The invention relates to a device for the block-wise conversion of a first digital block into a second digital block in accordance with the preamble to Claim 1. The invention further relates to the use of this device in accordance with the preamble to the other independent Claim.

For over ten years, transmission networks have been in worldwide use which use the Data Encryption Standard DES. This DES Standard of the American National Bureau of Standards (NBS) is used for block encryption with individually selectable keys (secret key block encryption). In this case, every plaintext block has a length of 64 bits, as does the ciphertext block. A sequence of 64 bits, of which 56 bits are freely selectable, is used as the secret key. The transmission of the ciphertext block is effected via a generally accessible network.

In general, the Data Encryption Standard DES is regarded as a very good encryption tool. However, it is an open matter of debate whether the DES Standard has in the meantime become insecure or not. On this point, the relatively short length of the secret key plays an important part.

A further block-by-block encryption method is known from EP-A-0 221 538. In this case, in a plurality of parallel processing channels, the data fed to the input side of the various channels are functionally mixed directly or indirectly with the data from all the other channels. The new channel data finally generated are mixed at the output end and are delivered jointly. The function operators used with this method are all the same and are combined with one another at random and with similarly uniform transformation operators.

Finally, a block encryption method for a local computer system in which one standard key is made available to all authorised sharers, is known from US-A-4 255 811. One central computer holds a list of all the issued authorised sharer keys. Encryption is performed by each sharer who uses the sharer key allocated to him, performing decryption by means of the appropriate key which can be obtained by accessing the central computer.

It is the problem of the invention to indicate a block encryption method which is improved compared with the prior art methods and which could be introduced as a European Standard. It is intended that this method of block encryption employ all known encryption techniques of confusion, diffusion etc. and above all use a longer key.

The solution to this problem is indicated by the characterising part of the independent Claims. The dependent Claims disclose developments of the invention.

The invention is by way of example described in greater detail hereinafter with reference to fourteen drawings which show:

Fig. 1 a basic block circuit diagram of a device for transmitting data in encrypted form
Fig. 2 a block circuit diagram of an encrypter
Fig. 3 a block circuit diagram of a primary encryption logic
Fig. 4 a truth table of operation units of a first kind
Fig. 5 a truth table of operation units of a second kind
Fig. 6 a block circuit diagram of an extended encryption logic
Fig. 7 a truth table of operation units of a third kind

Fig. 8 a block circuit diagram of a supplementary encryption logic
Fig. 9 a block circuit diagram of an encryption stage
Fig. 10 a table of key sub-blocks and decryption sub-blocks
Fig. 11 a block circuit diagram of a second supplementary encryption logic
Fig. 12 a block circuit diagram of a second encryption stage
Fig. 13 a block circuit diagram of a second encrypter and
Fig. 14 a second table of key sub-blocks and decryption sub-blocks.

Fig. 1 shows a basic block circuit diagram of a device for transmitting data in encrypted form. The data (plaintext $\underline{X}$) to be transmitted originate in a message source 11, e.g. a computer. These data are encrypted in an encrypter 12 and transmitted as ciphertext $\underline{Y}$ over a publicly accessible transmission line 13. The ciphertext $\underline{Y}$ reaches a decrypter 14 on the receiver side which feeds it to a destination 15, e.g. a second computer, in decrypted form.

For encryption and/or decryption of the data, the encrypter 12 and the decrypter 14 use a secret key block Z which is provided by means of a key source 16 and are supplied over a secure channel 17 to both units 12, 14. This channel 17 is for example a courier with a sealed cover.

The ciphertext $\underline{Y}$ on the transmission line 13 is always exposed to the risk that an enemy cryptanalyst 19 will also read this text $\underline{Y}$ and attempt to obtain the associated plaintext $\underline{X}$ or the key block Z. (The results of these attempts are designated $\hat{X}$ and $\hat{Z}$.) In principle, the cipher should be resistant to these attempts or should at least offer resistance for a sufficient length of time.

Fig. 2 shows a block circuit diagram of the encrypter 12 in the case of step-by-step block encryption. The plaintext $\underline{X}$ to be encrypted arrives continuously from the message source 11 and reaches the input unit 21, e.g. a series/parallel converter in the case of a serial bit stream. In this step-by-step manner, this input unit 21 assembles plaintext blocks X of preferably N = 64 bits (first length) which are partitioned into four sub-blocks X_1, X_2, X_3, X_4, each of m = 16 bits (second length). These plaintext sub-blocks of the respective plaintext block X reach a first encryption stage 61.1 via first inputs 25 to 28, each consisting of 16 parallel lines. In this stage 61.1, the sub-blocks X_1 to X_4 are grouped together with six different control blocks by means of suitable logical functions. During the encryption process, the (general) control blocks are (special) key sub-blocks Z_1 to Z_6 and during the decryption process they are decryption sub-blocks U_1 to U_6 which are in each case derived from the key block Z. This will be discussed in greater detail hereinafter. In the main it is the encryption process which is described in the following, which is why the term key sub-block is preferred.

The key sub-blocks Z_1 to Z_6 are connected to second inputs 29, 30, 32, 33, 49, 52 of the first encryption stage 61.1. They together with other key sub-blocks Z_7 to Z_{52} are delivered by a key sub-block generating unit 63. Via the secure channel 17, this unit receives the selected key-block Z which preferably forms a sequence of K = 128 bits.

The method of obtaining the key sub-blocks Z_1 to Z_8 from the key block Z resides in that this latter is subdivided into identical parts, each of 16 bits length. Then, the 128 bits of the key block Z are cyclically

shifted (cyclically exchanged) by 25 bits in a uniform direction, e.g. to the left, and the fresh sequence of 128 bits which is thus created is in turn divided into eight identical parts for forming the key sub-blocks Z_9 to Z_{16}, and so on until the formation of Z_{52}. Each key sub-block Z_1 to Z_{52} thus has a (second) length m of 16 bits, is derived in an unequivocal manner from the key block Z and is generally distinct from every other key sub-block. The key sub-blocks Z_1 to Z_6 are connected to the said six second inputs 29, 30, 32, 33, 49, 52 of the first encryption stage 61.1. The result of the grouping together in this stage 61.1 appears at four outputs or connections 35 to 38, and in fact as four first intermediate sub-blocks or intersub-blocks W_{11}, W_{12}, W_{13}, W_{14} each of m = 16 bits and together they form a first interblock W_1 of the (first) length N = 64 bits.

The first intersub-blocks W_{11} to W_{14} are for the second encryption step connected to the connections or inputs 35 to 38 (identical to the outputs of the preceding stage 61.1) of a second encryption stage 61.2. This encryption stage 61.2 is identical in construction to the first encryption stage 61.1. Connected to its six second key inputs are the described key sub-blocks Z_7 to Z_{12} and at its outputs appear the second intersub-blocks W_{21}, W_{22}, W_{23}, W_{24} or altogether the second interblock W_2.

The second intersub-blocks W_{21} to W_{24} are for the third encryption step connected to a third (not shown) encryption stage while the third intersub-blocks W_{31} to W_{34} are connected to a fourth encryption stage or up to a ninth encryption stage 69 having four second inputs 129, 130, 132, 133 which is different from the preceding stages.

Finally, four ciphertext sub-blocks Y_1, Y_2, Y_3, Y_4 of the second length m = 16 bits and which together form one ciphertext block Y which is associated with the relevant plaintext block X in a complicated but unequivocal manner, appear at the outputs 75 to 78 of the ninth stage 69. This ciphertext block Y is, in an output unit 79, e.g. a parallel/serial converter, so converted that it can be transmitted over the transmission line 13.

The encryption process thus takes place in nine successive encryption stages 61.1, 61.2, 69, of which the first eight are identical to one another. The altogether fifty-two aforesaid different key sub-blocks Z_1 to Z_{52} serve as a key. The encrypter 60 required for the encryption process X --> Y is indicated by broken lines in Fig. 2.

The encryption stages 61.1, 61.2, 69 can be carried out in various ways. On the one hand, a so-called software solution can be envisaged in which one or more processors operate according to a predetermined programme. For example, each input (e.g. the first inputs 25 to 28) can have its own processor assigned to it, which in a serial manner takes into account the in each case m = 16 parallel lines of each input. On the other hand, it is also possible to provide a hardware solution in which the logical function elements take the form of independent circuit units. These are then either constructed from discrete chip elements or preferably from several very large scale integration units (VLSI). Where the hardware solution is concerned, all lines of all inputs are preferably processed in parallel. However, a partial serial procedure is also possible in this case in that for example the different inputs (e.g 25 to 28) are serially connected by multiplexers to partial central circuit units.

The hardware solution has over the software solution the advantage that it can operate substantially more quickly, in fact up to clock frequencies of about 100 Mbits/second and faster. Hereinafter, therefore, and for reasons of illustration, the hardware solution is given greater emphasis for the encryption stages 61.1. 61.2 and 69.

Fig. 3 shows the block circuit diagram of a primary encryption logic 40. This logic comprises four operation units 41 to 44 of two different kinds ⊞, ⊙, which are connected to one another by three connections 45 to 47, the last (47) of which at the same time constitutes an output of the logic 40. In addition there is a further output 48 and two first inputs 50, 51 and two second inputs 59, 52 of the logic 40.

Each operation unit 41 to 44 has two inputs and one output. Each input and output is constructed as a 16-bit parallel input or output to which a 16-bit block is connected in a bit-parallel manner. Correspondingly, the operation units 41 to 44 are constructed for the logical joining together of in each case two input blocks E_1, E_2 and for forming an assigned output block A of 16 bits. By virtue of the method, the operation units are connected serially in four stages, the two kinds of units 41 to 44 alternating.

The operation units of the first kind ⊞, i.e. the units 42 and 44, have the following characteristics: these units regard each input block E_1, E_2 as an integer in binary representation, this number belonging to the number set or quantity $(0, 1, 2, \ldots, (2^m-1))$. (The number m (second length) is preferably the number 16 but it may also be 4 or 8.) The units 42, 44 thus form the sum modulo 2^m from the input blocks E_1, E_2 and

deliver a corresponding output block A. The operation units 42, 44 of the first kind are thus adder modulo 2^m.

Fig. 4 shows the truth table for this first kind ⊞ of operation units 42, 44, in fact as an example for m = 2. In this case, the two input blocks E_1, E_2 and the output block A are respectively indicated as a number in binary and in decimal representation.

The operation units 41, 43 of the second kind ⊙ have the following characteristics: these units regard the block, whose bits are all zero, as an integer 2^m. Otherwise, they interpret the blocks as integers in binary representation, wherein these numbers belonging to the number set or quantity (1, 2, 3,..., (2^m-1)) in which m = 4, 8 or 16. The relevant output block A is then the product modulo (2^m+1) of the input blocks E_1, E_2. The units 41, 43 are thus multiplier modulo (2^m+1). Fig. 5 shows the truth table for this second kind ⊙ of operation units 41, 43 for m = 2, again as an example, and corresponding to the truth table in Fig. 4.

The primary encryption logic 40 produces a very satisfactory diffusion since each of its two output blocks a_1, a_2 depends on the two input blocks e_1, e_2 and the two key sub-blocks Z_5, Z_6, in other words the values at all inputs. It can be proved that the number of four operations constitutes a minimum for satisfying this problem of diffusion. The said use of operation units of different kinds serves to create the necessary confusion.

Fig. 6 shows the block circuit diagram of an extended encryption logic 140. This encryption logic has four first inputs 125 to 128 for four input blocks e_5 to e_8 which are to be encrypted in parallel, four outputs 35 to 38 for delivering four output blocks a_5 to a_8

and two already mentioned second inputs 49, 52 for the input of two key sub-blocks Z_5, Z_6.

The primary logic 40 already described constitutes the core of the extended encryption logic 140. The logic 40 is supplemented by six operation units 115 to 120 of a third kind ⊕, in fact so that the input 125 leads to the units 115 and 117, the input 126 to the units 116 and 118, and input 127 to units 115 and 119, the input 128 to the units 116 and 120, the outputs of the units 115 and 116 forming the inputs 50 or 51 of the logic 40, the outputs 47, 48 of the logic 40 forming the inputs of the units 117, 119 and 118, 120 respectively, the outputs of the units 117 to 120 forming the outputs 35 to 38. The extended encryption logic 140 is functionally so constructed that each output 35 to 38 depends on all inputs 125 to 128 and 49, 52, operation units of each different kind ⊞, ⊙, ⊕ following one another consecutively, providing the characteristic of involution. This last-mentioned characteristic means that the extended encryption logic 140 is a self-inverse function for the blocks e_5 to e_8 connected to its first inputs 125 to 128, in fact for each given pair of key sub-blocks Z_5, Z_6.

Bit-by-bit exclusive-OR, as is known from the aforementioned DES Standard, is preferably used as operation units 115 to 120 of the third kind ⊕. Corresponding to Figs. 4 and 5, Fig. 7 shows the truth table for a bit-by-bit exclusive-OR and m = 2, but again only as an example in order to demonstrate the functioning.

Fig. 8 shows the block circuit diagram of a supplementary encryption logic 240. This comprises two operation units 111, 112 of the second kind ⊙ and two operation units 113, 114 of the first kind ⊞. Their

inputs are in each case a first input 225 to 228 for the input of an input block e_n and a second input 29, 30, 32, 34 for the input of a key sub-block Z_n (n = 1 ... 4). The outputs of the logic 240 are equal to the outputs 135 to 138 of the operation units 111 to 114.

Fig. 9 shows the block circuit diagram of one of the first eight identical encryption stages Fig. 2, for example the first stage 61.1. Accordingly, this encryption stage is constituted by the combination of a supplementary encryption logic 240 and an extended encryption logic 140, the outputs 135 to 138 of the logic 240 being (galvanically) connected directly to the inputs 125 to 128 of the following logic 140. The inputs 25 to 28 of the respective encryption stage (61.1) are identical to the inputs 225 to 228 of the supplementary encryption logic 240. The outputs of the extended logic 140, when crossed, form the outputs 35 to 38 of the encryption stage 61.1. Connected to the second inputs 29, 30, 32, 33, 49, 52 are six key sub-blocks, e.g. blocks Z_1 to Z_6 while either four plaintext sub-blocks X_1 to X_4 or four intersub-blocks W_{n1} to W_{n4} are connected to the first inputs 25 to 28. Assigned to the outputs 35 to 38 are the intersub-blocks W_{11} to W_{14} or $W_{(n+1)1}$ to $W_{(n+1)4}$, where n = 1, 2, ... 7).

The ninth encryption stage 69 corresponds solely to the supplementary encryption logic 240, the four outputs 135 to 138 of this logic 240 being identical to the four outputs 75 to 78 of the encryption stage 69.

As an overall logic for the encryption of plaintext blocks X which correspond to a sequence of 64 bits in each instance, the encryption unit 60 (Fig. 2) has altogether the following characteristics:

· It has four first inputs 25 to 28, fifty-two second inputs 28, 29, 32, 33, 49, 52 and four outputs 75 to 78.

· It has eight identical encryption stages 61.1, 61.2 plus another encryption stage 69.
· It has one hundred and sixteen operation units of altogether three different kinds ⊞, ⊙, ⊕.
· In the direction of flow of the logic operations, the kinds ⊞, ⊙, ⊕ of the successive operations generally and always alternate.
· It is suitable both for encrypting plaintext blocks X and also for decrypting ciphertext blocks Y.
· Each block at the outputs 75 to 78 is dependent upon all blocks at the first inputs 25 to 28 and almost all blocks at the second input 29, 30, 32, 33, 49, 52, all in all 53 blocks. (Not dependent are the output blocks of in each case three blocks which are connected to the second inputs 129, 130, 132, 133 of the ninth encryption stage 69.)
· Where each of the first eight encryption stages 61.1, 61.2 of the encryption unit 60 is concerned, each bit of each block $W_{(n+1)1}$ to $W_{(n+1)4}$ at the outputs 35 to 38 is dependent upon all bits of all blocks W_{n1} to W_{n4} and Z_n at the first (25 to 28) and/or second inputs 29, 30, 32, 33, 49, 52.

By reason of the said characteristics, an encryption unit 60 can be used either for encrypting a plaintext block X or for decrypting a ciphertext block Y. Therefore, it is possible to use the unit 60 both for the encryption process X --> Y and also for the decryption process Y --> X.

The key block Z used for the encryption process and the fifty-two key sub-blocks Z_1 to Z_{52} derived therefrom have already been described. Fig. 10 shows, then, fifty-two decryption sub-blocks U_1 to U_{52} which have to be used for the decryption process Y --> X, in fact in comparison with the key sub-blocks Z_1 to Z_{52} and in their relationship to these key sub-blocks and to the nine encryption stages 61.1, 61.2, 69 (Fig. 2).

During encryption X --> Y, in the first stage, the key sub-blocks Z_1 to Z_6 are used and in the second stage the blocks Z_7 to Z_{12} and so on. In the ninth stage, only the blocks Z_{49} to Z_{52} are used.

During decryption Y --> X, the following applies for each stage i:

· The first two decryption sub-blocks of each stage i (i = 1, 2 .... 9) of the decryption process Y --> X are equal to the modulo-$(2^{16}+1)$ multiplication inverses of respectively the first and second key sub-blocks in the (10-i)th stage of the encryption process X --> Y. This means for instance for the first two decryption sub-blocks U_1, U_2 of the first stage:
$U_1 = Z^{-1}_{49}$; $U_2 = Z^{-1}_{50}$.

· The third and fourth decryption sub-block in the i-th stage (i = 1, 2 .... 9) of the decryption process Y --> X are the negative values of the modulo-2^{16} addition of the third and fourth key sub-blocks in the (10-i)-th stage of the encryption process X --> Y. This means for instance for the decryption sub-blocks U_3, U_4 of the first stage: $U_3 = -X_{51}$; $U_4 = -Z_{52}$.

· The fifth and sixth decryption sub-blocks in the i-th stage (i = 1, 2 ... 8) of the decryption process Y --> X are equal to the fifth and respectively sixth key sub-block in the (9-i)-th stage of the encryption process X --> Y. This means for instance in the case of decryption sub-blocks U_5, U_6 of the first stage: $U_5 = Z_{47}$; $U_6 = Z_{48}$.

In this instance, Z^{-1}_j modulo-$(2^{16}+1)$ multiplied by Z_j is 1. Furthermore, $-Z_j$ modulo-2^{16} added to Z_j is 0.

The invention allows a large number of variants. Some of these are listed as follows.

· Other kinds of operation units 42 to 44, 111 to 114, 115 to 120 are used.

· The various kinds of operation units 41 to 44, 111 to 114, 115 to 120 are differently distributed in the various aforementioned logics 40, 240, 140. For example, the operation units of the two kinds ⊞, ⊙, are interchanged with each other in the primary encryption logic 40. It is however also possible for the primary encryption logic 40 to be of more complicated construction and/or for the two inputs 49, 52 to be omitted from such a variant.

· Fewer or more than eight identical encryption stages 61.1, 61.2 are used. Generally, a first majority S of stages are provided and then a second majority T of key sub-blocks is assigned to them. As a relationship between T and S, $T = 6 \cdot S + 4$. In this general case, for the relationships between the decryption sub-blocks U_1 to U_T and the key sub-blocks Z_1 to Z_T apply:
- the first two decryption blocks of each stage i (i = 1, 2 .... (S+1)) are equal to modulo-(2^m+1) multiplication inverses of the first and second key sub-block of the relevant first and second key sub-block in the (S-i+2)-th stage of the encryption process,
- the third and fourth decryption sub-block in the i-th stage (i = 1, 2 .... (S+1)) are equal to modulo-2^m addition inverses of the third and respectively fourth key sub-block on the (S-i+2)-th stage in the encryption process and
- the fifth and sixth decryption sub-block in the i-th stage (i = 1, 2 ... S) are equal to the fifth and respectively sixth key sub-block in the (S-i+1)-th stage in the encryption process.

· It is possible to discard the principle whereby the kinds ⊞, ⊙, ⊕ of directly successive operation units are always different. However, it is advantageous if at least the predominant number of all pairs of directly consecutive operations consist of two operations of a different kind ⊞, ⊙, ⊕.

· Derivation of the key sub-blocks Z_1 to Z_{52} from the key block Z is accomplished by a method other than that described.

· The encryption unit 60 is mainly constructed by using discrete operation units 41 to 44, 111 to 114, 115 to 120 as special logic units (hardware solution), predominantly while using commercially available processors and memories which work according to an associated programme (software solution) or in mixed construction.

Each of the described logics 40, 140, 240, 60, 61.1, 61.2, 69 can be conceived as a "black box" with first and second inputs and outputs. Each of these logics converts the two or four first sub-blocks connected to the first inputs into associated second sub-blocks of the same length which can be tapped at the outputs. The conversion process is influenced thereby by the key sub-blocks applied to the second inputs or in general by suitable control blocks. Parallel inputs and outputs are advantageous if higher working speeds are desired. For the aforementioned software solution, it is preferable to provide a single first and second input and a single output via which the associated input and output blocks can be input and output serially.

Vital to the conversion process is that the (second) length m be either 4, 8 or preferably 16 bits.

In addition to the characteristics mentioned in the object of the invention, the invention has the further advantageous characteristic feature that it is of relatively uncomplicated construction and works rapidly and without problem in both the hardware and software versions. The encryption logics 40, 140, 240 can be constructed as VLSI (very large scale integration) semi-conductor components which means that they can be produced at a competitive price.

A further specific alternative embodiment is described hereinafter with reference to Figs. 11 to 14 which are modifications of Figs. 8, 9, 2 and 10.

Fig. 11 shows the block circuit diagram of a second supplementary encryption logic 240v. This has two operation units 111v, 114v of the second kind ⊙ and two operation units 112v, 113v of the first kind ⊞. Their inputs are in each case a first input 225 to 228 for the input of an input block e_n and a second input 29, 30, 32, 33 for the input of a key sub-block Z_n (n = 1 ... 4). The outputs of the logic 240 are identical to the outputs 135 to 138 of the operation units 111v to 114v.

Fig. 12 shows the block circuit diagram of a second encryption stage 61.1v. This is constituted by the combination of the supplementary encryption logic 240v and an extended encryption logic 140, the outputs 135 to 138 of the logic 240v being connected directly (galvanically) to the inputs 125 to 128 of the subsequent logic 140. The inputs 25 to 28 of the respective encryption stage (61.1v) are identical to the inputs 225 to 228 of the second supplementary encryption logic 240v. The outputs of the extended logic 140 directly form the outputs 35 and 38 and, when crossed, form the outputs 35 and 37 of the encryption stage 61.1v. The rest of the construction corresponds entirely to that shown in Fig. 9.

Fig. 13 shows the block circuit diagram of a second encryption unit 60v which corresponds substantially to Fig. 2. In this case, eight identical second encryption stages 61.1v, 61.2v are connected in series and as a final stage 69v are followed by a second supplementary encryption logic 240v. In this case, the inputs W_{82} and W_{83} are connected cross-wise to ...W_{22} and ...W_{23} respectively.

Finally, Fig. 14 shows a second table of key sub-blocks Z_n and decryption sub-blocks U_n, corresponding to Fig. 10.

During encryption X --> Y, the key sub-blocks Z_1 to Z_6 are used unchanged in the first stage while in the second stage, the blocks Z_7 to Z_{12} are used and so on. In the ninth stage, only blocks Z_{49} to Z_{52} are used.

During decryption Y --> X, for each stage i, the following applies:

· The first and fourth decryption sub-block of each stage i (i = 1, 2 ..... 9) of the decryption process Y --> X are equal to the modulo-($2^{16}+1$) multiplication inverses of the respective first and fourth key sub-block in the (10-i)th stage of the encryption process X --> Y. For the first and fourth decryption sub-block U_1, U_4 of the first stage for example, this means:
$U_1 = Z^{-1}_{49}$; $U_4 = Z^{-1}_{52}$.

· The second and third decryption sub-block in the i-th stage (i = 2, 3 .... 8) of the decryption process Y --> X are the negative values of the modulo-2^{16} addition of the third and second key sub-block in the (10-i)-th stage of the encryption process X --> Y. This means for instance for the decryption sub-blocks U_8, U_9 of the second stage: $U_8 = -Z_{45}$; $U_9 = -Z_{44}$.

· The second and third decryption sub-block in the first and ninth stages of the decryption process Y --> X are the negative values of the modulo-2^{16} addition of the second and third key sub-block in the ninth and respectively first stages of the encryption process X --> Y. For instance for the decryption sub-blocks U_2, U_3 of the first stage, this means: $U_2 = -Z_{50}$, $U_3 = -Z_{51}$.

· The fifth and sixth decryption sub-block in the i-th stage (i = 1, 2 ... 8) of the decryption process Y --> X are equal to the fifth and sixth key sub-block in the (9-i)-th stage of the encryption process X --> Y. This means for example for the decryption sub-blocks U_5, U_6 of the first stage: $U_5 = Z_{47}$; $U_6 = Z_{48}$.

In this case, in turn, Z^{-1}_j modulo-$(2^{16}+1)$ multiplied by Z_j is 1. Furthermore, $-Z_j$ modulo-2^{16} added to Z_j is 0.

Patent Claims

1. A device for the conversion of in each case a given first binary digital block of a first length (N) into an associated second binary digital block of equal length (N) with the use of at least one freely selectable binary control block, characterised
- by at least one first input (25-26; 50, 51; 125-128) for inputting at least two first sub-blocks (X_1-X_4; e_1, e_2; e_5-e_8) of a second length (m) which together form the first digital block (X; W_n),
- by at least one second input (29, 30, 32, 33, 49, 52, 129, 130, 133) for inputting at least two control blocks (Z_1-Z_{52}) of the second length (m),
- by a logic means (40, 60, 61.1, 61.2, 140) which in each case and serially perform at least four logical operations of at least two different kinds ($\boxplus$, $\odot$, $\oplus$),
· wherein at least the predominant number of all pairs of immediately successive operations consist of two operations of different kinds ($\boxplus$, $\odot$, $\oplus$),
· wherein which by each operation in each case two input blocks (E_1, E_2) of the second length (m) are converted into an output block (A) of this length (m),
· wherein which first sub-blocks (X_1-X_4; e_1, e_2; e_5-e_8), control blocks (Z_1-Z_{52}) and/or output blocks (A) of a respectively preceding operation serve as input blocks (E_1, E_2) and
- by at least one output (75-78; 47, 48; 35-38) for outputting at least two second sub-blocks (W_{n1}-W_{n4}, Y_1-Y_4; a_1, a_2; a_5-a_8) of the second length (m) associated with the first sub-blocks (X_1-X_4; e_1, e_2; e_5-e_8) and which together form the second digital block (W_n, Y).

2. A device according to Claim 1, characterised

- in that at least one first input (50, 51) is provided for the input of two first sub-blocks (e_1, e_2),
- in that at least one second input (49, 52) is provided for the input of two control blocks (Z_5, Z_6),
- in that the logic means is a primary encryption logic (40) which in each case performs four logical operations of two different kinds ($\boxplus$, $\odot$),
  - wherein one after another, by the first operation the one first sub-block (e_1) is operated with the one control block (Z_5) in one kind ($\odot$),
  - by the second operation the other first sub-block (e_2) is operated with the output block of the first operation in the other kind ($\boxplus$),
  - by the third operation the output block of the second operation is operated with the other control block (Z_6) in the one kind ($\odot$) and
  - by the fourth operation the output block of the first operation is operated with the output block of the third operation in the other kind ($\boxplus$), and
- in that at least one output (47, 48) is provided for outputting two second sub-blocks (a_1, a_2),
  - wherein the one second sub-block (a_1) being the output block of the fourth operation and the other second sub-block (a_2) being the output block of the third operation.

3. A device according to Claim 1, characterised

- in that at least one first input (125-128) is provided for inputting four first sub-blocks (e_5-e_8),
- in that the logic means is an expanded encryption logic means (140) comprising a central logic

means and performs six logical operations of the third kind (⊕),

· wherein

- the first and the second operation of the third kind (⊕) operate the first (e_5) with the third (e_7) and the second (e_6) with the fourth first sub-block (e_8), respectively,
- the output blocks of the first and the second operation are operated by the central logic means,
- a first output block of the central logic means is operated with the first (e_5) and with the third first sub-block (e_7) by the third and the fourth operation of the third kind (⊕), and
- a second output block of the central logic means is operated with the second (e_6) and with the fourth first sub-block (e_8) by the fifth and the sixth operation of the third kind (⊕), and

- in that at least one output (35-38) is provided for outputting four sub-blocks (a_5 - a_8),

· wherein the first (a_5), the second (a_6), the third (a_7) and the fourth second sub-block (a_8) are associated respectively with the output block of the third, the fifth, the fourth and the sixth operation.

4. A device according to Claim 2 and 3, characterised in that

- at least one second input (49, 52) is provided for inputting two control blocks (Z_5, Z_6), and in that
- the primary encryption logic means (40) serves as a central logic means.

5. A device according to Claim 1 and 4, characterised in that

- at least one first input (25, 26) is provided for inputting four first sub-blocks (X_1-X_4; W_{n1}-W_{n4})

- in that at least one second input (29, 30, 32, 33, 49, 52) is provided for inputting six control blocks (Z_1-Z_6)
- in that the logic means is an encryption stage (61.1, 61.2) which in each case performs fourteen logical operations of three different kinds ($\boxdot$, $\odot$, $\oplus$),
· wherein by the first four operations in parallel the first first sub-block (X_1, W_{n1}) and the second first sub-block (X_2, W_{n2}) associated are operated with the first (Z_1) and the second control block (Z_2) in the second kind ($\odot$) and the third first (X_3, W_{n3}) and the fourth first sub-block (X_4, W_{n4}) associated are operated with the third (Z_3) and the fourth control block (Z_4) in the first kind ($\boxplus$),
· wherein the further ten operations being those of the expanded encryption logic means (140) and
· wherein the output blocks of the first four operations are the input blocks of the expanded encryption logic means (140) and
- in that at least one output (35-38) is provided for outputting four second sub-blocks (W_{11}-W_{14}; $W_{(n+1)1}$-$W_{(n+1)4}$),
which, interchanged cross-wise, correspond to the output blocks of the expanded encryption logic means (140).

6. A device according to Claim 1 and 4,
characterised in that
- at least one first input (25-28) is provided for inputting four first sub-blocks (X_1-X_4; W_{n1}-W_{n4}),
- in that at least one second input (29, 30, 32, 33, 49, 52) is provided for inputting six control blocks (Z_1-Z_6),

- in that the logic means is an encryption stage (61.1, 61.2) which performs in each case fourteen logical operations of three different kinds ($\boxplus$, $\odot$, $\oplus$),
· wherein by the first four operations in parallel the first first (X_1, W_{n1}) and the third first sub-block (X_3, W_{n3}) associated are operated with the first (Z_1) and the third control block (Z_3) in the second kind ($\odot$) and the second first (X_2, W_{n2}) and the fourth first sub-block (X_4, W_{n4}) associated are operated with the second (Z_2) and the fourth control block (Z_4) in the first kind ($\boxplus$),
· wherein the further ten operations being those of the expanded encryption logic means (140) and
· wherein the output blocks of the first four operations being the input blocks of the expanded encryption logic means (140) and
- in that at least one output (35-38) is provided for outputting four second sub-blocks (W_{11}-W_{14}; $W_{(n+1)1}$-$W_{(n+1)4}$), wherein the first (35) and the fourth output (38) corresponding directly and the second (36) and the third output (37) corresponding after cross-wise interchange to the output blocks of the expanded encryption logic means (140).

7. A device according to Claim 1 and 5, characterised in that
- at least one first input (25-28) is provided for inputting four first sub-blocks (X_1-X_4),
- in that at least one second input (29, 30, 32, 33, 49, 52, 129, 130, 132, 133) is provided for inputting a second plurality (T) of control blocks (Z_1-Z_{52})
- in that the logic means is an encryption unit (60) comprising a first plurality (S) of identical encryption stages (61.1, 61.2) which follow one another in such a way that the outputs of the relevant

preceding stage form the inputs of whichever is the following stage,

- in that the encryption unit (60) comprises a divergent final encryption stage (69) which performs in parallel four operations of two different kinds ($\boxplus$, $\odot$),
- in that at least one output (75-78) is provided for outputting four second sub-blocks (Y_1-Y_4) which correspond to the output blocks of the divergent final encryption stage (69),
- wherein the second plurality (T) is equal to six times the first plurality (S) plus four,
- wherein the first (W_{n1}) and the second output block (W_{n2}) associated are operated with the (T-3)rd and the (T-2)nd control block (Z_{49}, Z_{50}) in the second kind ($\odot$) and the third (W_{n3}) and the fourth output block (W_{n4}) of the preceding stage associated are operated with the (T-1)st and Tth control block (Z_{51}, Z_{52}) in the first kind ($\boxplus$).

8. A device according to Claim 1 and 6, characterised in that

- at least one first input (25-28) is provided for inputting four first sub-blocks (X_1-X_4),
- in that at least one second input (29, 30, 32, 33, 49, 52, 129, 130, 132, 133) is provided for inputting a second plurality (T) of control blocks (Z_1-Z_{52})
- in that the logic means is an encryption unit (60v) comprising a first plurality (S) of identical encryption stages (61.1v, 61.2v) which follow one another in such a way that the outputs of the relevant preceding stage form the inputs of whichever is the following stage,
- in that the encryption unit (60v) comprises a different final encryption stage (69v) which performs in parallel four operations of two different kinds ($\boxplus$, $\odot$),

- in that at least one output (75-78) is provided for outputting four second sub-blocks (Y_1-Y_4) which correspond to the output blocks of the divergent final encryption stage (69),
· wherein the second plurality (T) is equal to six times the first plurality (S) plus four,
· wherein the first (W_{n1}) and the second output block (W_{n2}) of the preceding final one of the identical encryption stages (61.1v, 61.2v) associated are operated with the (T-3)rd and the (T-2)nd control block (Z_{49}, Z_{50}) in the second kind ($\odot$) and the third (W_{n3}) and the fourth output block (W_{n4}) of the preceding stage associated are operated with the (T-1)st and the Tth control block (Z_{51}, Z_{52}) in the first kind ($\boxplus$), and
- wherein the second and the third input of the divergent final encryption stage (69v) are interchanged with each other.

9. A device according to Claim 7 or 8,
characterised in that
the second plurality (T) is equal to fifty-two and the first plurality (S) is equal to eight.

10. A device according to Claim 1,
characterised in that
- the operation of a first kind ($\boxplus$, addition modulo 2^m) is so disposed that
· each input block (E_1, E_2) of the operation is considered as an integer in binary representation and as an element of the quantity (0, 1, 2, 3..., (2^m-1)),
· that the associated output block (A) is the binary representation of the sum modulo 2^m of the input blocks (E_1, E_2)
- in that the operation of a second kind ($\odot$ multiplication modulo (2^m+1)) is so disposed

· that, in so far as all bits of a block (E_2, E_2, A) are zero, this block is regarded as the integer 2^m in binary representation,
· that otherwise each input block (E_1, E_2) is considered as an integer in binary representation and as an element of the quantity (1, 2, 3, ... (2^m-1)),
· that the associated output block (A) is the binary representation of the product modulo (2^m+1) of the input blocks (E_1, E_2)
- and in that the operation of a third kind ($\oplus$, bit-for-bit-exclusive-OR) is so disposed that
· each block (E_1, E_2, A) of the operation is considered as a sequence of bits, by which a fixed position is associated with each bit,
· and that in the sequence given by this, each bit of the output block (A) is the exclusive-OR of the two bits of the relevant position of the two input blocks (E_1, E_2).

11. A device according to Claim 10,
characterised in that
the second length (m) is either four, eight or sixteen.

12. A device according to Claim 1,
characterised in that
in order to carry out each individual logical operation an individually associated operation unit (41-44, 111-120) is provided which has two inputs for inputting the relevant input blocks (E_1, E_2) and an output for outputting the relevantly associated output block (A).

13. A device according to Claim 1,
characterised in that
in order to carry out the logical operations, operation units are provided which comprise at least

one common processor which links the inputted input blocks to one another in accordance with a predetermined programme.

14. The use of two devices according to Claim 7 for the encryption of a digital plaintext ($\underline{X}$) and for decryption the associated ciphertext ($\underline{Y}$),
wherein the plaintext ($\underline{X}$) is delivered continuously by a message source (11) and the ciphertext ($\underline{Y}$) is delivered by a transmission line (13) and fed block-wise by a respective input unit (21) to the inputs (25-28) of an encryption unit (60) or to a decryption unit identical thereto, respectively, as plaintext sub-blocks (X_1-X_4) or of ciphertext sub-blocks (Y_1-Y_4) of a second length (m), respectively,
wherein for the encryption and decryption a common secret key block (Z) is used, the resulting ciphertext sub-blocks (Y_1-Y_4) or the plaintext sub-blocks X_1-X_4), respectively, of the same second length (m) being delivered to a respective output unit (79) and being delivered continuously by this unit as a ciphertext ($\underline{Y}$) or as a plaintext ($\underline{X}$), respectively,
characterised in that
- from the key block (Z) as control blocks a second plurality (T) of encryption sub-blocks (Z_1-Z_T) or decryption sub-blocks (U_1-U_T), respectively, of the second length (m) are formed and are fed to the inputs (29, 30, 32, 33, 49, 52, 129, 130, 132, 133) of the encryption unit (60) or the decryption unit, respectively, which comprise a first plurality (S) of identical successive stages (60.1, 60.2), in such a way,
that for each stage i of the decryption unit
· a first and second decryption sub-block of each stage i (i = 1, 2 .... (S+1)), are identical to the modulo (2^m+1) multiplication inverses of a

respectively first and a second encryption sub-block in the (S-i+2)nd stage of the encryption unit (60),
· a third and fourth decryption sub-block in the i-th stage (i = 1, 2 .... (S+1)) are identical to the negative value of the modulo-2^m addition of a third and a fourth encryption sub-block in the (S-i+2)nd stage of the encryption unit (60) and
· a fifth and sixth decryption sub-block on the i-th stage (i = 1, 2 ... S) are identical to the fifth and the sixth encryption sub-block in the (S-i+1)st stage of the encryption unit (60).

15. The use of two devices according to Claim 8 for the encryption of a digital plaintext (X) and for decryption of the associated ciphertext (Y),
wherein the plaintext (X) is delivered continuously by a message source (11) and the ciphertext (Y) is delivered by a transmission line (13) and fed block-wise by a respective input unit (21) to the inputs (25-28) of an encryption unit (60v) or to a decryption unit identical thereto, respectively, as plaintext sub-blocks (X_1-X_4) or the ciphertext sub-blocks (Y_1-Y_4) of a second length (m),
wherein for the encryption and decryption a common secret key block (Z) is used, the resulting ciphertext sub-blocks (Y_1-Y_4) or plaintext sub-blocks (X_1-X_4) of the same second length (m) being delivered to a respective output unit (79) and being delivered continuously by this unit as a ciphertext (Y) or plaintext (X), respectively,
characterised in that
- from the key block (Z) as control blocks a second plurality (T) of encryption sub-blocks (Z_1-Z_T) or decryption sub-blocks (U_1-U_T), respectively, of the second length (m) are formed and are fed to the inputs (29, 30, 32, 33, 49, 52, 129, 130, 132, 133) of the encryption unit (60) or the decryption unit,

respectively, which comprise a first plurality (S) of identical successive stages (60.1v, 60.2v), in such a way,
that for each stage i of the decryption unit
· a first and fourth decryption sub-block of each stage i (i = 1, 2 .... (S+1)), are identical to the modulo (2^m+1) multiplication inverses of a respectively first and a fourth encryption sub-block in the (S-i+2)nd stage of the encryption unit (60v),
· a second and third decryption sub-block in the i-th stage (i = 2, 3 .... S) are identical to the negative value of the modulo-2^m addition of a third or second encryption sub-block in the (S-i+2)nd stage of the encryption unit (60v),
· a second and third decryption sub-block in the first and the (S+1)st stage are identical to the negative value of the modulo-2^m addition of a second and third encryption sub-block in the (S+1)st and the first stage of the encryption unit (60v) and
· a fifth and sixth decryption sub-block in the i-th stage (i = 1, 2 ... S) are identical to the fifth and sixth encryption sub-block in the (S-i+1)st stage of the encryption unit (60v).

16. The use according to Claim 14 or 15,
characterised in that
· the key sub-blocks (Z_1-Z_T) are obtained in that in a first step the key block (Z) is subdivided into eight first encryption sub-blocks (Z_1-Z_8) of the second length (m)
· in that in a second step the bits of the key block (Z) are cyclically offset by a predetermined bit number and the resulting new block is subdivided into eight further encryption sub-blocks (Z_9-Z_{16})
· and in that the second step is repeated until such time as all the encryption sub-blocks (Z_1-Z_T) are formed.

17. The use according to Claim 14 or 15, characterised in that the second plurality (T) is fifty-two and in that the first plurality (S) is eight and in that the second length (m) is sixteen.

Ten sheets of drawings