PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

EP 11.615

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification: G09C 1/00; H04L 9/00	A1	(11) International Publication Number: WO 79/00418
		(43) International Publication Date: 12 July 1979 (12.07.79)

(21) International Application Number: PCT/SE78/00100

(22) International Filing Date: 20 December 1978 (20.12.78)

(31) Priority Application Number: 7714587-8

(32) Priority Date: 21 December 1977 (21.12.77)

(33) Priority Country: SE

(71) Applicant: BRÄNDSTRÖM, Hugo; 22, Johan Enbergs väg, S-171 91 Solna, Sweden.

(72) Inventor: Applicant is also the inventor.

(74) Agent: AB STOCKHOLMS PATENTBYRÅ, ZACCO & BRUHN; Box 3129, S-103 62 Stockholm, Sweden.

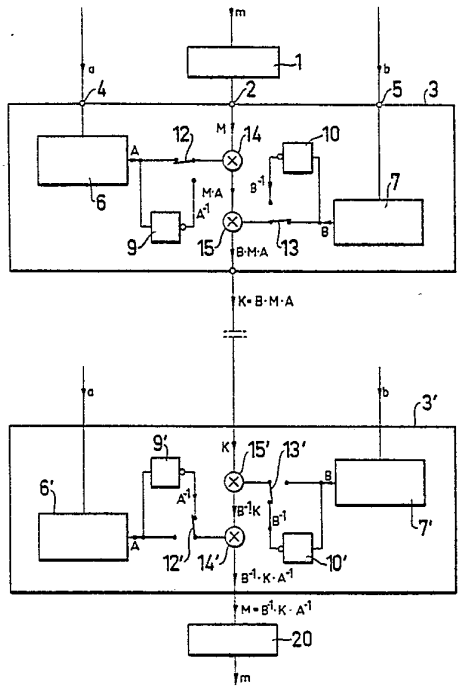
(81) Designated States: CH (European patent), DE (European patent), DK, FR (European patent), GB (European patent), JP, US.

Published with:
International search report

(54) Title: METHOD AND DEVICE FOR ENCRYPTION AND DECRYPTION

(57) Abstract

Encryption and decryption of information of a message is performed by partitioning a plaintext message into blocks of binary digits and by further partitioning said blocks into subblocks which are interpreted as elements in a Galois-field. A plaintext matrix (M) of said elements is multiplied by a first key matrix (A) of a group over said Galois-field, the resulting product (M·A) being multiplied by a second key matrix (B) of the same group over said Galois-field. The final product (B·M·A) thus received constitutes the encrypted message block (K). Decryption is performed by multiplying the transmitted product (B·M·A) by inverse key matrices (A^{-1}, B^{-1}) generated by the same keys (a, b) as used for decryption and taken in the proper order.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT

AT	Austria	LU	Luxembourg
BR	Brazil	MC	Monaco
CF	Central African Empire	MG	Madagascar
CG	Congo	MW	Malawi
CH	Switzerland	NL	Netherlands
CM	Cameroon	SE	Sweden
DE	Germany, Federal Republic of	SN	Senegal
DK	Denmark	SU	Soviet Union
FR	France	TD	Chad
GA	Gabon	TG	Togo
GB	United Kingdom	US	United States of America
JP	Japan		

Method and Device for Encryption and Decryption

Technical field

The present invention refers to a method of encryption of data using one or more encryption keys and the same keys for decryption. The invention also refers to a device for the realization of said method.

The cryptosystem shall be able to work according to the principles for ciphers dependent or independent of the unenciphered text (the plaintext).

The cipher independent of the plaintext is distinguished by a usually very long sequence of key symbols, consisting of zeros and ones, being added modulo-2 to the plaintext which is also a sequence of zeros and ones.

Background art

As an example of this kind of ciphers may be mentioned form ciphers in which the complete sequence of key symbols constitutes the key. This kind of encryption, for example, has been implemented within defence organizations. The drawback of a form cipher is that keys are comsumed at the same rate as that of the information being transmitted. Also, the keys which may be stored on a disc memory both at the transmitter end and at the receiver end of the information, has to be deposited for safe-keeping.

For making the circumstantial handling of keys needed unnecessary when form ciphers are being used, the key sequences are often generated by use of feedback shift registers. The sequences of zeros and ones generated by such

a shift register have a character that makes them very similar to randomly generated sequences, and they are often called pseudo-random sequences. Such a sequence is completely determined by the values stored in the shift register at the start. This content in the register is in the following called the key. Thereby, the key will be very short in comparison with the key sequences generated by the shift register, thus considerably simplifying the handling of the key as comparad to corresponding problems when using a form cipher.

However, one drawback when using a feedback shift register is that the resistivity against breaking the enciphered information is very unfavourable. If a part of the plaintext and the corresponding enciphered text are known, the length of which needs only be two times the length of the shift register, the key may be determined by solving a system of linear equations.

Different ways have been considered to introduce non-linear operations upon the bits in the key sequence generated by a feedback shift register in order to increase the resistivity. For this purpose, also more than one shift register may be used for enabling the connecting together of the outputs of different registers in a non-linear way for the generation of a new key sequence to be used in modulo-2 additions of the symbols in the plaintext.

It may be proved mathematically that the key sequence generated in such a way in most cases may be generated by an equivalent linear shift register. Therefore, it is always difficult to guarantee sufficient resistivity against code breaking when such methods are used.

In order to secure high resistivity it is therefore necessary to use ciphers which are dependent on the plaintext. One such cipher developed by the International Business Machines Corporation (IBM) in the U.S.A. to be used by the Federal Authorities in U.S.A. according to Federal Information Processing Standards Publication No. 46, January 15, 1977, has been suggested by the National Bureau of Standards (NBS) in the U.S.A. This cryptological standard is denoted Data Encryption Standard (DES). Said system is shown in Fig. 1 of the present specification.

According to this system the plaintext is partitioned

into blocks M consisting of 64 bits. These bits are as a first step permuted according to a fixed permutation schedule which is dependent on the 16 key words K_1, K_2 .. K_{16} defined by a KEY consisting of 64 bits, 8 of which are parity check bits. After permutation the block is partitioned into two blocks, a left block L_0 and a right block R_0, each one consisting of 32 bits. This is followed by an iteration process in 16 steps, defined by the relations

$$L_n = R_{n-1}$$
$$R_n = L_{n-1} + f(R_{n-1}, K_n) \qquad n = 1, 2 \ldots 16$$

where f is a non-linear function mapping R_{n-1} and the keyword K_n into a 32-bits block which is added modulo-2 to L_{n-1}. The keyword K_n consists of 48 bits and depends on KEY and the iteration step n defined by a function KS:

$$K_n = KS(n, KEY).$$

In the last step $L' = R_{16}$ and $R' = L_{16}$ are combined into a 64-bits block

$$M' = L'R'$$

which is subjected to a permutation defined to be the inverse of the permutation of M as discussed earlier. As a result of this last permutation the enciphered block KB is obtained.

Decryption is effectuated by passing KB through an identical device with the same key KEY, but in order to obtain the correct order with

$$K_n = KS(17-n, KEY).$$

Each bit of the enciphered block KB is depending on all the bits in the plaintext block M. The DES system copes with relatively high demands for the resistivity against breaking the ciphertext since the only way known today for breaking it is to try different keys in a decryption device, and to look for meaningfull plaintexts in the outputs when the enciphered blocks are applied to the inputs. The number of possible keys KEY is 2^{56}, or about 10^{17}.

The DES system also copes with the demands for high rates of encryption and decryption since it may be realized in hardware using LSI chips, and said chips are already available on the market.

In spite of these qualities the DES system has been criticized in several instances (cf. the "Communications of the ACM" vol. 19(1976):3 ,March, pp. 164 to 165). This criticism

maintains that the resistivity will not be sufficient in the future (about the year 1990), depending on the rapid development of minicomputers and microcomputers and the downward trends of the costs of computations. Before the year 1990 it might be necessary to change said standard crypto, implying heavy expenses and much labour. The DES system is namely not flexible enough in this respect, w ich is also a disadvantage in another respect: it will not be possible to adjust it to fit special applications.

Another problem which is inherent in all plaintext depen dent crypto systems proposed until now is that a one-bit-error in the transmission of the enciphered block normally implies that all the bits in the deciphered block will be affected. This might possibly be tolerated if a purely linguistic message is transmitted, but can not be tolerated if the message concerns numerical data.

One way to avoid this drawback is to let the plaintext block contain a password which has to be identified by the receiver before the block is approved.

As a summary of drawbacks of known crypto systems connected to data communication or data storing, it may be established that:

1. Plaintext independent ciphers have low resistivity against breaking. Form ciphers constitute an exception. However, they require extremely long key strings, the handling of which meets with difficulties.

2. Plaintext dependent ciphers are "stiff". They are rather expensive to change if the resistivity against breaking is regarded to be insufficient.

3. Plaintext dependent ciphers require passwords within the plaintext blocks in order that errors in the transmission caused by noise may be detected.

The invention

The object of the invention is to avoid said drawbacks of plaintext dependent ciphers and to obtain a possibility of adapting the system to existing applications including databanks, data communication and speach communication.

According to the invention encryption is performed by partitioning the characters of a plaintext message into blocks of binary digits, each such block being further partitioned into subblocks, each of which is to be possible to interpret as an element in a Galois-field. Said elements are brought to generate a plaintext matrix which is multiplied from the right in a first matrix multiplier by a first key matrix belonging to a prescribed matrix group over said Galois-field and being generated by means of a first encryption key which is applied to a first matrix generator, the output of which is multiplied from the left in a second matrix multiplier by a second key matrix belonging to the same matrix group and being generated by means of a second encryption key which is applied to a second matrix generator. The output from said last-mentioned generator constitutes the encrypted plaintext block which is thereafter transmitted to a receiver where it is to be decrypted.

For the purpose of decryption said plaintext block is multiplied from the left in a third matrix multiplier by a third key matrix being the inverse of the second key matrix and being generated by means of the second encryption key which is applied to a third matrix generator. The output of said generator is then multiplied from the right in a fourth matrix multiplier by a fourth key matrix being the inverse of the first key matrix and being generated by means of the first encryption key which is applied to a fourth matrix generator. The output from said last-mentioned generator constitutes the restored original plaintext matrix, and after decoding the original plaintext block will be received.

Thus, in a simple way, the invention allows a receiver to decide if a received message is correctly received or not. Furthermore, the cryptosystem according to the invention is suitable as a means for encryption and decryption of both stored data and data used in communication. The system is readily realizable by means of integrated circuits.

The system according to the invention is further characterized by great resistivity against breaking, and it renders it possible to use algorithms for encryption and for decryption. The implementation is technically simple and cheap.

The demand for resistivity against breaking strongly depends on the actual application, but is especially high in connection with the processing of stored information, when in extreme cases it is necessary for the cryptosystem to resist breaking during 50 years, independently of the breakers access to technical facilities and to the unknown development of technology.

Fast algorithms are especially important in connection with data communication where multiples of 9600 bits/s may be required, and in connection with digitalized speech communication where transmission rates of even more than 20000 bits/s seem to be necessary. In computers connected to data terminals transmission rates of 10^6 bits/s (= 1 Mbits/s) are realistic values. The object of the present invention is further to make such applications possible.

Theory underlying the invention

The method of encryption and decryption according to the invention is founded on the use of matrices belonging to matrix groups with elements belonging to Galois-fields. Accordingly, a short review will be given of the properties of such fields. Further information may be drawn from the book "An Introduction to Error-Correction Codes" by Shu Lin, Prentice-Hall, London.

A Galois-field ($GF(p^r)$) contains p^r elements, where p is a prime number and r is an arbitrary positive integer. Two arbitrary elements in $GF(p^r)$ may be added or multiplied, and the result of such operations will be -usually other- elements in the field. A Galois-field also contains a unit as regards addition (denoted 0), implying that $0+1=a$ for all a in the field, and a unit as regards multiplication (denoted 1), implying that $1 \cdot a = a$ for all a in the field. For each a and b in a Galois-field the equation $a+x=b$ always has a solution in the field which is $x=b-a$. Also, for each $a \neq 0$ and each b in the Galois-field, the equation $a \cdot y = b$ always has a solution in the field which is $y=b/a$. The set of elements differing from 0 in the Galois-fields has the character of a cyclic group, implying that each such element in the field can be interpreted as a power of a

generating element, also called a primitive element. Such an element is a root of an irreducible polynom of degree r with the coefficients belonging to the prime field GF(p) in $GF(p^r)$. Such a polynom, the roots of which are primitive elements, is called a primitive polynom. Still another property of the Galois-field $GF(p^r)$ is that each element may be written as a polynom in α over GF(p) of degree r-1. If p=2 and r=4, hence x^4+x+1 is a primitive polynom.

If u and v are two arbitrary elements in $GF(2^4)$ none of which equals 0, and if

$$u = x_0 + x_1 \cdot \alpha + x_2 \cdot \alpha^2 + x_3 \cdot \alpha^3 \qquad x_i = 0 \text{ or } 1$$
$$v = y_0 + y_1 \cdot \alpha + y_2 \cdot \alpha^2 + y_3 \cdot \alpha^3 \qquad y_j = 0 \text{ or } 1$$

and if $u = \alpha^{n1}$ and $v = \alpha^{n2}$, then $u \cdot v = \alpha^{n1+n2}$, also belonging to $GF(2^4)$.

This implies that $u \cdot v = z_0 + z_1 \cdot \alpha + z_2 \cdot \alpha^2 + z_3 \cdot \alpha^3$.

The coefficients z_0, z_1, z_2 and z_3 are bilinear expressions in x_i and y_j, where i and j assume values 0, 1, 2 or 3.

According to the invention the addition and multiplication rules for the elements in $GF(p^r)$ are used when matrices of order n (the number of rows and of columns in equal to n) are multiplied.

The "general linear group" $GL(n,p^r)$ of order n over the Galois-field $GF(p^r)$ consists of all the non-singular matrices. This group contains a number of subgroups. One such subgroup of special interest in connection with the present invention is the "special linear group" $SL(n,p^r)$ which consists of all determinants which are equal to 1.

As an example, let us consider the binary field which is a realization of GF(2). There exist exactly 16 matrices of order n=2 over this field, 6 of which being non-singular. In this case the "general linear group" GL(2,2) and the "special linear group" SL(2,2) coicide. The six matrices in SL(2,2) are

$$\begin{pmatrix}0&1\\1&0\end{pmatrix}, \begin{pmatrix}0&1\\1&1\end{pmatrix}, \begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\1&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix} \text{ and } \begin{pmatrix}1&1\\1&0\end{pmatrix}$$

Expressing these matrices in hexadecimal form will give, for instance, 6, 7, 9, B, D and E, respectively. They constitute a group (which is isomorphic to the symmetric group S_3).

This implies that the product of two arbitrary matrices in this set of six matrices also belongs to the same set. As an example, we get $6 \cdot 7 = D$. By storing in a ROM or PROM memory in the multiplication table of matrices intended to be used in a cryptosystem according to the present invention, the product of matrices is easily obtained by a table-look-up routine.

As mentioned before, the invention utilizes matrices belonging to a certain matrix group. A plaintext is partitioned into blocks consisting of strings of elements in a Galois-field $GF(p^r)$ or a bit string. These blocks will then define a plaintext matrix. A key may also be looked upon as a block consisting of a string of elements defining in the same way a key matrix. By multiplying the plaintext matrix with at least two key matrices a crypto matrix will be received and will be able to transmit to the receiver.

Description of drawings

The invention will in the following be further described in connection with the Figures on the accompanying drawings. On the drawings Fig. 1 illustrates an already known and above described standardized cipher system from the U.S.A. Fig. 2 shows a block diagram of an encryption and decryption system Figs. 3 and 4 show diagrammatically two shift register circuits for use in connection with the system according to Fig. 2. Fig. 5 shows diagrammatically how two shift registers may be connected to cooperate.

The block diagram of Fig. 2 shows a plaintext message applied as blocks m consisting of, for example, data bits to a matrix encoder 1. The output of said encoder delivers a matrix M for each block m. The elements in the matrix M belong to a Galois-field as described above.

The matrix M is supplied to a first input 2 of an encryption device 3. Before that a first cipher key a consisting of data bits has been supplied to a second input 4 of said device, and a second cipher key b to a third input 5 of the same device.

If each key a and b consists of 16 bits a key can assume 2^{16} or 65536 different values. In the most simple embo-

diment of the invention one will obtain $2^{32} = 4\,294\,967\,304$, or about $4 \cdot 10^9$ different combinations of key values a and b. If two repeated encryptions are executed with two sets of keys a_1, b_1 and a_2, b_2 one will obtain 2^{64} or about $1{,}6 \cdot 10^{19}$ different combinations of key values. It is practically impossible to break such an encrypted message using search routines to find the correct keys.

Each cipher key is supplied to a device 6 and 7, respectively for the generation of key matrices. One embodiment for the realization of such a device will be explained in connection with Fig. 3.

Fig. 3 diagrammatically illustrates a key matrix generator utilizing a Galois-field with $p = 2$ and $r = 4$. A key a consisting of 16 bits passes via a switch 31 into a shift register 32 having 16 positions. After that the switch 31 is switched over to the not shown position, and becomes fed back and will be able, at the outputs of each step, to generate a pseudorandom sequence of maximal length. In the example chosen a feedback is used corresponding to the primitive polynom $x^{16} + x^{12} + x^3 + x + 1$, defining the modulo-2 addition of the positions 33, 34 and 35. The outputs from each step in the shift register are grouped together into a tetrade μ_0, μ_1, μ_2, μ_3 each consisting of four bits as indicated by the arrows 36, 37, 38 and 39. The elements μ_i may be used to generate addresses to two matrices having elements in a Galois-field, or they mey be considered as elements in the Galois-field GF(16). Said last case is shown here. The four elements μ_i in the tetrade are supplied two by two to two matrix encoders 40, 41. The encoder 40 generates the matrix A_1 and the encoder 41 generates the matrix A_2. These matrices may, for example, be

$$A_1 = \begin{pmatrix} 1 & \mu_0 \\ \mu_1 & 1 + \mu_0 \mu_1 \end{pmatrix} \text{ and } A_2 = \begin{pmatrix} 1 & \mu_2 \\ u_3 & 1 + \mu_2 \mu_3 \end{pmatrix}$$

The matrix encoders 40 and 41 may be replaced by a single matrix encoder having two outputs A_1 and A_2 for the matrices. These matrices are supplied to a matrix multiplier 42 the output of which will give the product $A = A_1 \cdot A_2$. Alternatively, also the matrix encoder 42 may be a part of a common matrix encoder 40, 41.

All three matrices A, A_1, A_2 belong to the "speciel linear group" SL(2,16) as discussed earlier.

For the purpose of the invention it is in the same way necessary to generate a second key matrix B. This is performed by means of a separate feedback shift register and a matrix encoder, processing the key b. In Fig. 2 the block 7 is intended for generating the key matrix.

Instead of using feedback shift registers to generate the key matrices the tetrade μ_i may also be generated by random using a noise generator.

If the matrix A is used for encryption its inverse A^{-1} is needed for decryption. The inverse matrix may either be obtained by multiplying inverted submatrices ($A^{-1} = A_2^{-1} \cdot A_1^{-1}$), or a separate inverter 9, 10, according to Fig. 2, may be used on which one input is connected to the output of a matrix encoder. By means of a change-over switch 12, 13 between the matrix encoder and its multiplier either the output of the matrix encoder may be directly connected to the multiplier (generating the matrix A or the matrix B) or the same output may be connected to the multiplier via the inverter 9, 10 (generating the matrix A^{-1} and the matrix B^{-1}).

As can be seen from Fig. 2 the plaintext matrix M is supplied to a first input on a first matrix multiplier 14. To a second input on said multiplier the first key matrix A is supplied. In the embodiment shown said key matrix A is multiplied from the right to give the product M•A which has the form of a matrix and which is supplied to a first input on a second matrix multiplier 15. To a second input on said multiplier 15 the second key matrix B is supplied. Due to the multiplication order in the first matrix multiplier 14, the multiplication in the second matrix multiplier 15 requires the second key matrix B to be multiplied from the left to generate the product K = B•M•A, said product giving the encrypted matrix.

Decryption of the encrypted matrix is performed in an identical cipher device 3'. The only difference between the cipher device 3 and this further cipher device 3' is that in the latter the change-over switches 12' and 13' are arranged to supply the inverse key matrices A^{-1} and B^{-1} to the matrix multipliers 14' and 15', respectively. The combined multi-

pliers 15' and 14' will then generate the final result $M = B^{-1} \cdot K \cdot A^{-1}$. In a matrix decoder 20 the original plaintext block m will be recovered.

The invention does not require the limitation of generation of 2•2 matrices. Square matrices of arbitrary order n may be utilized. Fig. 4 exemplifies the generation of matrices of order 3 belonging to the "special linear group" SL(3,16) over a finite field (Galois-field) containing sixteen elements as shown in Fig. 4. In this embodiment the same shift register 30 is being used as in Fig. 3. The elements μ_1 and μ_2 in the tetrade according to Fig. 3 will appear in both the matrices A_1 and A_2. Considering the elements μ_i in the tetrade as elements in the Galois-field GF(16) and putting

$$A_1 = \begin{pmatrix} 1 & 0 & 0 \\ \mu_0 & 1 & 0 \\ \mu_1 & \mu_2 & 1 \end{pmatrix} \quad \text{and} \quad A_2 = \begin{pmatrix} 1 & \mu_1 & \mu_2 \\ 0 & 1 & \mu_3 \\ 0 & 0 & 1 \end{pmatrix}$$

as well A_1 as A_2 will belong to the "special linear group".

These matrices are easily inverted, offering a convevenient possibility of generating the inverse of the matrix $A = A_1 \cdot A_2$. The appearence of the submatrices A_1^{-1} and A_2^{-1} is shown below in the formula of the inverse matrix A^{-1}:

$$A^{-1} = A_2^{-1} \cdot A_1^{-1} = \begin{pmatrix} 1 & -\mu_1 & -\mu_2+\mu_1 \cdot \mu_3 \\ 0 & 1 & -\mu_3 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ -\mu_0 & 1 & 0 \\ -\mu_1+\mu_2 \cdot \mu_0 & -\mu_2 & 1 \end{pmatrix}$$

Fig. 5 shows an embodiment using two shift registers 50 and 51 to generate a key matrix A. A key a may be partitioned in an arbitrary way into two subkeys a_1 and a_2. Each one of them is supplied to one of the shift registers 50, 51, said registers being, if desired, of the type previously described. Outputs on the shift registers are connected to a matrix encoder 52 in such a way that an output thereon will generate a key matrix A.

Another modification of the invention may be used to increase the resistivity against breaking. This is obtained by making the cycle-time of the shift register a fraction 1/k of the rate by which the plaintext matrices M are supplied to the cipher device. In that way a key matrix consisting of the product of k consecutive matrices A will be gene-

rated. Said key matrix may then be utilized as a factor in the matrix multiplication with the plaintext matrix M.

The control of the processes in the cipher devices, in the matrix encoders and in the matrix decoders requires synchronization of the transmitter and the receiver by means of clock pulses, if necessary under the control of a microcomputer.

Matrices M generated during decryption have certain characteristic properties which may be the basis for checking the correctness of transmitted messages. A plaintext matrix may, for example, have the characteristic feature that its determinant is 1. It is also possible that a certain element in each plaintext matrix has a predefined value. These and other characteristics may easily be checked and identified.

Error detection and error correction is also, at least in principle, possible to perform before decryption. Correct reception requires that the matrices even prior to the decryption belong to the actual matrix group, let it be denoted G. This matrix group is a subgroup of the "general linear group" $GL(n,p^r)$. Said group may be partitioned into "cosets" in relation to G, quite analogously to the theory for linear codes. However, an important difference is that the group $GL(n,p^r)$ will not be commutative, and that further development of the said theory must be performed. A primary objective will be to find subgroups (G) to the group $GL(n,p^r)$ that are suitable both from the encryption and from the encoding point of view.

Said correction may, for instance, be performed if the set S of plaintext matrices M to be used in a communication system is the set of singular 2•2 matrices over the Galois-field GF(16), i.e. the matrices the determinant of which is 0. Then also K = B•M•A will belong to S. However, the matrix K' received by the receiver may differ from the matrix K transmitted, because of noise in the communication channel. Since all matrices have binary representation the Hamming distance between two arbitrary matrices will be well defined. If K' is non-singular an error will be detected, and one should look for a singular matrix K the Hamming distance of which is as small as possible.

C L A I M S

1. A method of encryption of information characters in a message using at least one encryption key, and of decryption of a message so encrypted, using the same keys, c h a r a c t e r i z e d in that for the purpose of encryption the characters of a plaintext message are partitioned into blocks (m) of binary digits, and that each block is partitioned into subblocks, each of which is interpreted as an element in a Galois-field, said elements being brought to generate a plaintext matrix (M) which is multiplied from the right in a first matrix multiplier (14) by a first key matrix (A) belonging to a prescribed matrix group over said Galois-field and generated by means of a first encryption key (a) applied to a first matrix generator (6), the output (M•A) of which is multiplied from the left in a second matrix multiplier (15) by a second key matrix (B) belonging to the same matrix group and generated by means of a second encryption key (b) applied to a second matrix generator (7), the output ($K = B \cdot M \cdot A$) of which being the encrypted plaintext block, which is transmitted to a receiver in which said encrypted plaintext block (K) for the purpose of decryption is multiplied from the left in a third matrix multiplier (15') by a third key matrix (B) and being generated by means of the second encryption key (b) applied to a third matrix generator (7'), the output ($B^{-1} \cdot K$) of which is multiplied from the right in a fourth matrix multiplier (14') by a fourth key matrix (A^{-1}) being the inverse of the first key matrix (A) and being generated by means of the first encryption key (a) applied to a fourth matrix generator (6'), the output ($M = B^{-1} \cdot K \cdot A^{-1}$) of which being the restored original plaintext matrix which after decoding gives the original plaintext block.

2. A method according to claim 1, c h a r a c t e r i z e d in that the procedure of encryption is repeated at least twice, each time utilizing unchanged or two new encryption keys (a, b ...), and that decryption is performed an equal number of times, each time utilizing said unchanged or two new encryption keys (a, b ...).

3. A device for the realization of the method according to claim 1 for encryption of information characters in a message using at least one encryption key, and of decryption of a message so encrypted, using the same keys, c h a r a c t e r i z e d in that a plaintext message, consisting of binary digits, and partitioned into blocks, has each block partitioned into subblocks, each of which is interpreted as an element in a Galois-field, said elements being brought to generate a plaintext matrix (M), and that at least two encryption keys (a, b ..) are supplied each one to a matrix generator (6, 7) being arranged to generate each one a key matrix (A, B ..) each one belonging to a prescribed matrix group over said Galois-field, said plaintext matrix (M) being supplied as multiplicand to a first input on a first matrix multiplier (14); a first key matrix (A) being supplied as multiplier to a second input on said first matrix multiplier (14) to give a product (M•A), said product being supplied as multiplicand to a first input on a second matrix multiplier (15) to which a second key matrix (B) as multiplier is supplied at a second input to give a product (B•M•A) in which the plaintext matrix (M) is placed between the key matrices (B, A), said product representing an encrypted message matrix (K); and that for the purpose of decryption an identical device (3') is used, in which, however, inverted key matrices (B^{-1}, A^{-1}) are being used and are so arranged that the key matrices (B, A) introduced by the encryption are eliminated, giving the restored plaintext matrix (M).

4. A device according to claim 3, c h a r a c t e r i z e d in that an encryption key (a, b ..) is generated in a shift register (30) and that said key has such a length that all steps in the shift register are filled, and that the shift register is so connected and arranged that output signals are interpreted as a string of elements in said Galois-field, said elements being supplied to a matrix generator to generate a key matrix (A, B ..).

5. A device according to claim 4, c h a r a c t e r i z e d in that shift register and matrix generator are combined to form a unit (6, 7).

6. A device according to claim 3, c h a r a c t e -

r i z e d in that each key matrix (A, B ..) is supplied from the output on a matrix generator (6, 7) to separate matrix multipliers (14, 15) via one of two parallel paths, one of which comprises an inverter (9, 10) and which are connectable by means of a change-over switch (12, 13).

7. A device according to anyone of claims 3 to 6, c h a r a c t e r i z e d in that shift registers (30), matrix generators (6, 7), inverters (9, 10), matrix multipliers (14, 15) and connecting circuitry are arranged to form at least one integrated circuit or to form part of the circuitry of at least one printed circuit.

8. A device according to anyone of claims 3 to 7, c h a r a c t e r i z e d in that each shift register (30) is arranged for feedback and is subdivided into equally large subregisters, the outputs of which are arranged to supply the content of a subregister in the form of elements (u_0, u_1, u_2, u_3) in a Galois-field, and that said elements are supplied to at least one matrix generator (40, 41), the outputs of which are so arranged that at least two subkey matrices (A_1, A_2) are supplied, said subkey matrices being supplied to a matrix multiplier (42), the output of which delivers a key matrix (A).

FIG.1

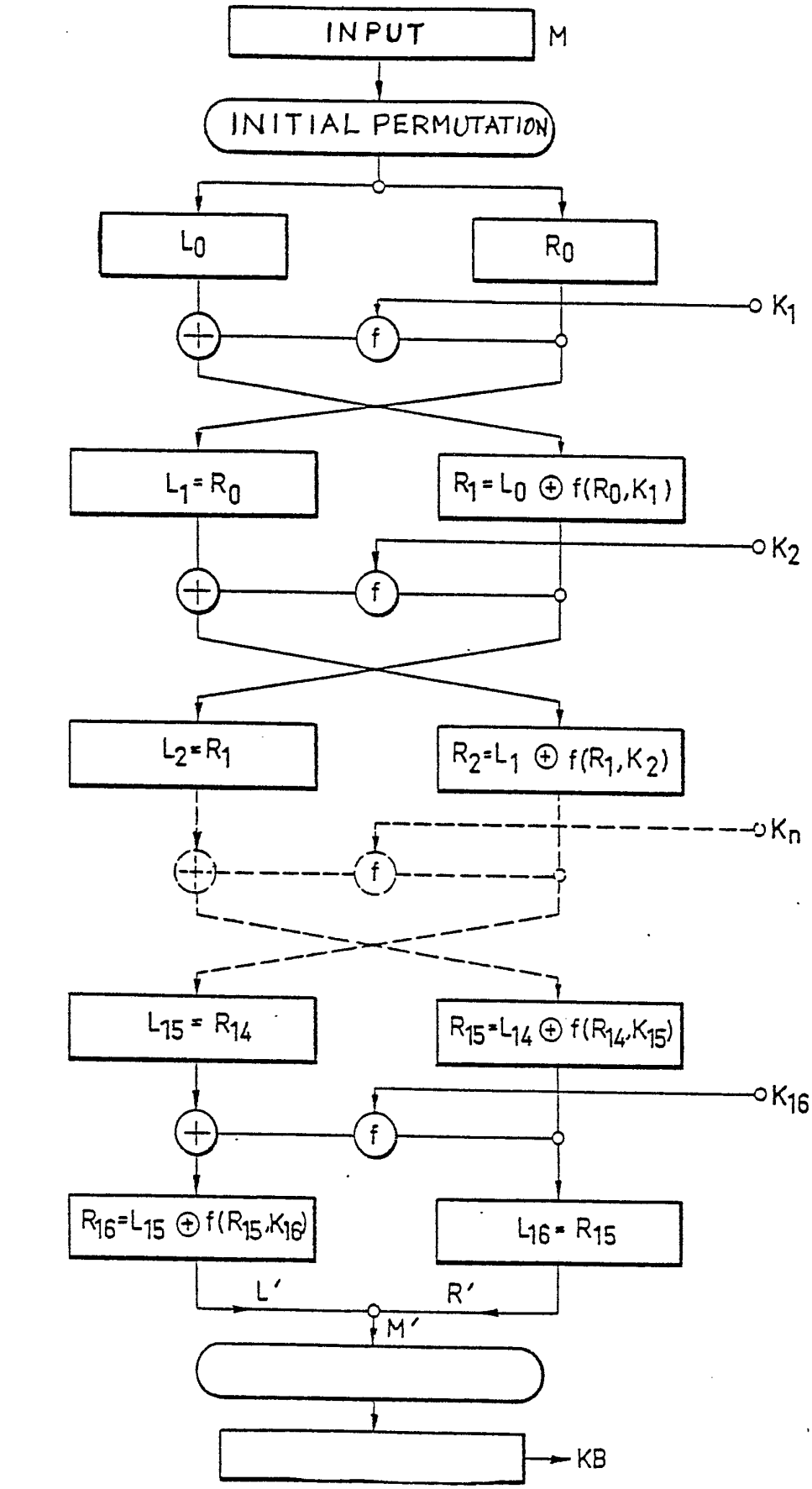


FIG. 2

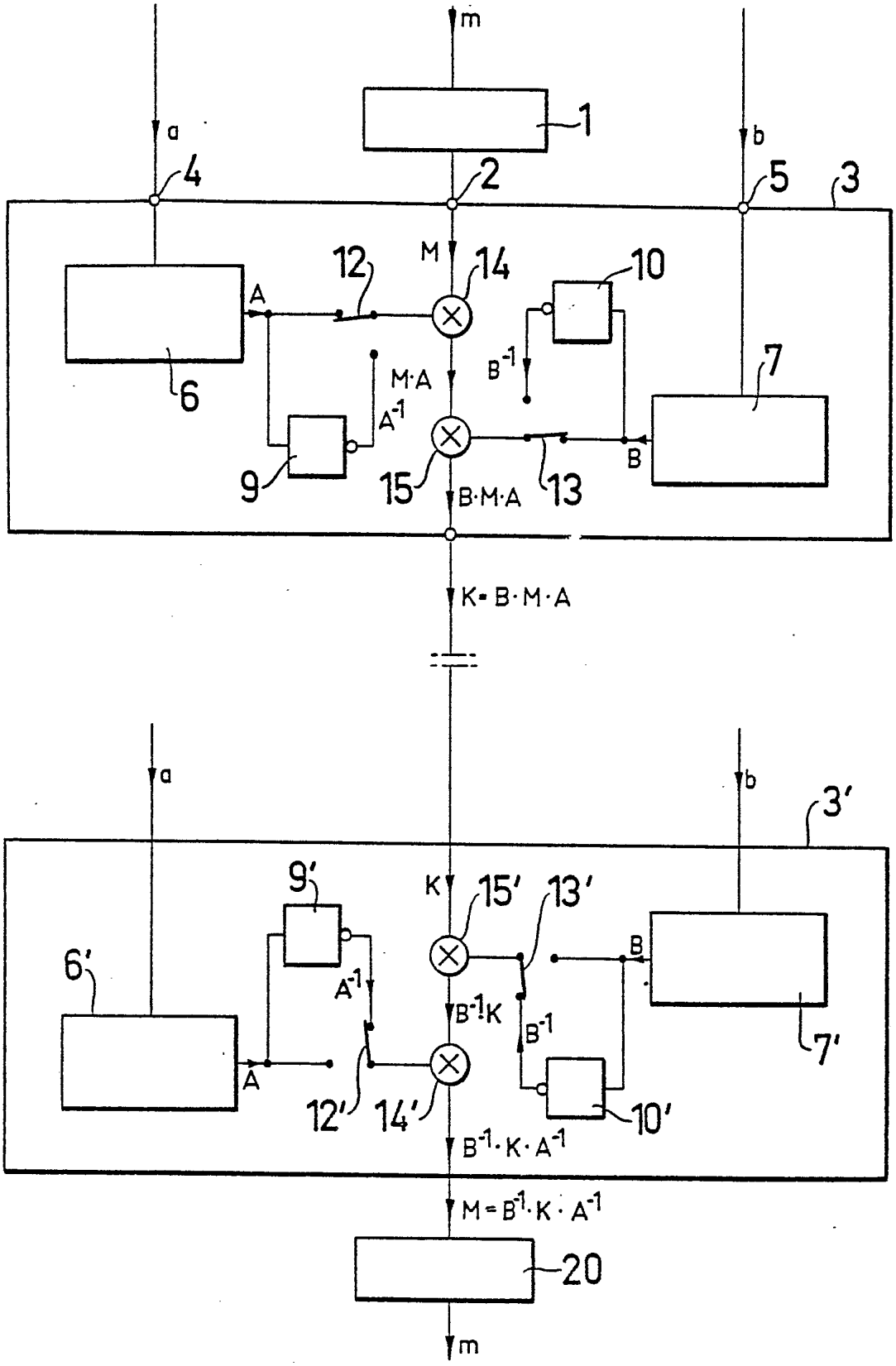


FIG.3

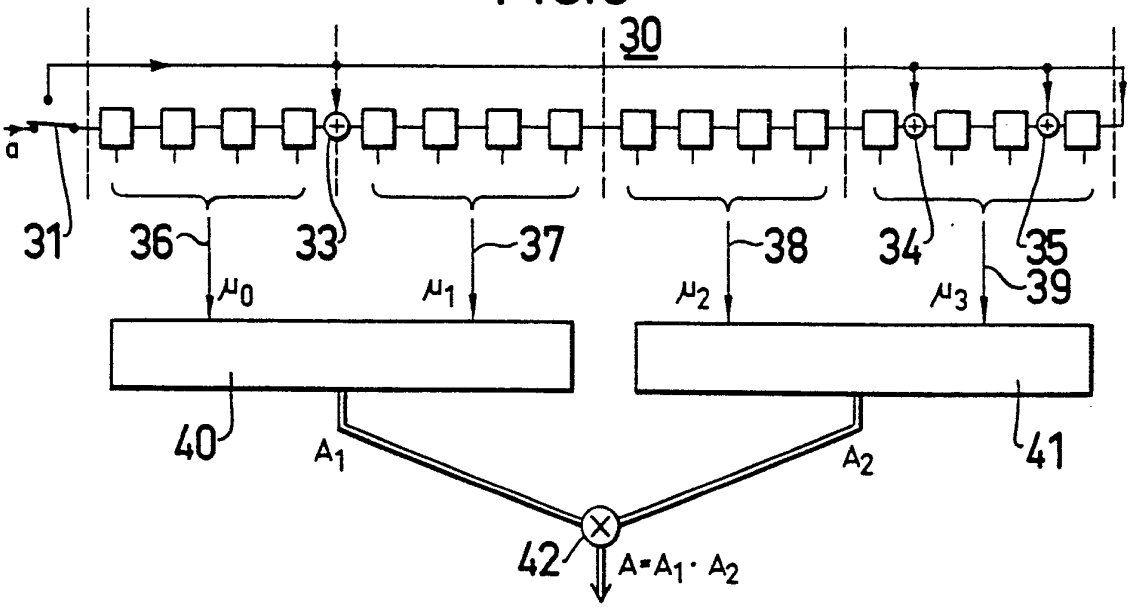


FIG.4

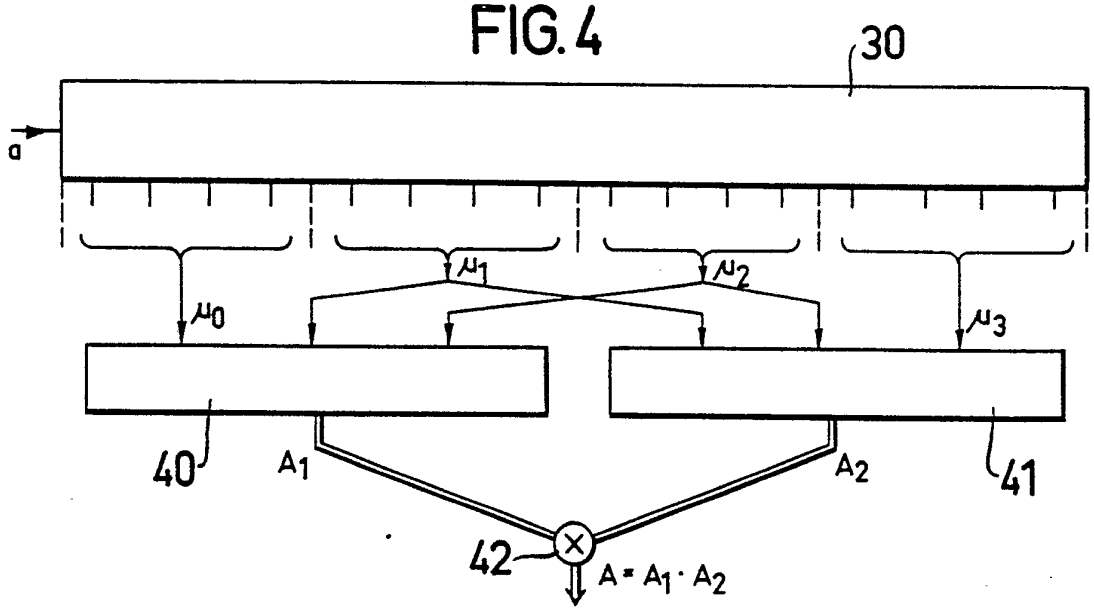
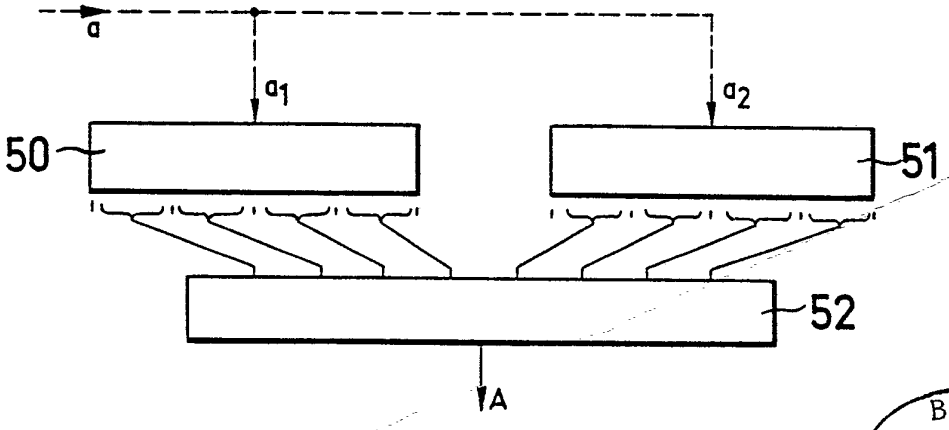


FIG.5



INTERNATIONAL SEARCH REPORT

International Application No PCT/SE78/00100

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [3]

According to International Patent Classification (IPC) or to both National Classification and IPC

G 09 C 1/00, H 04 L 9/00

II. FIELDS SEARCHED

Minimum Documentation Searched [4]

Classification System	Classification Symbols
IPC 2	G 09 C 1/00-5/00; H 04 K 1/00, 1/02; H 04 L 9/00-9/04 .../...

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched [5]

SE, NO, DK, FI classes as above

III. DOCUMENTS CONSIDERED TO BE RELEVANT [14]

Category *	Citation of Document, [16] with indication, where appropriate, of the relevant passages [17]	Relevant to Claim No. [18]
A	US, A, 3 798 359 published 1974, March 19, International Business Machines Corporation	
A	US, A, 3 798 360 published 1974, March 19, International Business Machines Corporation	

* Special categories of cited documents: [15]

"A" document defining the general state of the art

"E" earlier document but published on or after the international filing date

"L" document cited for special reason other than those referred to in the other categories

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but on or after the priority date claimed

"T" later document published on or after the international filing date or priority date and not in conflict with the application, but cited to understand the principle or theory underlying the invention

"X" document of particular relevance

IV. CERTIFICATION

Date of the Actual Completion of the International Search [2]	Date of Mailing of this International Search Report [2]
1979-02-21	1979-02-27
International Searching Authority [1]	**Signature of Authorized Officer [20]**
Swedish Patent Office	Stefan Lennefors Stefan Lennefors

Form PCT/ISA/210 (second sheet) (October 1977)

FURTHER INFORMATION CONTINUED FROM THE SECOND SHEET

II Continuation classification system.
Deutsche Klassen: 21a1:21, 42n:14
US classification: 35/3-4, 178/22

V. ☐ OBSERVATIONS WHERE CERTAIN CLAIMS WERE FOUND UNSEARCHABLE [10]

This international search report has not been established in respect of certain claims under Article 17(2) (a) for the following reasons:

1. ☐ Claim numbers....., because they relate to subject matter [12] not required to be searched by this Authority, namely:

2. ☐ Claim numbers....., because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out [13], specifically:

VI. ☐ OBSERVATIONS WHERE UNITY OF INVENTION IS LACKING [11]

This International Searching Authority found multiple inventions in this international application as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims of the international application.

2. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims of the international application for which fees were paid, specifically claims:

3. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claim numbers:

Remark on Protest

☐ The additional search fees were accompanied by applicant's protest.

☐ No protest accompanied the payment of additional search fees.