Symmetric-Key Encryption Algorithms

Worldwide experience in information protection systems convincingly demonstrates that all serious designs use cryptographic methods. This fact can be explained by one practical conclusion. Any software/hardware protection means necessarily uses particular features of the platform or chipset on the basis of which it has been implemented. From this standpoint, only cryptographic methods have sufficient versatility that permits to prescind from a specific type of information processing and transmission systems when developing information protection systems.

High reliability is another positive aspect of cryptographic methods of information protection. Properties of cryptographic algorithms are substantiated under conditions when the enemy knows not only a ciphertext, but also description of the encryption process and, in some cases, even has additional opportunities associated with obtrusion or selection of a specified plaintext.

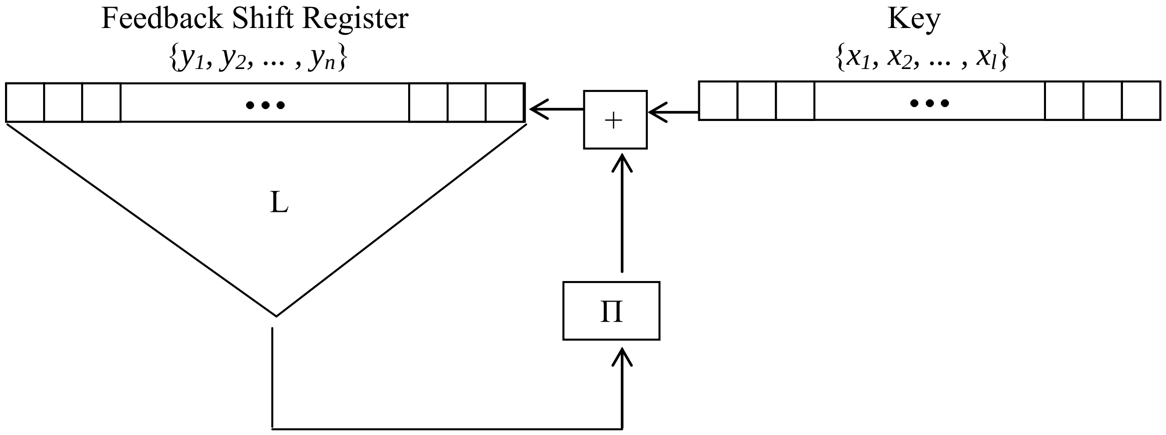
The third important aspect of cryptographic protection methods is associated with the possibility to create cryptographic algorithms with specified operational characteristics – required format of processed data, speed, software or hardware implementation.

Low-Speed Encryption Algorithms (up to 1 Mbyte/sec)

The use of cryptographic algorithms in electronic commerce and computerized payment systems imposes a number of specific requirements for utilized cryptographic solutions. Utilized algorithms must be easy to implement with any computing machinery, including the simpliest microcomputers with very limited hardware resources. On the other hand, decimal notation of data is most often the principal form of data representation in payment systems. The necessity of combining all mentioned requirements has led to creation of a dedicated automatic coding system having an original cryptographic algorithm.

Description Of The *Signal* Automatic Coding System

For encryption, automatic coding systems utilize a keystream overlay node that uses modulo 10 operations. In order to obtain one-time keys, the following block-type transformation is used, instrumented with an feedback shift register on the ring Z/100 of the residues of integral numbers to the modulus 100:



The transformation is made with the blocks $y_1, y_2, \dots ,y_n$, where for $y_i \in Z/100$:

$(y_1, y_2, \dots ,y_n) \to (y_{k+1}, y_{k+2}, \dots ,y_{k+n})$,

$(y_{k+1}, y_{k+2}, \dots ,y_{k+n})$ are state obtained from the formula

$y_{i+n} = \Pi(\mathrm{L}(y_i, y_{i+1}, \dots , y_{i+n-1},)) + x_i,\ i=\overline{1,k}$.

Π is a fixed substitution from the symmetrical group of degree 100, $x_1, x_2, \ldots ,x_k$ is an input word dependent on the key, $x_i \in Z/100$, $i=\overline{1,k}$. Feedback function L is an operation on the ring Z/100.

The diagram of a coding system consists of three blocks (Fig. 1):

- one-time key generation block;
- keystream generation block;
- keystream overlay block.

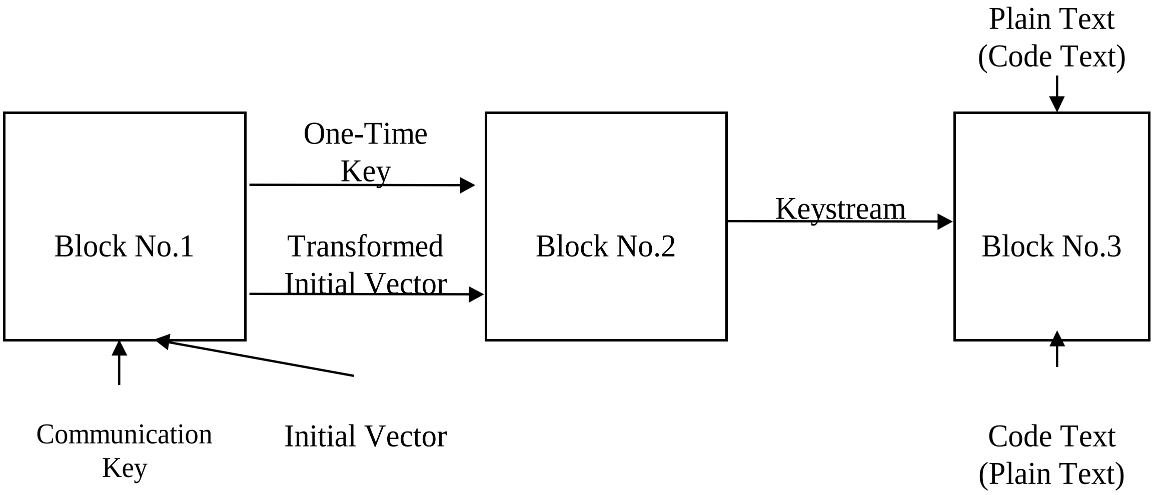


Figure 1. Diagram of a coding system.

Block No.1 generates the one-time key for a message on the basis of the communications key and initial vector. As an initial state for the shift register, a double initial vector of a message ($t_1, \ldots, t_{n/2}$) is used:

$(y_1, \ldots, y_n) = (t_1, \ldots, t_{n/2}, t_1, \ldots, t_{n/2})$: $y_i \in Z/100$, $i=1 \div n$, $t_j \in Z/100$, $j=1 \div n/2$.

Block No.2 generates a keystream on the basis of the one-time key. Its diagram is shown in Figure 2.

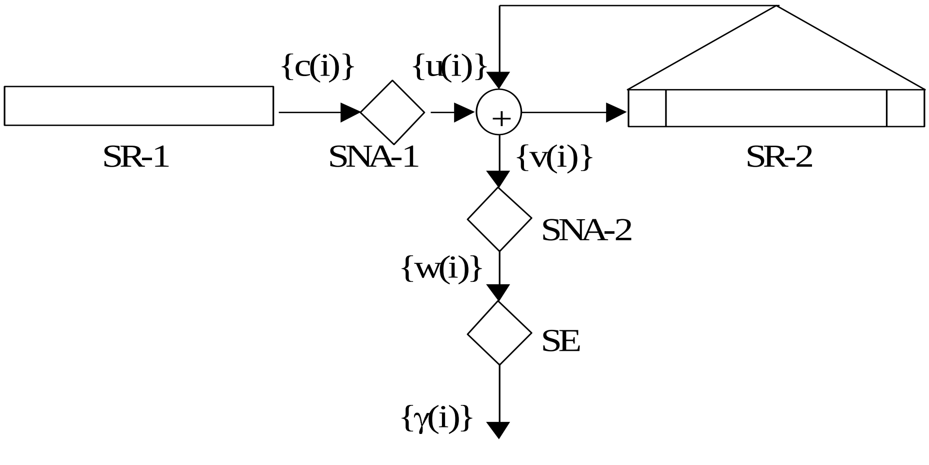


Figure 3. Diagram of Block No.2.

Here, SR-1 is an linear feedback shift register that implements a counter sequence, SNA-1 and SNA-2 are transformations determined by shifting nonalgebraic adders, SR-2 is an linear feedback shift register, SE is a keystream character splitting element that produces sequence counts {γ(j)} of the resulting keystream to the modulus 10.

As a result of implementation of Block No.2, a keystream sequence {γ(*j*)} enters Block No.3. Its length is determined by the length of a plaintext (in case of encryption) or the length of a ciphertext (in case of decryption).

After that, a code text (in case of decoding) or primary text (in case of encoding) is residuated on the character-at-a-time basis from the gamming sequence γ to the modulus 10. A sequence of ASCII codes for the plain text characters serves as a primary text for alphanumeric data processing.

The key system of the Automatic Coding System includes:

- a public communications key $(x_1, x_2, ... ,x_l)$, $x_i \in Z/100$, $i=\overline{1,l}$;
- a system of message markants $\{(t_1, ..., t_{n/2})\}$, $t_j \in Z/100$, $j=\overline{1,n/2}$.

A markant is generated with the use of the pseudorandom-number generator. A markant is inserted into a telegram in clear form.

The algorithm described above can also be used as an encryption algorithm. However, it should be noted that the *Signal* Automatic Coding System can be used also as an authentication code generating system in possible payment systems in the banks.

A possibility to process data in decimal notation should be emphasized as an original feature of the developed system. Experienced cryptographers know that, in data processing, a formal transition from one notation to another creates potential weaknesses in a cryptographic algorithm and gives cryptoanalysts possibilities to develop effective cryptanalysis methods. Moreover, data conversion from one form to another requires additional time and resources. Decimal data-processing mode in the *Signal* system uses an original algorithm, based on the decimal arithmetic properties, and does not involve techniques of binary operation adaptation to a specified data format.

While comparing cryptographic algorithms of the *Signal* Automatic Coding System with known standards of cryptographic data protection, it should be noted that, despite the principle of block encryption common to them, the solutions utilized are original from the cryptographic point of view and do not belong, unlike the above-mentioned standards, to the Feistel class schemes.

TIGER Encryption Algorithm

A shift register R1 with linear feedback of length 101, containing numbers to the modulus 7, is a main component in a scheme that implements the TIGER encryption algorithm. In one clock cycle of the scheme, 24 characters of the keystream are generated, that constitute numbers to the modulus 7 and are called a keystream-vector. This keystream-vector is determined by the R3 register status that is updated three times prior to generation of the next initil vetor, with such updating being accomplished by way of addition of certain elements from R1, polynomial transformation Ω and linear mapping Ψ. The modulo 7 sum of the keystream and a plaintext, transformed into numbers to the modulus 7, is taken.

Non-linear polynomials Ω, applied twice to the key-dependent input data prior to encryption, serve as a basis for encryption.

A key consists of 101 characters to the modulus 7. An initial vector *m* that is transmitted in clear mode and is not confidential. Using the initial vector *m* and parameter *c*, a key is loaded into the register R1 at the beginning of encryption.

In 1996, the TIGER algorithm obtained a certification in the Republic of South Africa.

High-Speed Encryption Algorithms (up to 10 Mbyte/sec)

When developing data encryption systems having the rates up to 10 Mbyte/sec, designers have to consider the architecture and possibilities of those computer systems that would be an implementation basis for such encryption systems.

At the present time, block and stream encryption schemes are the principal types of cryptographic algorithms. Despite the fact that block algorithms are both Russian and American standards, the experts currently do not recommend to use block ciphers to encrypt long messages. This is because block ciphers in the electronic code book mode do not permit to reveal such error as a loss of individual blocks, which is particularly critical in the payment systems. Therefore, when long messages are to be encrypted, preference is given to such block cipher modes as the block-linking encryption or ciphertext feedback encryption. In both cases processing of information reduces virtually to the stream data processing. Therefore, specialists, based on analysis of the best efforts of the world cryptography in cryptographic algorithms of up to 10 Mbyte/sec, created an original class of highly strong stream cipher algorithms permitting effective software and hardware implementation.

Transformations utilized in this cryptographic algorithm give maximum consideration for the possibilities of standard computer systems available on the world market of computing machinery.

Cloud Encryption Algorithm

This algorithm is designed for encryption and decryption of data represented in a byte form. Encryption and decryption is accomplished using the primary key - $K=(k_1, k_2, ..., k_n)$, $k_i \in GF(2)^8$, $i=\overline{1,n}$.

A keystream generator is shown in Figure 4.

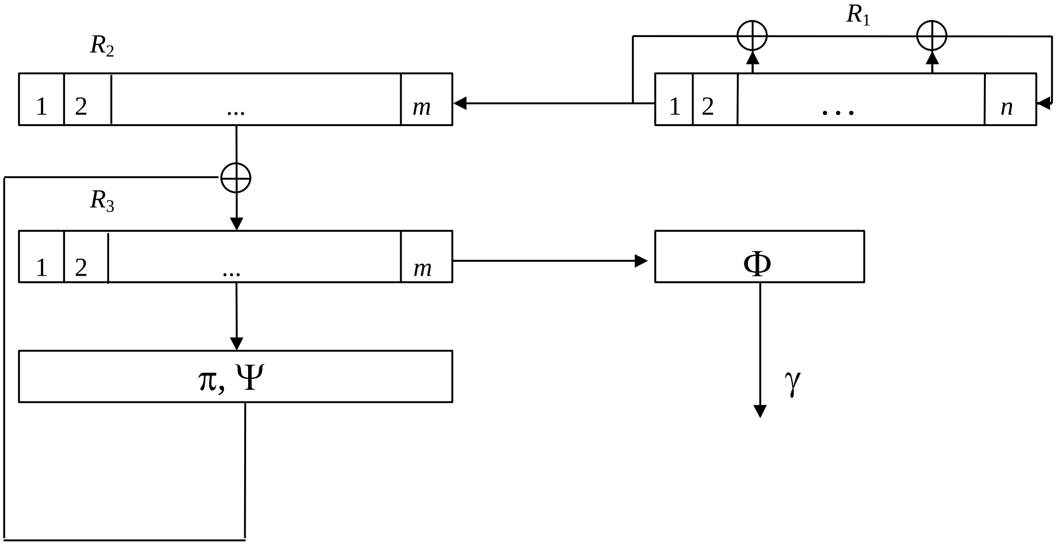


Figure 4. Keystream γ computation.

In this Figure, R_1 and R_2 are shift registers of length n and m bytes correspondingly; R_3 is a shift register of length m bytes; $\mathit{\Pi}$ is transformation Π:GF(2^{8m}) → GF(2^{8m}) of a form $\Pi(x_1, x_2, ..., x_m) = (\Pi_1(x_1), \Pi_2(x_2), \dots, \Pi_m(x_m))$, where Π_i is transformations Π_i:GF(2^8) → GF(2^8) defined in tabular or polynomial form; Ψ is a linear transformation $\Psi: GF(2)^{8m} \rightarrow GF(2)^{8m}$ defined by matrix A, $\Psi(X)=XA$; Φ is a transformation $\Phi: GF(2)^{8m} \rightarrow GF(2)^{8m}$, $\Phi(x_1, x_2, ..., x_m) = (\Phi_1(x_1), \Phi_2(x_2), \dots, \Phi_m(x_m))$.

Transformations Φ_i, Φ_i:GF(2^8)→GF(2^8) are defined in tabular form.

A primary key $K=(k_1, k_2,..., k_n)$ consists of n bytes.

An initial vector (markant) $v=(v_1, \dots, v_l)$ includes bytes. The markant is generated with the use of a program random-number generator that must ensure random, equiprobable and independent selection of elements from GF(2^8).

At the beginning of the scheme operation, the keys are entered into the register R_1 using the on-line shift register R_4 that ensures generation of a session (one-time) key dependent on the primary key and initial vector.

A value $\Phi(R_3)$ (i.e. a vector of length m bytes) after each scheme cycle is a keystream block. One scheme cycle consists of 3 steps.

Step i, $i=\overline{1,3}$. The transfer register R_2 is filled up with the help of the linear register R_1. After that, the register R_3 changes its status in the following way:

$$R_3^{(t+1)} = R_2^{(t)} \oplus \mathrm{F}_i(R_3^{(t)}),$$

with

$$F_i(R_3^{(t)}) = \begin{cases} \Pi(R_3^{(t)}), & i = 1; \\ \Psi(\Pi(R_3^{(t)})), & i = 2,3. \end{cases}$$

The statuses of registers R_1 and R_3 after the 3rd step are initial for generation of the next keystream block.

A plaintext is broken down into blocks of *m* bytes each. Plain text characters are encoded on the byte by byte basis. A generated keystream, treated as a concatenation of serial blocks, is also represented in a byte form. When the last block is not full, it is supplemented by a fixed character. A ciphertext has the following structure. A markant is used as the first *m* bytes of a ciphertext, *m* bytes of a plain text, enciphered with the next *m* bytes of the keystream, are used as the second block. Encryption is accomplished by way of XOR addition with appropriate sign of the keystream.

The structure of a ciphertext appears as follows:

Initial vector (*m* bytes)	The first block of ciphertext (*m* bytes)	The second block of ciphertext (*m* bytes)	. . .

So, ciphertext characters are represented by bytes. An initial vector markant (*m* bytes) is taken from the first block of the ciphertext. Decryption is accomplished by way of bitwise addition with appropriate sign of the keystream to the modulus 2.

It should be noted that our company follows a policy of using various cryptographic solutions depending on functionality of produced protection means. In doing so, it places a special emphasis upon service performance of the offered means. From this standpoint, the Company-developed class of high-speed encryption algorithms permits, on the one hand, to resolve the problem of data security in the most common telecommunication and information systems and, on the other hand, to construct, by changing algorithm parameters, a class of cryptoschemes having a wide range of capabilities.

Very-High-Speed Encryption Systems (up to 10 Gbyte/sec)

Our Company has developed a cryptographic security device *Eagle* that ensures encryption rates of up to 1.6 Gbyte/sec with the use of modern computer systems and information processing techniques.

The encryption principle has been implemented based on combination of two block algorithms. The use of a dual-processor computer permits these algorithms to operate consistently in a parallel mode. The first algorithm directly implements a high-speed block encryption algorithm with a small amount of key. The second algorithm generates keys to encipher the next data array, which are subject to change in the process of encryption. Encryption strength is ensured by dynamic change of a key. Such approach permits to increase data processing rates without prejudice to the scheme strength due to reduced amount of key and number of iterations in the block encryption algorithm. On the other hand, such separation of functions allows to decrease requirements for the speed of the running key generating algorithm and use known and well-examined cryptographic algorithms for that purpose.

High speed of the *Eagle* device is ensured not only by technical capabilities of modern computer systems allowing to implement an approach that involves execution of encryption and running key generating functions in a parallel mode. An implementation of "pipeline processing" and "preliminary computing" principles contributes greatly to increasing efficiency of the *Eagle* system. With the "pipeline processing", during encryption of a data block substantial amount of computation is executed that is required for encryption of the next block. "Preliminary computing" allows to perform time-consuming and frequent transformations of encryption and running key generating algorithms only once at the preliminary stage.

Therefore, an alloy of advanced technical solutions and scientific potential of our company allowed to develop a cryptographic protection means that is superior to the known domestic and foreign analogs in capabilities.

Eagle is the first one in a series of high-speed information protection means under development. The second version of this product is in development stage, with expected performance increase of up to 30%. New modifications of encryption algorithms are based on advanced information processing techniques. Multithreading techniques, that allow maximum use of processor capabilities due to minimization of downtime during memory accessing operations, provided new possibilities for application of parallelization principles in creation of high-speed encryption algorithms.

The use of *Eagle* in the ready-keystream information security systems should be noted separately. Such systems implement a gamming cipher in which a random sequence is generated in advance and stored on a special medium in a ready form. This line was animated by a wide use of computer engineering in information protection, when storage and in-line processing of large data arrays became possible. If randomness and equiprobability of a keystream is ensured and its repeated use is excluded, then the ready- keystream gamming cipher could be assigned to absolutely resistant high-speed cryptographic protection means.

Cryptographic Algorithms For Voice Data Protection

Analog and digital encoders are used as voice data protection algorithms.

Analog encoders, or scramblers, performed very well in secure communications networks with any types of PBX, including **Hicom** and **Ericsson**. Flexible software allows to account for virtually any customer's requests and guarantees excellent performance in severe environment.

Scramblers are used to encrypt voice signals and secure fax messages transmitted via public telephone networks. Providing temporal cryptographic protection, they operate with stability in the duplex mode in real telephone circuits, including long-distance and international lines with satellite and radio-relay insertions and any types of multiplexing, and provide compatibility with all types of telephone and facsimile sets, with any types of mini ATX possessing an analog output.

Scramblers use a mosaic encryption method: frequency and time displacements are used that ensure high quality of restored voice. Both symmetric keys and key systems based on public key cryptographic methods are used for setting-up calls. An additional key can be introduced for the purpose of subscriber identification.

Along with it, unauthorized data reading from the link becomes absolutely impossible, even with the use of the third similar device (the third scrambler cannot be synchronized).

At the present time, a new concept of voice and facsimile data protection is implemented fairly frequently, by analogy with GSM technology, within the section of a telephone link between a subscriber and a city station exchange. If a scrambler or identical complex is available to the other party, encryption of the whole communications path between the subscribers is possible. In this case, scramblers installed at the city exchange do not participate in a secure communications session and are "by-passed".

As a whole, a scrambler is a compact, fully autonomous encoding device that permits confidential conversations from any telephone set, including public pay phones, radiophones and cellular phones. A scrambler provides protection against both direct listening and interception with the use of embedded devices connected to the telephone link. However, scramblers that belong to the analog telephony class, as stated above, are capable of providing only temporary protection.

Unlike the analog telephony, the digital telephony transforms voice signals into a digital form and transmits them, as separate packages, via communications circuits. In this case, modems in such networks as public, leased, satellite, ISDN and GSM networks can be used as channeling equipment.

All telephony types are characterized by the necessity to process signals in real time mode in order to improve consumer qualities of equipment by reducing delays in transmission of voice signals via communications circuits. Therefore, the digital telephony places fairly stringent requirements upon encryption rate and timing cycle (secure communications restoration period) of the utilized cryptographic algorithms.

With binary information transmissions, such malfunctions as distortion, addition and loss of individual bits or groups of bit are critical for the block ciphers and the most characteristic of the digital telephony. In this case, the main concern of a cryptographer is to minimize propagation of such errors at the receiving end in order to maintain voice quality to a maximum degree. For Internet telephony, one more specific feature turns out to be the fact that in Internet transmissions a delay may be too great, or individual packages may arrive at the receiving end not in the same order they have been transmitted.

Therefore, high-speed stream ciphers with a short timing cycle may be recommended to use as an encryption algorithm. This solution was used by our company for the development of *AncVoiceCoder* telephone encoders.