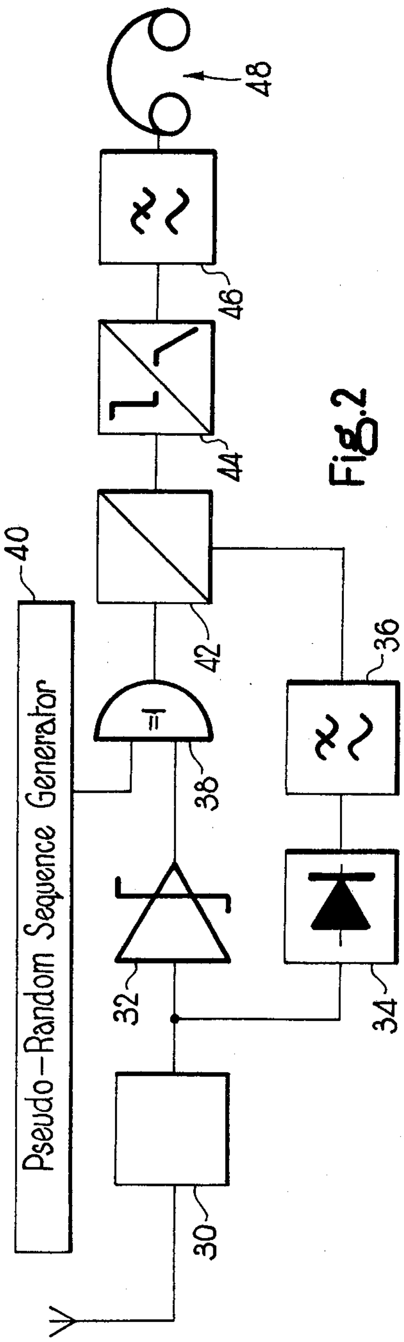

Pseudo-Random Sequence Generator
30
32
34
36
38
40
42
44
46
48

Fig.2

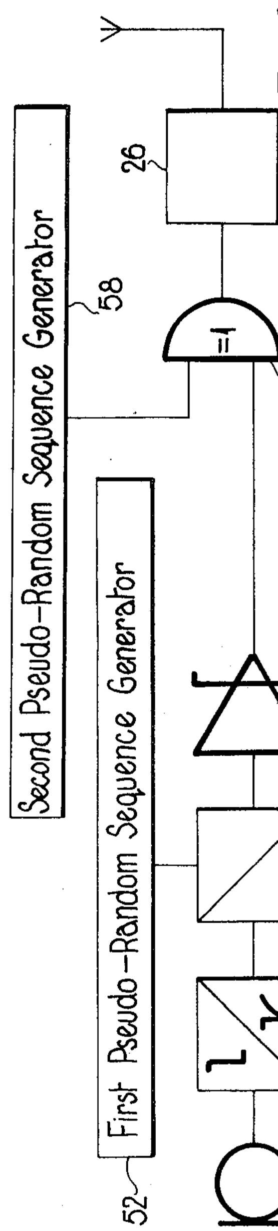

Second Pseudo-Random Sequence Generator
58
First Pseudo-Random Sequence Generator
52
10
12
50
54
56
26
=1

Fig.3

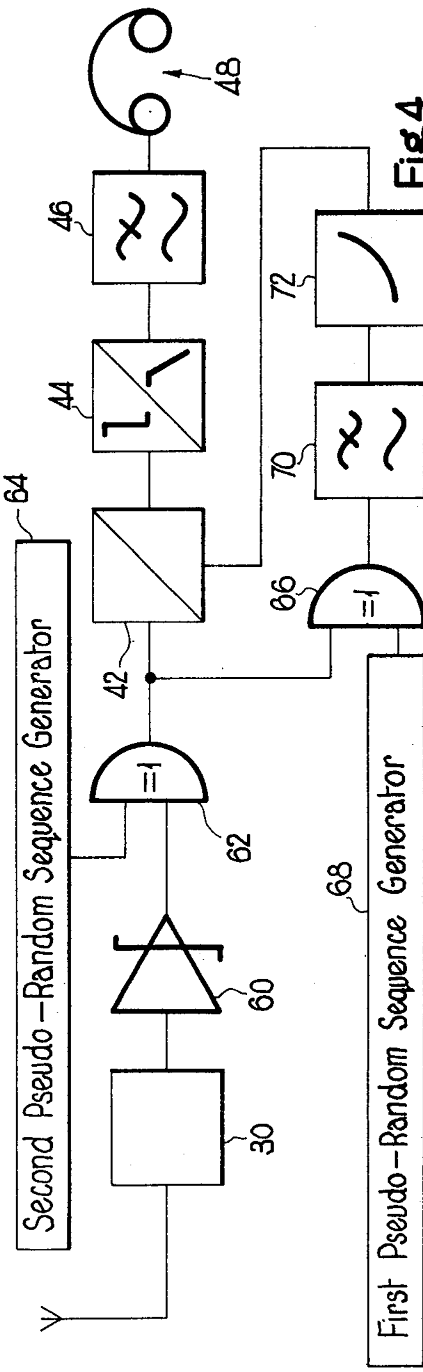

Second Pseudo-Random Sequence Generator
64
First Pseudo-Random Sequence Generator
68
30
60
62
42
44
46
48
66
70
72
=1

Fig.4

COMMUNICATION SCRAMBLER SYSTEM

This invention relates to communication systems and to apparatus for use in such systems.

The invention relates more particularly but not exclusively to communication systems and apparatus for the transmission and reception of speech.

Personal wireless transceivers are now widely used by policeman, for example while on a routine patrol, to maintain contact with their headquarters. However, the value of such communication systems is lessened by their vulnerability to eavesdropping by unauthorised persons.

Scramblers employing various forms of frequency shifting arrangements are known and have been widely employed. However, the time required by an unauthorised person having suitable equipment to unscramble a frequency-shift scrambled message is not very great, so that only a limited security is available. Transmissions scrambled on a truly random basis are undecodable, but the arrangements required are impracticable for widespread, everday use, wherein in any event, only, say, one hour of security is required.

It is therefore an object of the invention to provide an improved communication system and apparatus for use in such a system which allows at least a limited period of privacy or security.

According to a first aspect of the invention, in a communication system for transmitting the intelligence of an input signal, which said input signal is either a speech signal or other signal having components of variable frequency and variable amplitude, a transmitting terminal of the system has means to effect scalar combination of the input signal or of a signal which is derived from the input signal and which contains information as to at least the frequencies of higher frequency components of the input signal with a digital signal having a plurality of possible amplitude levels which occur in a pseudo-random sequence, the signal resulting from the combination or a signal derived therefrom constituting the signal transmitted to a receiving terminal of the system, this transmitted signal carrying information in respect both of the frequencies of said higher frequency components of the input signal (albeit masked by the digital signal) and of the amplitude envelope of the input signal, and the receiving terminal of the system has means to effect scalar combination of the received signal or of a signal derived from the received signal and a digital signal that is similar to that utilised at the transmitting terminal and has the same pseudo-random sequence to recover a first signal carrying information of at least the higher frequency components of the input signal without digital masking, means to recover a second signal carrying information as to the amplitude envelope of the input signal, and means to reconstitute from said first and second signals an output signal which is an intelligible approximation to the input signal.

The signal which is derived from the input signal may be derived by high-pass filtering or differentiation of the input signal.

The signal which is combined with the digital signal may be converted to a signal having a similar or the same plurality of amplitude levels as the digital signal.

The information contained in the transmitted signal in respect of the amplitude envelope may be or be derived from a signal representing the amplitude envelope or its conjugate, and the last-mentioned signal may contain a further digital signal having a plurality of possible amplitude levels which occur in a further pseudo-random sequence, the means to recover the second signal being such as to enable the masking effect of the further digital signal to be counteracted.

According to a second aspect of the invention, in transmitter terminal apparatus for transmitting the intelligence of an input signal, which said input signal is either a speech signal or other signal having components of variable frequency and variable amplitude, the apparatus comprises means to form a digital signal having a plurality of possible amplitude level which occur in pseudo-random sequence, means to effect scalar combination of the digital signal with the input signal or with a signal which is derived from the input signal and which contains information at to at least the frequencies of higher frequency components of the input signal, and means for including in the transmitted signal, which is formed by or derived from the output of the last mentioned means, information in respect of the amplitude envelope of the input signal.

The transmitter terminal apparatus preferably includes means for limiting the bandwidth of the signals to be transmitted to a bandwidth not substantially more than the bandwidth of the input signal.

According to a third aspect of the invention, in receiver terminal apparatus for receiving a transmission of the intelligence of an input signal which said input signal is either a speech signal or other signal having components of variable frequency and variable amplitude, the transmission being formed by or derived from a scalar combination of a digital signal having a plurality of possible amplitude levels which occur in pseudo-random sequence, with the input signal or with a signal derived from the input signal and which contains information as to at least the frequencies of higher frequency components of the input signal, the transmission including information in respect of the amplitude envelope of the input signal, the apparatus comprises means to form a digital signal similar to that utilised in the formation or derivation of the transmission and having the same pseudo-random sequence, means to effect scalar combination of the digital signal with the received signal or a signal derived therefrom to recover a first signal carrying information of at least the higher frequency components of the input signal without digital masking, means to recover a second signal carrying information as to the amplitude envelope of the input signal, and means to reconstitute from said first and second signals an output signal which is an intelligible approximation to the input signal.

The transmitter terminal apparatus may include means for generating a further digital signal having a plurality of possible amplitude levels which occur in a further pseudo-random sequence, and means for combining or superimposing the further digital signal with or on the signal representing the amplitude envelope or its conjugate, the receiver terminal apparatus including means for generating a further digital signal which is similar to the further digital signal utilised in the transmitter terminal apparatus and having the same pseudo-random sequence, means for affecting scalar combination of the further digital signal with said second signal to reconstitute the amplitude envelope or its conjugate.

The digital signals and further digital signals may have two, three, four, or more amplitude levels.

By limiting the bandwidth of the signals to be transmitted to the bandwidth of the original input signals (e.g. speech) the original transmitter and receiver of a pre-existing communication system may be used, i.e., an existing radio transceiver may readily be converted to the form of the present invention, without exceeding its bandwidth capabilities. Thus, for example, the transmitter terminal apparatus can function between the microphone and the remainder of an existing radio transmitter and likewise the receiver terminal apparatus can function between a standard radio receiver and its audio output stage.

Pseudo-random sequence generators of the feedback shift register type are readily adaptable to give different output sequences, by changing the points from which the feedback is taken. Thus code changing is easy. The sequence generators at the transmitter terminal and receiver terminal can be synchronised by breaking the feedback path of the receiver's sequence generator, (or the appropriate one of the two, as the case may be) feeding an intelligence-free (i.e., speech-free) received signal in to the shift register in place of the feedback, comparing the input and the feedback, and after an identity in the comparison for an adequate period of time (equal to the time required to prime the register with the sequence portion being transmitted, plus a safety margin), reconnecting the feedback and disconnecting the received signal which can then be decoded by the now synchronised pseudo-random sequence generator. (An unsynchronised receiver sequence generator or one not producing a correct sequence will cause the receiver output to be unintelligible).

Embodiments of the invention will now be described by way of example with reference to the accompanying drawings wherein:

FIG. **1** is a block schematic diagram of a first embodiment of transmitter terminal apparatus in accordance with the invention;

FIG. **2** is a block schematic daigram of receiver terminal apparatus for use with the transmitter terminal apparatus of FIG. **1**;

FIG. **3** is a block schematic diagram of a second embodiment of transmitter terminal apparatus in accordance with the invention; and

FIG. **4** is a block schematic diagram of receiver terminal apparatus for use with the transmitter terminal apparatus of FIG. **3**.

Referring first to FIg. **1**, transmitter terminal apparatus in accordance with the invention comprises a microphone **10** for converting an acoustic input signal such as speech to an electric signal representative of the intelligence to be transmitted, a differentiator **12** which enhances the high frequency components of the signal, and thereby increases the rate of zero crossing in the signal, for a purpose to be explained hereafter, and a high gain saturating amplifier or Schmitt trigger **14** whose output is a binary signal and is fed as one input of a module-two adder **16** (which may conveniently be considered as an "exclusive OR" circuit). The other input to the module two adder **16** is a digital signal having a pseudo-random binary sequence from a sequence generator **18**. The output of the differentiator **12** is passed through an envelope amplitude detector comprising a rectifier **20** and a low pass filter **22**, the output of which is a unidirectional signal the level of which at any instant is a measure of the amplitude envelope of the data to be transmitted. The latter signal, and the output of the modulo two adder **16** are combined in a suitable signal combination circuit **24**, and subsequently broadcast by a conventional wireless transmitter **26**. The circuit **24** preferably amplitude modulates the signal supplied by the adder **16** with the signal supplied by the filter **22** through useful results can be obtained by linear addition.

With speech having a band-width in the range 300 Hz to 3 kHz and the output of the sequence generator **18** being within this range, for example about 2,000 bits per second, the band-width of the signals reaching the transmitter **26** can be restricted to lie within the above band without any serious loss of information. For this purpose, a low-pass or band-pass filter (not shown) may be connected between the circuit **24** and the transmitter **26**. Alternatively, the transmitter **26** may be constructed or adapted to accomplish the necessary bandwidth limitation. Thus no special frequency capability is required of the transmitter **26**, which may be any conventional form of transmitter. The transmitted signal, though possessing speech like qualities in terms of waveform, is completely unintelligible without knowledge of the pseudo-random sequence. Although the envelope of the speech input is not scrambled, it contains substantially no meaningful intelligence by itself.

Referring now to FIG. **2**, receiver terminal apparatus for receiving the transmissions of the arrangement of FIG. **1** comprises a wireless receiver **30** which is compatible with the transmissions of the transmitter **26**. The output of the receiver **30** is fed both to a high gain limiting amplifier or Schmitt trigger **32** and an envelope amplitude detector comprising a rectifier **34** and a low pass filter **36**.

The outpt of the amplifier **32** is a binary signal whose level transitions correspond to the level transitions in the combined signal which is the output of the modulo two adder **16** (FIG. **1**). Thus the amplifier **32** creates a homologue of the combined signal of the transmitter. This homologue is fed to a modulo two adder **38** as one input thereof, the other input to the adder **38** being a digial signal comprising a pseudo-random binary sequence from a sequence generator **40**, and which is instantaneously identical to the sequence being produced by the sequence generator **18** (FIG. **1**). (The achievement of this identity will be explained hereafter).

The output of the modulo two adder **38** is a binary signal whose transitions represent transitions in the output of the amplifier **154** at the transmitter (FIG. **1**); i.e., the output of the adder **38** is a homologue of the output of the amplifier **14**. This arises from the fact that a binary number which is modulo two added twice to another number gives the other number; i.e., even numbers of modulo two additions of any binary number or sequence are self-cancelling.

The binary output of the adder **38** is combined with the amplitude envelope signal from the low pass filter **36** in a suitable combination circuit **42** (which will be an amplitude modulator if the circuit **24** is an amplitude modulator); integrated in an integrator **44** to cancel out the effects of the differentiator **12** (FIG. **1**); filtered in a low pass filter **46** to remove the noise and spurious high frequency components introduced for example by the limiter **32**, the sequence generator **40**, and the adder **38**; and converted to audible signals in a suitable transducer **48** such as headphones or a loudspeaker. The output of the transducer **48** will be an intelligible reproduction of the speech or other data received by the microphone **10** (FIG. **1**).

The pseudo-randon sequence generators **18** and **40** may be synchronised in any convenient manner. Where the generators **18** and **40** are shift registers whose inputs are the outputs of respective exclusive OR gates fed from, say, the last stage and one other stage of each register, (a known fomr of pseudo-random binary sequency generator), the following synchronising procedure may be followed. With a speech-free signal being received, the input of the shift register in the sequence generator **40** is disconnected and the output of the amplifier **32** substituted. This causes the shift register to take up the portion of the sequence currently being generated at the transmitter terminal, and so primes the register correctly. The output of the exclusive OR gate within the generator **40** is compared with the input to the register and when they have maintained identity for a suitable length of time (i.e., the time required for the register to be primed (equal to the time required to clock one bit through the length of the register) plus any desired safety margin) the generators **18** and **40** are assumed to be in synchronism. The amplifier **32** is then disconnected from the register and reconnected as shown in FIG. **3**, and the exclusive OR gate reconnected to the input of the register. The sequence generator **40** then continues in a self-sustaining mode. Register clocking signals may be obtained at the receiver in any known manner from the broadcast signal to maintain synchronism of the respective generators. It can be arranged that the above procedure is carried out automatically at commencement of reception, or manually performed when required. (It is assumed of course that the connections to the exclusive OR gates are the same in the transmitter and receiver terminals, i.e., that the correct "code of the day" is being used).

The larger the number of zero crossings, the better will be the quality of the reconstituted speech or other date at the receiver; hence the inclusion of the differentiator **12** in the transmitter to produce a greater number of zero crossings in the data to be transmitted. The effect of the differentiator **12** is substantially nullified at the receiver by the integrator **44**. The data transmission system of FIGS. **1** and **2** will function without zero-crossing enhancement i.e., if the differentiator **12** and the integrator **44** were omitted, but transmission quality will be somewhat poorer.

The transmitted signals in the system of FIGS. **1** and **2** may be summarised as being the true envelope and scrambled zero-crossings. The transmitted signals of the system now to be described with reference to FIGS. **3** and **4** may be summarised as being scrambled envelope and scrambled zero-corssings.

Referring to FIG. **3**, the transmitter terminal apparatus of the system again comprises the microphone **10** and the differentiator **12**. A first pseudo-random binary sequence from a first pseudo-random binary sequence generator **52** is linearly added to the output of the differentiator **12** in a suitable analogue linear addition circuit **50**. The first sequence is at a very low amplitude level compared to the output of the differentiator **12**. The combined signal from the addition circuit **52** is then passed through a high gain limiting amplifier **54** whose output is a binary signal wherein transitions represent zero-crossings in the input to the amplifier **54**.

The binary output from the amplifier **54** is applied to a modulo two adder **56** as one input thereof. The other input to the adder **56** is a second pseudo-random binary sequence from a second pseudo-random binary sequence generator **58**. The output of the modulo two adder **56** is broadcast by the transmitter **26**, and is completely unintelligible without knowledge of both the first and second pseudo-random sequences. A filter (not shown) may again be provided between the adder **56** and the transmitter **26**.

A form of receiver terminal apparatus suitable for receiving and unscrambling data transmitted by the transmitter apparatus of FIG. **3** is shown in FIG. **4** to which reference will now be made. The output of the receiver **30** is converted to a binary sequence by a high gain limiting amplifier **60**, and this binary sequence forms one input of a modulo two adder **62**. The other input to the adder **62** is the second pseudo-random sequence produced by a sequence generator **64** arranged to produce the same sequence as the generator **58** (FIG. **3**) and synchronised therewith. The output of the adder **62** is passed to a further modulo two adder **66** whose other input is the first pseudo-random sequence, produced by a sequence generator **68** arranged to produce the same sequence as the generator **52** (FIG. **3**) and synchronised therewith. The output of the adder **66** is passed through a low-pass filter **70**, a non-linear circuit **72** which corrects for the inherent non-linearity of the amplitude channel coding, and thence to the combination circuit **42**, the integrator **44**, the low pass filter **46**, and the output transducer **48** (c.f. FIG. **2**). The arrangement of FIGS. **3** and **4** functions as follows:

In the absence of a speech input to the microphone **10** (FIG. **3**), the signal transmitted by the transmitter **26** is the modulo two addition of the first and second sequences. With a very high amplitude speech input, the limiting amplifier **54** is "captured" by it, and the first sequence is suppressed from the output of the amplifier **54** (This arises from the constancy of the power output of the amplifier **54**). Thus the transmitted signal tends towards the limiting case of the modulo two addition of the speech input and the second sequence, as the amplitude of the speech increases.

In the receiver (FIG. **4**) the received signal (the output of the receiver **30**) is limited or "sliced" in the limiting amplifier **60** and then modulo two added to the second sequence. The output of the first adder **62** is in turn modulo two added to the first sequence in the second modulo two adder **66**. In the absence of a speech representative signal in the received signal, the output of the second adder **66** is all "zero," but as the speech level increases and the first sequence is suppressed, the output of the second adder **66** contains an increasing amount of "one" level, until with an infinitely large speech signal, the output of the adder **66** is 50 percent "one" level. When the output of the adder **66** is passed through the low pass filter **70** and the non-linear circuit **72**, the envelope component of the speech is obtained. The combination in the amplitude modulator circuit **42** of this envelope signal, and the zero-crossing signal from the adder **62** results in a signal, which when integrated in the integrator **44** and low pass filtered in the filter **46** (for reasons given with reference to FIG.**2**), causes the output transducer **48** to give an intelligible reproduction of the speech received by the microphone **10**.

In the above described arrangements, a greater degree of scrambling may be obtained by transmitting signals representative of the conjugate, or inverse, of the amplitude envelope, rather than of the actual envelope. This has the additional advantage that it becomes much more difficult, if not impossible, to determine when speech is being transmitted, which would otherwise be indicated by bursts of "noise." Furthermore, there is a signal continuously available for synchronising transmitter and receiver sequence generators.

Although the embodiments above described refer only to two-level or binary signals (when not referring to analogue signals), other numbers of levels in the multi-level signals may be employed; for example three and four level signals may be employed. In these cases, subtraction circuits are required at the receivers in place of the modulo-two adders. (Conversely, subtraction of the pseudo-random sequences may be performed at the transmitters with corresponding addition at the receivers).

Signals other than speech signals may be transmitted as above described, and transmission may be by means other than wireless transmission, for example, by line transmission, as in a telephone system.

Other modifications and variations are possible within the scope of the invention.

I claim:

1. Receiver terminal apparatus for receiving an input signal containing intelligence and delivering as an output signal the intelligence contained in the input signal, the input signal comprising superimposed first and second components, said first component being the scalar combination of a first digital signal having a plurality of possible amplitude levels which occur in a pseudo-random sequence and a second digital signal having a plurality of possible amplitude levels wherein amplitude level transitions represent amplitude datum level transitions in an analogue signal containing said intelligence, said second component representing the amplitude envelope of said analogue signal containing said intelligence, said receiver terminal apparatus comprising

a. first signal generator means to generate a first replica signal which is a replica of said first digital signal,

b. second signal generator means responsive to said input signal to generate a second digital signal which has a plurality of possible amplitude levels and in which transitions between said amplitude levels represent traversals of at least one amplitude datum level by said input signal,

c. first signal combining means to combine said first replica signal with said second digital signal to derive a second replica signal representing said amplitude datum level transitions in said analogue signal,

d. signal processing means to recover a third replica signal which is a replica of said amplitude envelope, and

e. second signal combining means to combine said third replica signal with said second replica signal to form said output signal.

2. Apparatus according to claim **1** in which said signal processing means comprises amplitude envelope detector means coupled to receive said input signal and coupled to said second signal combining means in signal bypass relationship both to said second signal generator means and to said first signal combining means.

3. Apparatus according to claim **1** in which said signal processing means comprises third signal generator means to generate a third digital signal which has a plurality of possible amplitude levels which occur in pseudo-random sequence, third signal combining means to combine said third digital signal with said second digital signal to form a fourth digital signal, and amplitude envelope derivation means coupled to receive said fourth digital signal and to produce said third replica signal therefrom.

4. A speech descrambler comprising

a. means to receive a scrambled speech signal,

b. signal squaring means to square the received scrambled speech signal,

c. a pseudo-random sequence generator,

d. first signal combining means to combine the output of the squaring means with the output of the pseudo-random sequence generator,

e. a further pseudo-random sequence generator,

f. second signal combining means to combine the output of the first signal combining means with the output of the further pseudo-random sequence generator,

g. amplitude envelope derivation means to derive the amplitude envelope from the output of said second signal combining means,

h. third signal combining means to combine the output of said first signal combining means with the output of said amplitude envelope derivation means to produce a descrambled speech signal, and

i. audio transducer means to convert said descrambled speech signal to audible descrambled speech.

5. A speech descrambler according to claim **4** in which said amplitude envelope derivation means comprises series-connected low-pass filter means and non-linear circuit means.

6. A speech descrambler according to claim **4** further including high-frequency de-emphasizing means coupled between said third signal combining means and said transducer means.

7. A speech descrambler according to claim **6** in which said high-frequency de-emphasizing means comprises signal integrator means.

8. A speech descrambler according to claim **4,** further including noise and spurious high-frequency signal component suppression means coupled between said third signal combining means and said transducer means.

9. A speech descrambler according to claim **8,** in which said suppression means is a low-pass filter.

10. A communication system for transmitting the intelligence of an intelligence containing signal having components of variable frequency and variable amplitude, said intelligence containing signal frequently traversing at least one amplitude datum level including zero amplitude, said intelligence containing signal having an amplitude envelope, said system comprising:

i. a transmitter terminal;

ii. a receiver terminal; and

iii. a communication path between said transmitter and receiver terminals;

iv. said transmitter terminal comprising:

a. first signal generator means to generate a first digital signal having a plurality of possible amplitude levels which occur in pseudo-random sequence;

b. second signal generator means responsive to said intelligence containing signal to generate a second digital signal which has a plurality of possible amplitude levels and in which transitions between said amplitude levels represent traversals of said at least one amplitude datum level by said intelligence containing signal;

c. first signal processing means comprising a first scalar combination means to effect scalar combination of the first digital signal and the second digital signal to form a first component of an output signal of the transmitter terminal;

d. second signal processing means comprising amplitude envelope processing means for processing said amplitude envelope separately from said second digital signal to form a second component of the output signal of the transmitter terminal;

e. means to include said second component in the output signal of said transmitter terminal with said first component; and

f. means to transmit said output signal along said communication path to said receiver terminal;

v. said receiver terminal comprising:

a. means to receive the transmitter terminal output signal as a receiver terminal input signal;

b. third signal generator means to generate a first replica signal which is a replica of said first digital signal;

c. fourth signal generator means responsive to said receiver terminal input signal to generate a third digital signal which has a plurality of possible amplitude levels and in which transitions between said amplitude levels represent traversals of at least one amplitude datum level by said receiver terminal input signal;

d. first signal combining means to combine said first replica signal with said third digital signal to derive a second replica signal representing said amplitude datum level transitions in said intelligence containing signal;

e. third signal processing means to recover a third replica signal which is a replica of said amplitude envelope; and

f. second signal combining means to combine said third replica signal with said second replica signal to form an output signal containing the intelligence that was in said intelligence containing signal.

11. A system according to claim **10** in which said second signal processing means comprises bypass means to couple the amplitude envelope signal directly to said means to include said second component in the transmitter terminal output signal, in signal bypass relationship both to the second signal generator means and to the first signal processing means.

12. A system according to claim **10** in which the amplitude envelope processing means of said second signal processing means comprises a fifth signal generator means to generate a fourth digital signal which has a pluraity of possible amplitude levels which occur in pseudo-random sequence, and a further combination means to effect combination of the fourth digital signal with the amplitude envelope signal to form said second component.

13. A system according to claim **10** including circuit means through which the input signal is passed to increase the amplitude datum level transition rate.

14. A system according to claim **11** in which said third signal processing means comprises amplitude envelope detector means coupled to receive said receiver terminal input signal and coupled to said second signal combining means in signal bypass relationship both to said fourth signal generator means and to said first signal combining means.

15. A system according to claim **12** in which said third signal processing means comprises sixth signal generator means to generate a fifth digital signal which has a plurality of possible amplitude levels which occur in pseudo-random sequence, third signal combining means to combine said fifth digital signal with said third digital signal to form a sixth digital signal, and amplitude envelope derivation means coupled to receive said sixth digital signal and to produce said third replica signal therefrom.

16. A speech scrambler/descrambler system comprising microphone means, a first pseudo-random sequence generator, first signal combining means to combine the output of the microhphone means with the output of the first pseudo-random sequence generator, first signal squaring means to square the output of said first signal combining means, a second pseudo-random sequence generator, second signal combining means to combine the output of the signal squaring means with the output of the second pseudo-random sequence generator to produce a scrambled speech signal, means to receive the scrambled speech signal, second signal squaring means to square the received scrambled speech signal, a third pseudo-random sequence generator, third signal combining means to combine the output of the second squaring means with the output of the third pseudo-random sequence generator, a fourth pseudo-random sequence generator, fourth signal combining means to combine the output of the third signal combining means with the output of the fourth pseudo-random seqence generator, amplitude envelope derivation means to derive the amplitude envelope from the output of said fourth signal combining means, fifth signal combining means to combine the output of said third signal combining means with the output of said amplitude envelope derivation means to produce a descrambled speech signal, and audio transducer means to convert said descrambled speech signal to audible descrambled speech.

17. A system according to claim **16** in which high-frequency enphasizing means is coupled between said microphone means and said first signal combining means.

18. A system according to claim **16** in which said amplitude envelope derivation means comprises series-connected low-pass filter means and non-linear circuit means.

19. A system according to claim **16** further including high-frequency de-emphasizing means coupled between said fifth signal combining means and said transducer means.

20. A system according to claim **16** further including noise and suprious high-frequency signal component suppression means coupled between said fifth signal combining means and said transducer means.

* * * * *