1,172,971

PATENT SPECIFICATION

DRAWINGS ATTACHED

1,172,971

Date of Application and filing Complete Specification: 29 May, 1962.

No. 20697/62.

Application made in Netherlands (No. 265358) on 31 May, 1961.

Complete Specification Published: 3 Dec., 1969.

Index at acceptance: —**H4** P(B1, B2, B6A, B6Y, B9, E9, N1, S1); **G4** D1B3

International Classification: —**H 04 l 9/04**

COMPLETE SPECIFICATION

Secrecy Communication System

We, NEDERLANDSE ORGANISATIE VOOR TOEGEPAST - NATUURWETENSCHAPPELIJK ONDERZOEK TEN BEHOEVE VAN DE RIJKSVERDEDIGING, of 22 Wassenaarseweg, The Hague, The Netherlands, a corporate body duly organised and existing under the laws of the Netherlands, do hereby declare the invention, for which we pray that a patent may be granted to us, and the method by which it is to be performed, to be particularly described in and by the following statement:—

The present invention relates to a secrecy communication system, in which for the enciphering of messages consisting of numerically coded signals each of which signals is formed by a group of code elements having discrete values, use is made of an interference pattern equally known to transmitter and receiver comprising a limited number of code elements, which elements are arranged according to the same time frame as the code groups of the plain message.

Such a system is known from British patent specification No. 694,757.

The interference pattern used in this invention is produced with the aid of a number of electronic cyclically operating circuits. Because these cyclically operating electronic circuits form an analogue of a rotating wheel, these circuits are referred to as electronic wheels.

Each of these wheels has a number of positions. These numbers may be different for all the wheels and in that case preferably have no common divisor. Each electronic wheel produces an adjustable zero-one pattern, the number of the ones of which added to the number of its zeros equals the number of the positions of the wheel. These patterns are called sub-patterns.

One customary method consists in adding up the sub-patterns with the aid of a logical circuit according to the rules; an even number of ones is taken as a zero, an odd number of ones is taken as a one. The pattern obtained by this addition is used as the interference pattern, both when all the wheels step on regularly independently of each other in which case the numbers of positions are different, as also when the stepping along of some wheels is determined by the casual combination of ones and zeroes of sub-patterns produced by the wheels.

A second known method consists in using the combinations of ones and zeroes of the wheels that move independently of or in dependency of each other as the adjusting combination for an auxiliary device which produces the characters for the interference pattern.

The application of such an interference pattern has two drawbacks, both of which are caused by the fact that the interference patterns of the transmitter and of the receiver must have passed through an equal number of positions, if the receiver is to be able to decipher the message.

The first drawback is that an electronically operating receiver does not contain any correct data about the number of positions passed through if the supply voltage has momentarily been cut off or if interfering pulses have put one or more of the electronic wheels in an incorrect position.

The second drawback is that, when taking part in a secrecy communication network, all the subscribers must at one and the same time start going through the positions of the interference pattern starting from identical starting positions.

It would be possibly partly to remove these drawbacks by inserting a set to zero code group into the crypto signal at certain determined times, the occurrence of which code group would cause both transmitter and receiver to bring their interference patterns

[*Price 4s. 6d.*]

into a predetermined position, called zero position. In cases in which much disturbance is caused by local interfering pulses endangering the synchronous development of the interference patterns, the said set to zero code group could be inserted a few times in each cycle period of the interference pattern. This causes a shortening of the effective length of the interference pattern. By this shortening of the effective length of the interference pattern the method according to which zero set code groups set the pattern in a predetermined position is unsuitable for secrecy communication systems. By inserting at appointed times, a set to zero code group for each sub-pattern instead of one set to zero code group for the pattern, it is possible to achieve that the effective length of the interference pattern is not shortened, whilst a faulty position, of one or more quickly corrected wheels is occurring, is quickly corrected all the same. However, in a crypto-signal, in which all sorts of binary combinations are being used as crypto-code groups, there are no free code groups left which could be used as set to zero code groups.

The insertion is set to zero code groups in a crypto-signal, in which some code groups are still free, would cause the efficiency of the connection to go down considerably.

The present invention enables all these drawbacks to be removed by giving to some of the code groups occurring in the crypto-signal the significance of set to zero code groups.

At least one set to zero code group is provided for each wheel. Different set to zero code groups are provided for different wheels. In this manner, each wheel is, independently of the others, brought into the zero position at certain points of time determined by statistical laws.

This employment of the setting to zero of the wheels brings about a preference for those combinations of the sub-patterns for which one or more of the wheels are in the zero position, so that not all the code groups of the interference pattern have the same probability of occurring. This is unavoidable, but the effect is not disturbing if care is taken that each wheel on the average completes at least one entire revolution between two consecutive set to zero commands.

After a set to zero at least one of the wheels is in a predetermined (zero) position, whereas the others can be in any one of the possible positions.

Assuming that the numbers of the positions of the different wheels have no common divisor, the total number of positions the wheels are stepped through without zero set equals the product of the numbers of the positions of all the wheels. If there are m wheels having $k_1, k_2, \ldots . k_m$ positions the total number of positions will be the product $k_1, k_2, k_3 \ldots . k_m$, or in a conventional notation

$$\prod_{k=1}^{m} \pi^{n}_{k}$$

when the wheels are stepped regularly, the series of ones and zeroes will be periodic.

In thic case the pattern is periodic and all positions are reached consecutively, and the pattern is repeated after $\prod_{k=1}^{m} \pi^{n}_{k}$ steps

When zero set is introduced the wheels after each zero set will start from one of the positions indicated above and from that position a fragment of the periodic pattern will be reproduced until a new zero set is commanded and the pattern jumps to an other fragment of the periodic pattern. So the pattern consists if a number of fragments of the periodic pattern. The length of these fragments is variable as the occurrence of the next zero set depends on probability factors. These fragments have their beginning at one of the positions of the above group I and it can be shown that the total number of these fragments is equal to

$$\prod_{k=1}^{m} \pi^{n}_{k} - \prod_{k=1}^{m} (\pi^{n}_{k} - 1) = N$$

So the pattern consists of N fragments of the periodic pattern which are distributed randomly in the periodic pattern: moreover, the length of these fragments is subject to probability factors.

It will be clear, that by introducing the zero-set in all sub-patterns a non-periodic pattern of indefinite length is obtained, and that the pattern is different for different messages.

If it is required to choose the probability of the occurrence of a set to zero code group in deviation from the probability of the occurrence of a code group in the crypto-signal, the significance of a set to zero command can be given to any combination of elements in the crypto-code groups. For instance, by giving the significance of set to zero command to a determined code group and to a determined value of the first element of the next code group in a crypto-telex code, a probability amounting to $\frac{1}{64}$ of the occurrence of the set to zero is obtained if the crypto-signal is statistically homogeneous. In this latter case it was further demanded that the six elements should be positioned on the first to fifth place inclusive of one code group and on the first place of the next code group. By dropping this demand and by considering six elements to be found in consecutive informa-

tion positions in the cryptosignal, an entirely different probability of the occurrence of the set to zero command is obtained. From this, it is apparent that there is a measure of freedom in choosing the probability of the occurrence of a set to zero command.

At the occurrence according to determined statistical laws of a combination of elements in the crypto-signal to which is also given the significance of a set to zero command both the transmitter and the receiver bring the electronic wheel, for which the pertinent command is meant, into the zero position, starting from which it subsequently passes through its positions in the normal way.

The effect of the aforesaid set to zero commands is that, at the end of an interval of time the mathematical expectation of which can be calculated, at least one set to zero command has occurred for each of the electronic wheels, so that after this the interference patterns both of the transmitter and of the receiver which has observed the signal during the said interval of time, simultaneously take up identical positions.

An example is given hereinafter of a circuit in which the wheels are set to zero at points of time which are co-determined by statistical laws. In the explanatory part of this specification this is for convenience sake indicated as "statistical set to zero".

The interference pattern is here composed of three sub-patterns, having 8, 11 and 13 positions respectively. The interference pattern has 8.11.13=1144 positions.

The sub-pattern having 8 positions is produced by an electronic wheel comprising three triggers X, Y, Z which have complementary output voltages x,x', y,y' and z,z', each of which can have the assigned values 1 and 0.

The triggers XYZ are connected as a three-stage binary counter. The voltages x x', y y' and z z' are complementary voltages and the values 1 and 0 can be assigned to them.

X is the trigger which is least in value and Z is highest in value. This means that, if pulses are fed to the counter, the following combinations will occur xyz, x'yz, xy'z, x'y'z, xyz', x'yz', xy'z', x'y'z'.

These combinations of voltages are fed to the inputs of 8 AND gates.

As in only one of the combinations at a time all three voltages can have the value 1, the AND gates will successively transmit a pulse to the conductor 7 if the switch between the output of this gate and the conductor is closed.

By opening the appropriate selection of switches any of the possible subpatterns of pulses and no pulses (ones and zeroes) can be produced.

The described method for exciting a quasi random series of ones and zeroes is a conventional one and forms no part of the present invention. Such a method is represented by the sum of eight logical products.

$$F_8=f_1xyz + f_2x'yz + f_3xy'z + f_4x'y'z + f_5xyz' + f_6x'yz' + f_7xy'z' + f_0x'y'z'$$

in which f_0 to f_7 inclusive have the value 1 for a switch which is closed and the value 0 for an open switch and in which F_8 is the subpattern. The eight products mutually exclude each other, which means that, if a randomly chosen product is 1, all the others are zero. Each of the subpatterns having 11 and 13 positions is produced by an electronic wheel comprising four triggers the output voltages of which are x,x', y,y', z,z' and w,w'. The trigger W is the trigger which has the highest value. The counter for 11 positions is connected in such a way that, after the positions xyzw=1111 to x'yzw'=1111 inclusive have been passed through in a binarily ascending way, the position x'y'z'w'=1111 follows, after which the cycle is repeated again from xyzw=1111 on. The jumping of the positions xy'zw=1111 to x'y'z'w'=1111 inclusive is effected with the aid of an AND gate, which, if the condition x'.y.z.w.=1 is fulfilled, admits the next clock pulse to the triggers Y and Z, so that these are brought into positions y'=1 and z'=1. Simultaneously, a gate, which is closed if the condition (x'.y.z.w'=0 is fulfilled, blocks the entrance to the clock pulse input of the counter for clock pulse.

The counter for 13 positions passes through the positions xyzw=1111 to x'y'zw'=1111 inclusive in normal binary order. An AND gate, which is exclusively open at the condition x'.y'.z.w'=1, admits the clock pulse to the trigger Z. Simultaneously, a gate, which is closed if the condition (x'.y'.z.w')'=0 is satisfied, blocks the entrance of the clock pulse to the clock pulse input of the counter. As a result of these measures the next position of the counter is x'y'z'w'=1111, after which the cycle repeats itself.

The sub-patterns F_{11} have 11 positions, and F_{13} having 13 positions are represented by the sum of 11 and 13 logical products.

$$F_{11}=f_1xyzw + f_2x'yzw + f_3xy'zw + f_4x'y'zw + f_5xyz'w + f_6x'yz'w + f_7xy'z'w + f_8x'y'z'w + f_9xyzw' + f_{10}x'yzw' + f_0x'y'z'w'$$

$$F_{13}=f_1xyzw + f_2x'yzw + f_3xy'zw + f_4x'y'zw + f_5xyz'w + f_6x'yz'w + f_7xy'z'w + f_8x'y'z'w + f_9xyzw' + f_{10}x'yzw' + f_{11}xy'zw' + f_{12}x'y'zw' + f_0x'y'z'w'$$

Out of the three sub-patterns F_9, F_{11} and F_{13} the pattern F is determined by means of addition without carry. As logical-algebraical indication for addition without transmission use is made of the formula

$$A \oplus B \oplus C = AB'C + A'BC + A'B'C + ABC$$

it appears that the pattern F can be obtained by employing four AND gates having three inputs each and one OR gate having four inputs.

In the foregoing, during the change from the position x'yzw=1111 in the sub-pattern having 11 positions and from the position x'y'zw'=1111 in the sub-pattern having 13 positions respectively, the clock pulse is admitted only to those triggers which were not in the position corresponding to x'y'z'w'=1111. However, it makes no difference to the correct functioning of the circuit, if in the above-quoted cases the clock pulse is admitted to the four triggers X Y Z W in such a way that they are forced into the positions x'=1 y'=1 z'=1 w'=1.

Advantage is taken of this possibility, when statistical set to zero ought to take place, for admitting the next clock pulse to the triggers X Y Z W, in such a way as to force them into the positions x'=1 y'=1 z'=1 w'=1, whilst at the same time the entrance of the clock pulse to the clock pulse input of the counter is blocked.

In the example use is made of an encrypted telex signal having 5 elements. If in this crypto signal the combination of elements occurs which in the European telex code No. 2 is called K, the sub-pattern having 13 positions is brought into the zero position x'y'z'w'=1111. At the occurrence of the character Q the sub-pattern having 11 positions is brought into the position x'y'z'w'=1111. At the occurrence of the character U the sub-pattern having 8 positions is brought into the position x'y'z'=111. When writing 0 for an element having space polarity and 1 for an element having mark polarity, the sequential code is

K 1 1 1 1 0

Q 1 1 1 0 1

U 1 1 1 0 0

At the crypto-signal, in which each character has a probability of $\frac{1}{32}$ the probability for statistical set to zero is $\frac{1}{32}$ for each of the sub-patterns. In the example this probability is increased to $\frac{2}{32}$.

$$F = F_9 \oplus F_{11} \oplus F_{13}$$

By applying the arithmetical rule

This is achieved by having only the second to fifth elements inclusive of each combination act as set to zero commands. So the zero commands in this case are

1 1 1 1 0

and

0 1 1 1 0

for the sub-pattern having 13 positions

1 1 1 0 1

and

0 1 1 0 1

for the sub-pattern having 11 positions

1 1 1 0 0

and

0 1 1 0 0

for the sub-pattern having 8 positions.

The set to zero commands are recognized by passing all the characters of the crypto-signal at the transmitter as well as at the receiver side, through a seven-stage shift register. At the moment at which the start element is in the last stage and the stop element in the foremost stage, the elements in the stages from two to six inclusive are the elements from one to five inclusive of one and the same character. This moment is known owing to a synchronizing circuit of conventional type, which will not be discussed in this specification. If the elements from two to five inclusive are successively called b, c, d, e, and the moment at which the stop and start elements are in the correct place is called n, then the conditions for statistical set to zero are

(n.b.c.).d.e'=1

(n.b.c.).d'.e=1

(n.b.c.)d'.e'=1 respectively.

The condition n.b.c.=1, hereinafter to be called a=1, is realized with the aid of an AND gate having three inputs.

The conditions

a.d.e'=1 a.d'.e=1 and a.d'.e'=1

are realized by three AND gates having three inputs each.

The circuit according to the given ex-

ample is further explained with the aid of the accompanying drawings.

With the aid of Figure 1, the functions of some symbolical circuits, which are used in the Figures 2 to 6 inclusive, are more fully explained.

Figures 2 to 5 inclusive represent a circuit which is used for producing the interference pattern with set to zero.

Figure 6 represents a circuit for the derivation of the set to zero commands.

In Figure 1, 1 is a trigger T having output voltages t and t'. A pulse gate 2 allows a pulse supplied at point 3 to appear on the trigger 1, if the gate voltage 4 has the value 1, and blocks the entrance for the pulse to the trigger if the gate voltage has the value 0. Pulse gates 5 operate in the same way as the pulse gate 2. The pulse gates 2 and 5 operate completely independently of each other. An appearing pulse brings the trigger in such a position that the output voltage on the side from which the pulse was applied has the value 0.

An AND gate 6 supplies a voltage 7 having the value 1 only if all the input voltages 8 have the value 1, and in all other cases a voltage having the value 0. An OR gate 9 supplies a voltage 10 having the value 0 only if all the input voltages 11 have the value 0, and in all other cases a voltage having the value 1. An inverter circuit 12 emits a signal 13, which is equal to the inverted input signal 10.

Figure 2 shows a circuit for the sub-pattern having 8 positions. The triggers 1, 2 and 3 form a binary counter. The eight AND gates 5 represent a diode matrix having six incoming and eight outgoing lines. The switches 6 are adjusted in accordance with the desired sequence of ones and zeroes of the cyclic sub-pattern. The desired sub-pattern appears at the output of the OR gate 7 and is inverted by the inverter 8. If, consequentially to the occurrence of a character to which for the sub-pattern having eight positions the significance of a set to zero command is given, the condition $a.d'.e'.=1$ is fulfilled, the AND gate 14 is opened, which causes the pulse gates 9 to be opened too, whilst owing to the inverter 10 the admission of the clock pulse 11 to the clock pulse inputs 12 and 13 of the trigger 1 of the counter is blocked.

In Figure 3, a diagram for the development of the sub-pattern having 11 positions is given. An OR gate 16 and an AND gate 15 are in deviation with respect to the diagram in Figure 2. An AND gate 14 corresponds to the AND gate 14 in Figure 2. The AND gate 15 is provided for the purpose of reducing the positions of the counter from 16 to 11. Set to zero takes place if $a.d'.e=1$ or if $x'.y.z.w'=1$ or if both these occurrences coincide.

Figure 4 represents the diagram of the sub-pattern having 13 positions.

Figure 5 represents the addition without carry of the three sub-patterns.

Figure 6 represents a shift register comprising triggers 20 to 26 inclusive. The cryptotelex signal is supplied to a terminal 27 and inverted with the aid of an inverter 28. The cross-connections between the triggers of the shift register bear relation to the fact that the output voltage of a trigger assumes the value 0 at the side where a pulse appears. The shift pulses 11 are the same as the clock pulses 11 in Figure 2, 3 and 4.

The shift pulses 11 are derived from a synchronizing circuit not shown in the drawing. The shift pulses are timed in such a way with respect to the elements of the signal 7 which are fed to the terminal 27 that the said elements are scanned approximately in the centre. The synchronizing circuit also produces a gate voltage 30 which has the value 1 from the moment at which the shift pulse places a stop element in the trigger 20 till the moment at which the next shift pulse occurs. The AND gate 29 supplies the gate voltage $a=n.b.c.$ for the benefit of the AND gates 14 in the Figures 2, 3 and 4.

WHAT WE CLAIM IS:—

1. A secrecy communication system operating with binary coding, in which a plain message is enciphered by an interference pattern of finite length, which is determined by a number of sub-patterns all of which have different numbers of elements, in which each sub-pattern is produced by an electronic circuit, wherein for each of the sub-patterns electronic means are provided to put these sub-patterns in a predetermined (zero) position at the occurrence of certain determined groups of elements which occur in the enciphered message and which can be chosen as desired.

2. A secrecy communication system substantially as described with reference to the accompanying drawings.

ELKINGTON & FIFE,
Chartered Patent Agents,
Bank Chambers, 329, High Holborn,
London, W.C.1,
Agents for the Applicants.

Printed for Her Majesty's Stationery Office by the Courier Press, Leamington Spa, 1969.
Published by the Patent Office, 25, Southampton Buildings, London, W.C.2, from which copies may be obtained.

1172971 COMPLETE SPECIFICATION
4 SHEETS *This drawing is a reproduction of the Original on a reduced scale*
Sheet 1

FIG.1

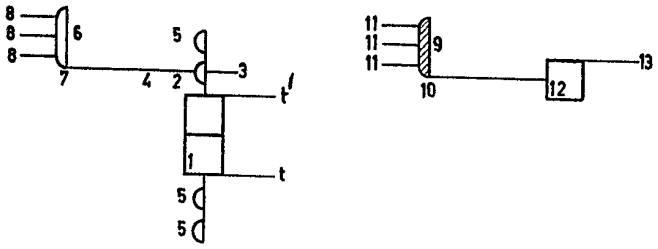


FIG.5

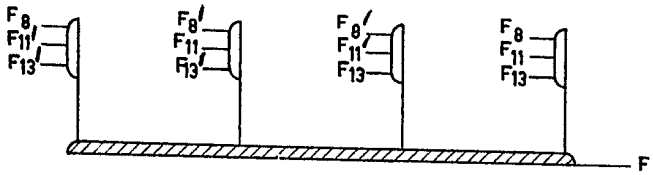


FIG.6

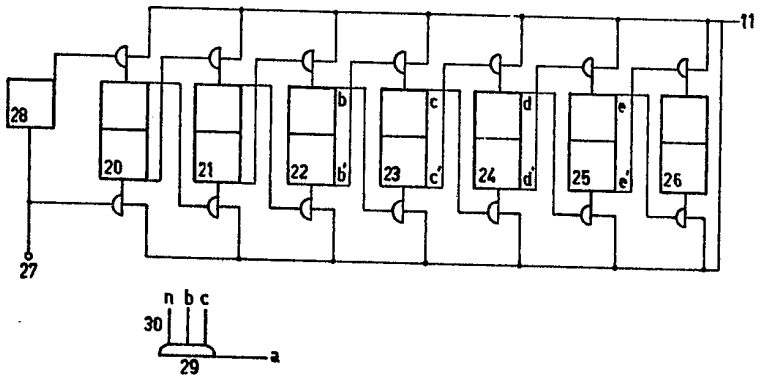
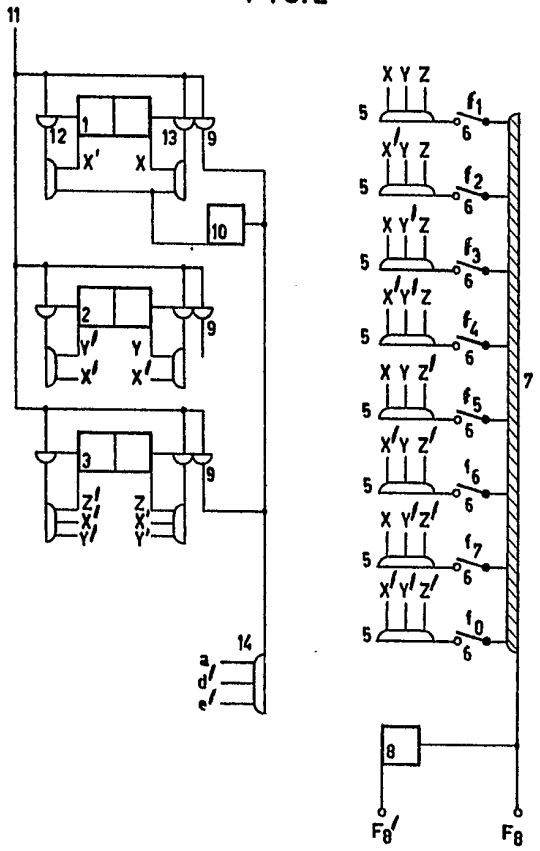
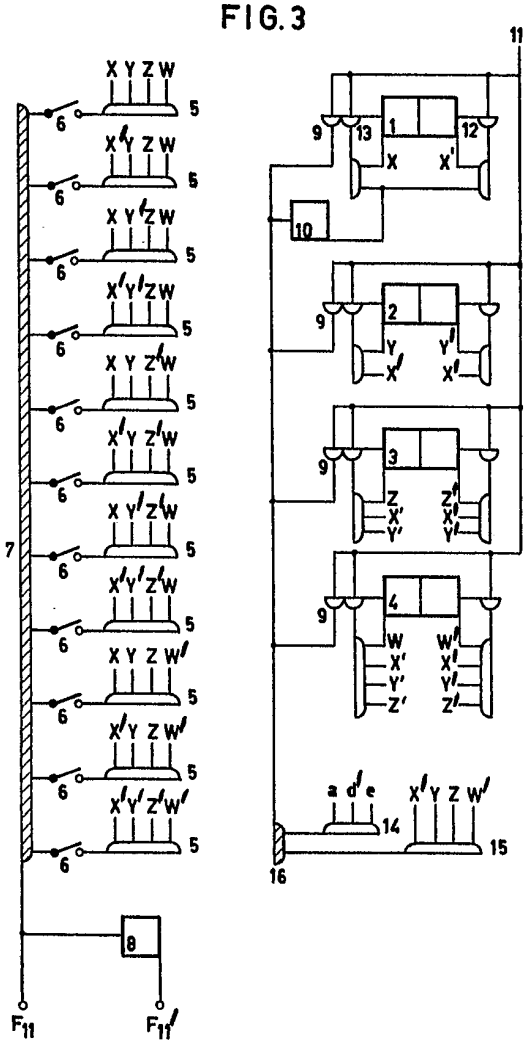


FIG.2


11
12
1
13
9
X'
X
10
2
Y'
Y
X'
X'
3
Z'
X'
Y'
Z
X'
Y'
14
a'
d'
e'
X Y Z
X' Y Z
X Y' Z
X' Y' Z
X Y Z'
X' Y Z'
X Y' Z'
X' Y' Z'
5
6
f1
f2
f3
f4
f5
f6
f7
f0
7
8
F8'
F8

1172971 COMPLETE SPECIFICATION
4 SHEETS *This drawing is a reproduction of the Original on a reduced scale*
Sheet 3

FIG. 3



1172971 COMPLETE SPECIFICATION
4 SHEETS *This drawing is a reproduction of the Original on a reduced scale*
Sheet 4

FIG. 4