DOI https://doi.org/10.36059/978-966-397-104-9/118-138

INFORMATION PROTECTION

Domnich V. I.

1. Information security issues

Internet and information security are incompatible by nature. It was born as a purely corporate network, but now, through a single stack of TCP / IP protocols and a single address space, it connects not only corporate and departmental networks (educational, government, commercial, military, etc.), which is by definition, restricted networks, but also ordinary users who are able to access the Internet directly from their home computers through modems and a public telephone network[1].

It is known that the easier access to the Web, the worse its information security, so it is reasonable to say that the original ease of access to the Internet – worse then theft, because the user may not even know that they were copied – files and programs, not to mention the possibility of spoiling and correcting them.

What determines the rapid growth of the Internet, which is characterized by an annual doubling in the number of users? The answer is simple – "freebie", that is, cheap software (TCP / IP), which is now included in Windows 95, ease and cheap access to the Internet (either by IP address or provider) and to all the world's information resources.

Paying for the use of the Internet is a general reduction of information security, so to prevent unauthorized access to their computers, all corporate and departmental networks, as well as enterprises using the Internet technology, put filters (firewall) between the internal network and the Internet, which in fact means leaving the single address space.

Even greater security will be given away from TCP/IP and access to the Internet through gateways.

This transition can be done simultaneously with the process of building a worldwide public information network, based on the use of network computers, which, using a 10Base-T network card and cable modem, provide high-speed access (10 Mbps) to a local Web server via a cable network TV.

[1] Библиотека Сетевой Безопасности URL: http://securitv.tsu.ru.

To address these and other issues when transitioning to the new Internet architecture, you must provide the following:

First, to eliminate the physical connection between the future Internet (which will become the World Wide Web Information Organization) and corporate and departmental networks by retaining only an information link through the World Wide Web.

Second, replace the routers with switches by switching off processing at the nodes of the IP protocol and replacing it with Ethernet frame broadcast mode, in which the switching process is reduced to a simple MAC address comparison operation.

Third, to move to a new single address space based on physical access points to the transmission medium (MAC layer), tied to the geographical location of the network, and within 48-bits to create addresses of more than 64 trillion nodes.

Data security is one of the major problems on the Internet. More and more scary stories are emerging about how hackers, using increasingly sophisticated techniques, get into other people's databases. Of course, all this does not contribute to the popularity of the Internet in business.

The mere thought that some hooligans, or worse, competitors, will be able to access commercial data archives is forcing corporate executives to refuse to use open information systems.

Experts say such fears are unfounded because companies with access to both open and private networks have almost equal chances of becoming victims of cyber terror.

Every organization that deals with whatever values are facing their encroachment sooner or later. The prudent start planning protection in advance, the unpredictable – after the first major "puncture". One way or another, the question arises as to what, how and from whom to protect.

Usually the first reaction to a threat is the desire to hide the values in an inaccessible place and to protect them. This is relatively straightforward when it comes to values that you don't need for a long time: taken away and forgotten. It is much more difficult if you need to work with them constantly.

Each request to the store for your values will require a special procedure, will take time and will create additional inconvenience. This is the security dilemma: you have to choose between the security of your property and its accessibility to you, and therefore the ability to use it.

All this is true in relation to information. For example, a database containing sensitive information is only then fully protected against encroachment when it is on disks removed from the computer and stored in a secure place.

Once you have installed these disks on your computer and started using them, there are several channels at which the attacker, in principle, has the opportunity to access your secrets without your knowledge. In other words, your information is either inaccessible to anyone, including you, or not 100 percent secure.

It may seem that there is no solution to this situation, but information security is the same as maritime security: both are possible only with some tolerable degree of risk.

In the area of information, the security dilemma is worded as follows: one must choose between the security of the system and its openness. It is more correct, however, to speak not of choice but of balance, since a system that does not possess the property of openness cannot be used.

In the banking sector, the problem of information security is complicated by two factors: first, almost all the values that the bank deals with (except cash, etc.) exist only in the form of one or another information. Secondly, a bank cannot exist without connections with the outside world: without customers, correspondents, etc. At the same time, the information that expresses the values with which the bank works (or information about these values and their movements, which sometimes cost more than the values themselves) is necessarily transferred from the links.

Documents are coming in from outside which the bank transfers money from one account to another. Outside, the bank sends orders to move funds to correspondent accounts, so that the bank's openness is set first.

It should be noted that these considerations hold true not only for automated systems, but also for systems built on traditional paper-based circulation and utilizing links other than courier mail.

Automation has added a headache to security services, and new developments in the banking industry, based entirely on information technology, are compounding the problem.

2. Basic methods of protection against remote attacks on the Internet

The simplest and most inexpensive are the administrative security methods: the use of persistent cryptography, static ARP tables, hosts files

instead of dedicated DNS servers, the use or non-use of certain operating systems, and other methods.

The following group of remote attack protection methods are firmware:

- network hardware encryption hardware;
- Firewall methodology;
- secure network crypto protocols;
- attack detection software (IDS – Intrusion Detection Systems or ICE – Intrusion Countermeasures Electronics);
- security analysis software tools (SATAN – Security Analysis Network Tool for Administrator, SAINT, SAFEsuite, RealSecure, etc.);
- secure network OS.

In general, the Firewall technique implements the following basic functions:

- multi-level filtering of network traffic; Proxy schema with additional authentication and user authentication on the Firewall host. The meaning of a proxy scheme is to create a connection to a destination through an intermediate proxy server on a Firewall host;
- creating private networks with "virtual" IPs. Used to hide the true topology of the internal IP network.

Here you can distinguish a subset of security methods – software methods. These include primarily crypt protocols, which can improve the security of connection protection.

3. Modern cryptographic methods

3.1 Introduction to Cryptography

The rapid development of cryptographic systems were during the first and second world wars. From the postwar period to the present day, the advent of computing has accelerated the development and improvement of cryptographic methods[2].

The problem of using cryptography methods in information systems is now particularly urgent because, on the one hand, the use of computer networks, in particular the global Internet network, through which large amounts of information of state, military, commercial and private nature

[2] An Introduction to Computer Security: The NIST Handbook. Draft. – National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 1994. 310 c.

are transmitted, does not allow access to it bystanders. On the other hand, the emergence of new powerful computers, network and neural computing technologies has made it possible to discredit cryptographic systems, which have recently been considered virtually undisclosed.

The problem of information protection through its transformation is addressed by cryptology (kryptos – secret, logos – science).

Cryptology is divided into two areas – cryptography and cryptanalysis. The purpose of these directions is the exact opposite.

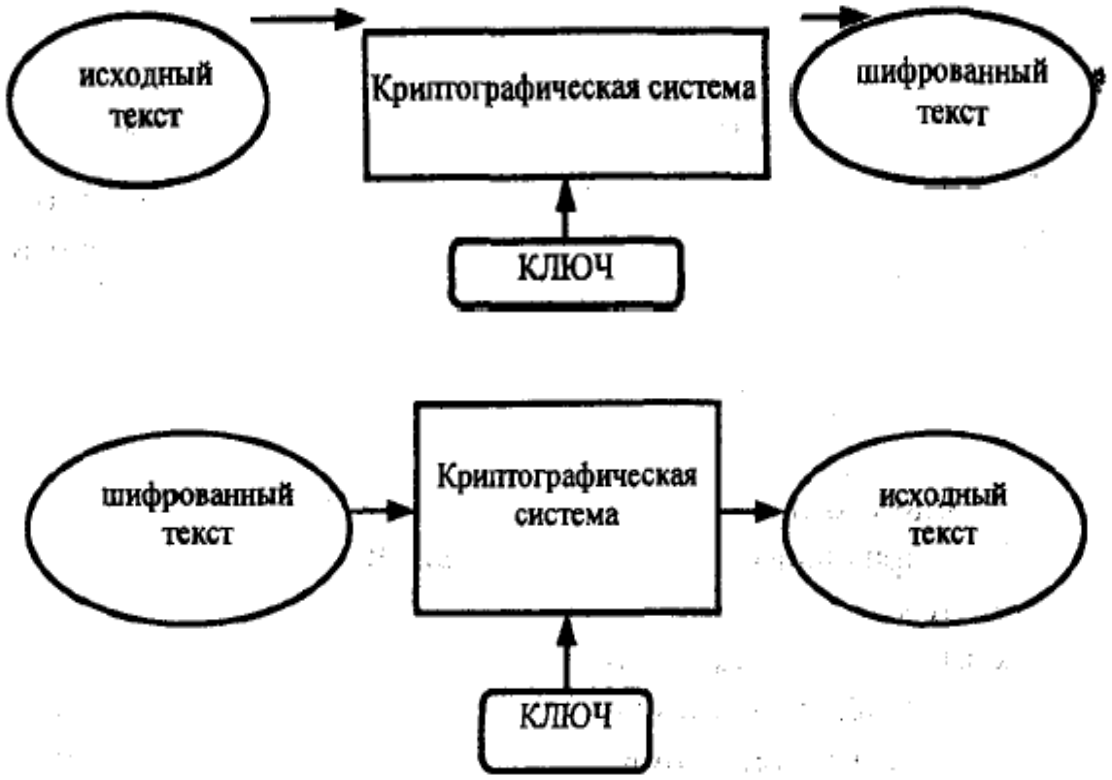
Cryptography deals with the search and research of mathematical methods of information transformation.

The area of interest of cryptanalysis is exploring the possibility of decrypting information without knowing the keys. "

Encryption is a transformative process: the source text, also called plaintext, is replaced by encrypted text.

Decryption is the reverse of the encryption process. Based on the key, the digitized text will be converted to output. Based on the key, the digitized text will be converted to output.

The key is the information needed to seamlessly encrypt and decrypt texts.



Cryptosystems are divided into symmetric and public key systems. In symmetric cryptos, the same key is used for both encryption and decryption.

Public key systems use two keys, public and private, that are mathematically related to each other. The information is encrypted with a public key accessible to all comers and decrypted with a private key known only to the recipient of the message.

An electronic (digital) signature is called text-encrypted conversion, which, when received by another user, verifies the authorship and authenticity of the message.

Crypto-stability is called the characteristic of a cipher, which is its resistance to decryption without knowing the key (ie cryptanalysis). There are several indicators of crypto-stability, including: the number of all possible keys; the average time required for cryptanalysis.

In the past, cryptography was only used for military purposes. But now, with the emergence of the information society, it is becoming a central tool for privacy.

As the information society is formed to the great powers, technological means of total surveillance of millions of people become available. Therefore, cryptography is becoming one of the main tools for securing privacy, trust, authorization, electronic payments, corporate security and countless other important things.

Encryption details. Encryption is the reverse conversion of data to hide them from third parties. Encryption methods have been devised in many ways – from simple-to-replace ciphers (the most famous example is Conan Doyle's "Dancing Men") to the Vernam cipher (binary addition of source text with a single random sequence).

Almost all encryption methods use the encryption key, a secret code sequence that is used in the information conversion process. Somewhere even read the following definition of encryption: "Encryption is the process of replacing your big secret (document) with a small one (key)."

If Vernam encryption is used, the encryption key is the length of the encrypted message, and must still be used once. Although Vernam's cipher, when properly used, provides "absolute" secrecy, it is not convenient for most applications. Modern cryptosystems use a key to encrypt 64 to 1024–2048 bits in length.

The tradition of measuring the key length in bits will probably stay with us forever. The question is – where did these figures come from, and why is TripleDES considered to be no less reliable than the 1024-bit RSA? And in general, how does the reliability of encryption (or, as they say, the stability of the cipher) depend on the length of the key used?

In order to answer these questions, you need to understand what encryption algorithms are currently used in practice. Generally, "classical ciphers" are called symmetric block ciphers. That is, those who use the same key to encrypt and decrypt information and encrypt information with blocks. The block length is usually 8 or 16 bytes.

There are algorithms that allow for variable block length. The first block cipher, widely used in practice, became DES (Data Encryption Standard), developed by IBM specialists in the early 70's of the last century and for a long time served as the standard for encryption of data in the United States. Then came many block algorithms – IDEA, Blowfish, Soviet GOST 28147-89 (and now is the Russian standard).

The original DES, for example, used a 112-bit key and a 64-bit encryption block. But after its analysis by NSA experts, the key length was reduced to 64 bits. In the key, there were only 56 bits of unique, and 8 bits of control, employees to control the integrity of the key. It is with a key length of 56 bits DES and has been approved as the National Standard.

At the same level of development of computers, the task of sorting 256 keys in an acceptable time was either technically not feasible or unreasonably expensive. Currently, a DES with a key length of 56 bits does not seem to be a stable algorithm.

Most modern symmetric algorithms use a key length of 64–256 bits (8–32 bytes). The following are the main currently used algorithms, their block lengths and key lengths.

Алгоритм	Длина ключа (в битах)	Длина блока (в битах)
DES	64	64
Blowfish	Переменная до 448 бит	64
IDEA	128	64
ГОСТ 28147-89	256	64
RC5	Переменная	Переменная

It should be noted that in addition to block ciphers, streaming ciphers exist and are being actively used. They, like block ciphers, use a symmetric key, but they encrypt the input stream byte or, sometimes, byte.

The idea behind the current cipher is that a symmetric key produces a key sequence, or a gamma sequence, which is modulated with an input stream. Streaming encryption is typically more productive than block cipher and is used to encrypt language, network traffic, and other data of a previously unknown length. With a fairly frequent change of key to produce gamma, the stream ciphers provide sufficient stability.

In particular, GSM-standard mobile communication provides the ability to encrypt the transmitted voice stream at a site from the telephone to the base station with a cipher that is streamed by it. One instructive story is associated with this algorithm. Initially, the description of the algorithm was closed. But due to a legal error of the company that owns the algorithm, its description has hit the Internet and the algorithm has been analyzed. Its resistance was even lower than that of DES.

Recognizing the importance of openness of algorithms to ensure their stability, developers of the third generation of GSM network have promised to make the proposed algorithms for voice encryption be acquired by the general cryptographic public. The example shows the importance of having an open description of the algorithm, even for its developers.

To date, algorithms with a key length of 64 bits or more provide acceptable stability.

The use of asymmetric cryptography radically simplifies the process of key distribution. The public key was therefore called "public" that it is no secret.

You can create a public "public key directory" where you can place the public keys of all participants in the exchange. In this case, each key owner is free to withdraw his key from the directory or replace it – this procedure will not affect the other participants of the exchange. This raises the problem of the authenticity of the key in the directory, but it is solved. But for convenience, you have to pay.

In the case of asymmetric cryptography, the key is the time and length of the keys. The characteristic length of the keys is when using asymmetric cryptography – 512–1024 bits. Now that high-performance computing systems are available, the use of 2048-bit keys is gaining popularity.

Is it possible to shorten the encryption time by keeping the asymmetric cryptography handy and adding block cipher speed? It turns out you can. They usually come as follows: produce a random (or pseudorandom) sequence and use it as a one-time (so-called session) key to encrypt a document with a fast symmetric algorithm. Then, using an asymmetric algorithm, they encrypt the session key and transmit it in encrypted form with the document.

When decrypting a document, first decrypt the session key, and then the document itself.

Because the session key is of small length, it takes a little time to encrypt it. Currently used symmetric crypto algorithms have a performance of about megabytes per second (for software implementations) and tens of megabytes when using specialized cryptoprocessors.

Asymmetric algorithms show performance from one to tens of kilobytes per second, depending on the length of the key. With a session key of 8-32 bytes, such a hybrid crypto scheme is quite effective.

3.2 A brief description of the basic data encryption algorithms

What is Blowfish? Blowflsh is a 64-bit block cipher developed by Schneier in 1993. This is a Feistel cipher and each pass consists of a permutation key dependent and a replacement key dependent. All operations are based on XORs and additions on 32-bit words.

The key has a variable length (max 448 bits) and is used to generate multiple subkey arrays. The cipher was created specifically for 32-bit machines and significantly faster DES.

In 1994, Dr. Dobb magazine sponsored an open competition with a $ 1,000 prize. This competition ended in April 1995 and several weak keys were found among the results. However, Blowfish may be considered secure, and Schneier invited crypto-analysts to continue investigating his code.

What is DES? DES (Data Encryption Standard) was announced in 1977 by the US National Bureau of Standards and was formally recognized as a result of the work of Subcommittee X3.92 of the US National Institute of Standards in 1981 (ANSI X3.92-1981, American National Standards Data Encryption Algorithm, © American National Standards Institute, 1981).

DES's status as a US national standard has aroused wide interest from both equipment developers and cryptographer theorists around the world. DES is based on national standards in some other countries of the world, such as Australia – Australian Standard AS2805.5-1985.

DES has penetrated and is widely used in Russia as an integral part of various software and hardware, of which the most widely known are the S.W.I.F.T. system, VISA and EUROPAY secret modules, ATMs and trading terminals, and, finally, smart cards.

Particularly intense debate over data encryption algorithms is caused by smart cards. However, there are good reasons to believe that the reliability of Russian cryptosystems of conversion origin will be superior to foreign counterparts.

DES's mathematical studies are devoted to thousands of huge investments. The general conclusion that can be drawn from open publications is that today DES sufficiently satisfies the requirements of reliability and there are no known methods of its direct reading (decryption) when fulfilling the relevant requirements for keys.

A little excursion into theory. The encryption algorithm is the implementation of some ambiguous mathematical function of converting one data (open) to other data (closed). This conversion is performed on the basis of some exclusively secret data – encryption keys, which are only owned by members of the secret correspondence. If the encryption algorithm itself is not a secret, and moreover, widely published, it is clear that the reliability of the secret is equivalent to the reliability of storage and use of keys.

All this is correct with one very important caveat – the algorithm itself must be a "very random" function and not generate a direct or statistical dependence of the closed data on the source-open data. This, in fact, is the mathematical understanding of crypto reliability.

Stability is an exceptionally broad concept, the number of which is considered to be the number of mathematical operations that can be read with certainty to read this encrypted message. It is clear that knowing the time of one elementary operation, you can calculate how much time, money, computers, etc. will be necessary for the attacker to acquire secret knowledge.

Let's look at a specific type of DES – encryption on keys 56 bits long (in fact – 8 bytes, but every lower bit – checks and is not used in

encryption). Since we seem to have tuned in to crack this code, then we will arm ourselves with a calculator and figure out what we will do.

Output: You should try to decrypt your existing encrypted text into 2^{56} possible key variants, that is, perform DES decryption approximately 10^{15} times.

Since the DES operation is long enough, we will immediately have a dedicated processor that performs 105 DES operations in 1 sec. priced at $ 20 per chip. Breaking the ciphers is serious, so let's build a computing system with thousands of such chips.

The result: a simple calculation shows that it will take us 10 million seconds to operate such a system, that is, about 3,000 hours. The code is broken for a total of 115 days.

You can doubt the possibility of creating the described cryptosystem, however, jokes aside, for the skeptics, here's a help: someone Matsui made a successful attack on a one-time DES, the code was broken 50 days later with 12 workstations HP 9735. Special methods of theoretical stability reduction were applied.

Modern cryptography assumes that the cipher, which can be broken by such available means, is not theoretically stable. The masses here are the main reasons, the most important of which is the current trend of increasing the power of computer systems.

A tragedy could be worldwide if it were not purely practical considerations: is information worth more than decrypting it; when the information is still decrypted, will it cost anything at all; just to take possession of the encrypted information, etc. However, the thoroughness and well-known maximism of the Russian cryptocurrency market contributed to the unambiguous conclusion: DES with a key length of 56 bits is virtually stable.

The same conclusion, but back in 1988, was made by experts of the French company NET1 Products Serge Bellamant and Andre Mansvelt when designing patented technology of cashless payments on the basis of smart cards under the name U.E.P.S. They also offered a way out – twice the consistent use of DES on a key pair.

This approach does not greatly increase the encryption time (which is important for a low-power smart card processor), but allows for very good theoretical stability – 2^{112}.

A simple calculation shows that if in our engineered super system each chip will perform 10 million DES operations in 1 second, then the whole process will take 25 thousand times for 10 billion years. In such cases, cryptographers who are satisfied with the result prefer to express themselves in space categories, for example, during periods of life of the solar system. It should be emphasized that sequential encryption on the same keys practically does not increase stability, since the number of key-search options does not change.

Double DES looks very attractive and maybe it would be enough. However, how to deal with systems still using one-time encryption, how to ensure the compatibility of key distribution schemes and hardware solutions? A rather original answer was found. Recently, the standard of encryption – the triple DES on a key pair – has been de facto established.

The idea of using a triple DES with a key pair is very simple: if the keys are the same, then the encryption result is equivalent to a single encryption. This ensures full compatibility with existing key distribution and use systems on both single and dual DES. (Double DES – single use sequential application).

According to the Center for Democratic Technology (CDT) February 13, 1995, a new triple-DES standard is being developed by the Accredited Standards Committee (ASC) Subcommittee X9, which implements data protection standardization in the US financial and banking field. In addition, AT&T and VLSI Technologies, major developers of custom hardware and hardware, have announced plans to build triple-DES applications.

It can be noted that the leading world manufacturer of smart cards GEMPLUS International has already announced the transition to a new standard for triple DES encryption for a new line of their products – the MPCOS series cards.

What practical conclusions can be drawn?

If the keys are stored securely and the key length (key pair) is 112 bits, then the DES encryption algorithm provides sufficient stability.

Triple DES encryption for a pair of stability keys does not exceed double encryption for the same pair and provides full compatibility with both single and dual DES. Triple DES has become the de facto standard for protecting information in the banking and financial fields.

What is DES with independent subkeys?

DES allocates from the 56-bit key entered by the user 16 48-bit keys for use in each of the 16 permutations. It is interesting to compare the effect when using a 768-bit key (divided into 16 48-bit connectors) instead of using 16 dependent keys created by the key mode in the DES algorithm.

When using independent keys, the number of attempts required to exhaustively search for keys will increase significantly. Changing the cipher will only cause a slight increase in the stability of the cipher against differential and linear cryptanalytic attacks than in conventional DES. It was open to bits (Bitham).

What is IDEA?

IDEA (International Data Encryption Algorithm) is the second version of the block cipher developed by K. Lai D. Massey in the late 80's. This is a cipher consisting of 64-bit sequences of blocks with a 128-bit key and eight rounds. Although this encryption code is not Feistel encryption, decryption is performed on the same principle as encryption.

The cipher structure was designed for easy implementation both software and hardware, and IDEA security is based on the use of three incompatible types of arithmetic operations over 16-bit words. The IDEA software speed is comparable to the DES gray.

One of the principles of IDEA creation is to complicate differential cryptanalysis. Also, not one linear cryptanalytic attack ended successfully, as no algebraic weaknesses were identified.

The most comprehensive analysis was conducted by Daemen. It opened a large class of 2 ^ 51 weak keys, which, when used in the encryption process, the key can be detected and updated. Since there are 2 ^ 128 possible key variants in IDEA, this opening does not affect the practical security of the cipher.

What is RC5?

RC5 is a fairly fast block cipher developed by Rivest for RSA Data Security. This parameter algorithm, that is, with variable block size, key length, and variable number of passes. The block size can be 32, 64 or 128 bits. The number of passes in the range from 0 to 2048 bits. Parametric of this kind gives flexibility and efficiency of encryption.

RC5 consists of key expansion, encryption and decryption.

When entering the key, the number of passes, block size, etc. are also entered. Encryption consists of 3 primitive operations: compilation, bit XOR and rotation. The exceptional simplicity of the RC5 makes it easy to

use, and the RC5 text, as well as the RSA, can be added to the end of the email in encrypted form.

RC5 security is based on data-dependent interleaving and mixing of the results of various operations. An RC5 with a block size of 64 bits and 12 or more passes provides good stability against differential and linear cryptanalysis.

What is RSA?

RSA (authored by Rivest, Shamir and Alderman) is a public-key system designed for both encryption and authentication; was developed in 1977. It is based on the difficulty of decomposing very large integers into prime factors. RSA is a very slow algorithm.

For comparison, at the software level DES is at least 100 times faster than RSA, on hardware 1,000-10,000 times, depending on the execution.

What is GOST 28147-89?

GOST 28147-89 is a standard adopted in 1989 in the Soviet Union and established an algorithm for encrypting data that constitutes state secrets. The history of this algorithm is a mystery. According to the witnesses involved in its implementation and use of people, the algorithm was developed in the 70-ies in the 8th General Directorate of the KGB of the USSR, at that time it had the stamp " Top Secret». Then the mark was reduced to "Secret", and when in the 89th year the algorithm was conducted through the State Standard and became the official state standard, the mark was removed from it. In the early 1990s, it became fully open.

GOST provides 3 modes of encryption (simple replacement, gamification, gamble with feedback) and one mode of imitation insertion. The first of the encryption modes is intended to encrypt key information and cannot be used to encrypt other data; two other encryption modes are provided.

The mode of production of the simulation insert (cryptographic control combination) is intended for imitation protection of encrypted data, ie for their protection against accidental or deliberate unauthorized changes.

The algorithm is built on the same principle as DES – a classic block cipher with a private key – but differs from DES'a longer key length, a large number of rounds and a simpler scheme for constructing the rounds

themselves. Below are its main parameters, for convenience – compared to the parameters DES'a:

1. Размер блока шифрования	64 бита	64 бита
2. Длина ключа	256 бит	56 бит
3. Число раундов	32	16
4. Узлы замен (S-блоки)	Не фиксированы	Фиксированы
5. Длина ключа для одного раунда	32 бита	48 бит
6. Схема выработки раундового ключа	Простая	Сложная
7. Начальная и конечная перестановки битов	Нет	Есть

Due to the much longer length of the GOST key, the DES'a is much more resistant to opening by "brute force" – by a complete search of the set of possible values of the key.

The GOST encryption function is much simpler than the DES'a encryption function, it does not contain bit permutations that are plentiful in DES and which are extremely ineffectively implemented on modern universal processors (though very simple in hardware). Because of that, with twice as many rounds (32 vs. 16), the software implementation of GOST on Intel 86 processors is more than 2 times higher than the DES'a implementation. Naturally, close to the optimum in speed of implementation were compared

Of the other differences GOST from DES'a note the following.

Each round of encryption uses a "round key", in DES'a it is 48-bit and is produced by a relatively complex algorithm that includes bit permutations and table replacements, in GOST it is taken as a fragment of the encryption key.

GOST encryption key length is 256 bits, round key length is 32 bits. Together we get that the GOST encryption key contains 256/32 = 8 round keys. In GOST 32 round, therefore, each round key is used 4 times, the order of use of round keys is set in the GOST and different for different modes.

The GOST Replacement Table – an analogue of DES'a blocks – is an 8x16 table (matrix) containing a number from 0 to 15. In each row, each of the 16 numbers must meet exactly once.

Unlike DES'a the table of changes in GOST is the same for all rounds and is not fixed in the standard, but is a changeable secret key element. The quality of this table depends on the quality of the cipher.

With a "strong" table, the substitution of the stability of the cipher does not fall below some permissible limit even in the case of its disclosure. Conversely, using a "weak" table can reduce the cipher's stability to an unacceptably low limit.

No information on the quality of the table of substitutions in the open press of Russia has been published, but the existence of "weak" tables is not in doubt – an example is the "trivial" table of replacement, each of which is replaced by itself. This makes it unnecessary for the competent authorities of Russia to limit the length of the key – you can simply put an insufficiently "strong" replacement table.

GOST, unlike DES'a, does not have the initial and final bit permutations of the encrypted block, which, according to some experts, do not significantly affect the stability of the cipher, although affect (downward) on the effectiveness of its implementation.

What is Encryption function?

Many algorithms, including DES and GOST, are built on the same principle: the encryption process consists of a set of rounds and steps are performed at each step. The input block is divided into halves (L) and younger (R).

The value of the encryption function from the younger part (R) and the round key (k) X = f (R, k) is calculated.

The function used at this stage is called the ROUND ENGINE FUNCTION. It can be one for all rounds or one for each round. In the latter case, the encryption functions of different rounds of the same cipher differ, as a rule, only in detail.

The output block is formed, its upper part is equal to the younger part of the input block L '= R, and the younger part is the result of performing a bitwise OR operation (denote it (+)) for the older part of the input block and the result of calculating the encryption function R' = L (+) f (R, k).

Symmetric cryptosystems. All the variety of existing cryptographic methods can be reduced to the following transformation classes (see diagram).

Mono- and poly-alphabet substitutions.

The simplest kind of transformation is to replace the source characters with others (of the same alphabet) by a more or less complicated rule.

The simplest kind of transformation is to replace the source characters with others (of the same alphabet) by a more or less complicated rule.

Permutations. Also a simple method of cryptographic transformation. It is usually used in combination with other methods.

Gamming. This method is to overlay the output of some pseudo-random key-generated sequence.

Block ciphers. Represents a sequence (with possible repetition and alternation) of the basic methods of conversion, applied to the block (part) of the ciphertext. Block ciphers are more common in practice than "pure" transformations of a particular class due to their higher cryptocurrency. Russian and American encryption standards are based on this particular class of ciphers.

3.3 RSA algorithm

If cryptographic systems were not sophisticated and reliable – their weak point in practical implementation – the problem of key distribution.

In order for confidential information to be exchanged between two IP entities, a key must be generated by one of them and then transmitted in confidence to the other. That is, in general, the transfer of the key again requires the use of some cryptosystem.

Public key systems were proposed to solve this problem based on the results obtained from classical and modern algebra.

The essence of them is that each IP addressee generates two keys that are linked by a specific rule.

One key is declared public and the other is private.

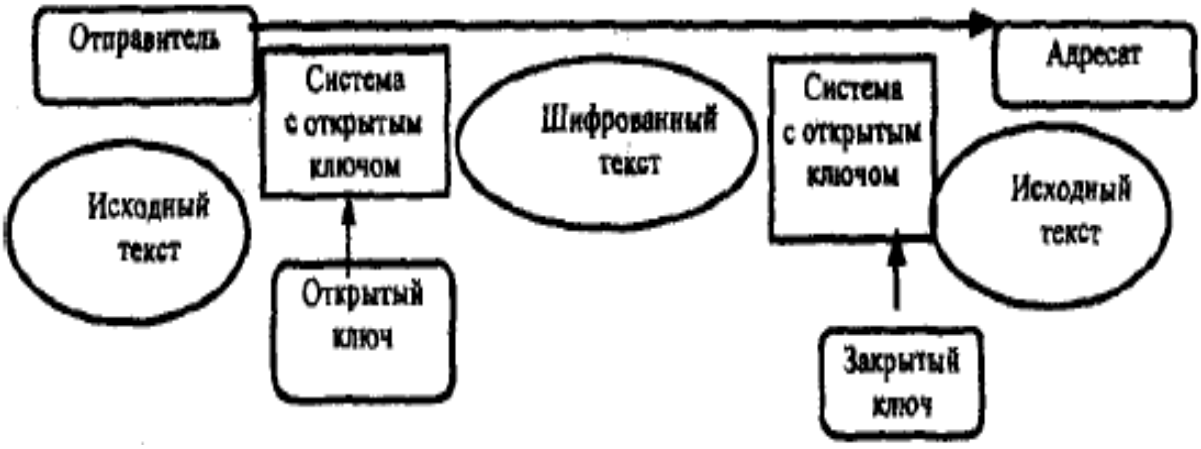
The public key is published and accessible to anyone who wishes to send a message to the addressee. The secret key is kept secret.

The source text is encrypted with the public key of the recipient and transmitted to him. Encrypted text cannot, in principle, be decrypted with the same public key.

The message can only be decrypted using a private key known only to the recipient.

Asymmetric cryptographic systems use so-called irreversible or one-sided functions that have the following property: given a value of x it is relatively simple to calculate the value of *f(x)*, but if *y= f(x)*, there is no easy way to calculate the value of *x*. Public key encryption algorithms are widespread in modern information systems.

Yes, the RSA algorithm has become the worldwide de facto standard for open systems.



Open-key cryptosystem algorithms can be used for three purposes:

1. Independent means of protection of transmitted and stored data.
2. Funds for key distribution.
3. User authentication tools.

Algorithms for public-key cryptosystems are more time consuming than traditional cryptosystems, so using them as standalone shields is irrational. Therefore, in practice, it is rational to distribute keys with a small amount of information as public information using cryptosystems. And then, using conventional algorithms, exchange large information flows.

Despite the large number of different open-key cryptosystems, RSA is the most popular cryptosystem, developed in 1977 and named after its creators: Rivest, Shamir, and Eidelman.

They took advantage of the fact that finding large prime numbers in the computational relation is easy, but decomposing the product of the product of two such numbers is almost impossible.

It has been proved (Rabin's theorem) that the disclosure of the RSA cipher is equivalent to such a decomposition. Therefore, for any length of the key, you can give a lower estimate of the number of operations to open the cipher, and given the performance of modern computers to estimate and the time required.

4. Internet: The evolution of the protection philosophy

The problem of information security on the Internet is posed and, with varying degrees of efficiency, is solved since the advent of networks based on TCP/IP family protocols.

In the evolution of security technologies, there are three main areas.

The first is the development of standards that implement certain network remedies, primarily administrative ones. An example is the IP security option and TCP / IP protocol variants used by the US Department of Defense.

The second direction is the culture of firewalls, long used to regulate access to subnets.

Third, the youngest and most actively developing direction is the so-called virtual secure network technologies (VPN, virtual private network, or Intranet).

The explosive rise in popularity of the Internet and related commercial projects in recent years has been the impetus for the development of a new generation of information security technologies on TCP/IP networks. Moreover, if earlier, up until the early 90's, the main task of protecting the Internet was to conserve resources mainly from hacker attacks, then nowadays the task of protecting commercial information becomes urgent.

Qualitatively, these are completely different types of protection. Attacking commercial information can entail high costs for hacking security and, therefore, significantly higher levels of traffic surveillance, information capture, cryptanalysis, and various types of imitations, diversions, and fraud.

Naive security methods, such as requesting a password and then forwarding it publicly over a communication channel and access lists on servers and routers, become ineffective under these conditions.

What can be contrasted with a skilled and technically armed attacking party? Of course, only a complete, cryptographically secure system.

There are a lot of offers of such means on the Internet market. However, for a number of parameters, none of them can be recognized as an adequate task of protecting information for the Internet.

For example, crypto-resistance and the great idea of forming a "web of trust" is the widespread PGP (Pritty good privacy) system. However, since PGP provides file encryption, it can only be used where file sharing is possible. It is difficult to protect online applications using PGP, for example.

In addition, the PGP security level is too high. Joining PGP protection with other applications requires some efforts, if of course it will prove feasible.

The choice of information security technology for a large open system – the Internet scale, large corporate network, communication network provider – must meet a number of specific requirements:

- the presence of an open specification, the absence of monopoly over technological solutions;
- wide scalability of solutions on technical and price parameters, versatility of technology, portability, multi-platform, compatibility of hardware, software, communication solutions;
- providing, where appropriate, comprehensive information security, ease of key management and secure communications for newly connected users.

Full use of the server requires its connection through a local router, which will become one of the security frontiers. The router can be programmed in such a way that it will block dangerous functions and allow the transmission of incoming requests from outside to dedicated servers only.

Partial protection is provided by port blocking, which is implemented in most modern routers by creating access control lists based on the language of the router commands. Another way to protect yourself is to configure your router so that it can only connect to the Internet with those computers on the network whose information is open to the public. The

rest of the network is isolated from these computers by firewalls or other means. This type of protection is used by many large corporations.

Standalone traffic filtering packages installed on PCs or workstations are attached to routers in their functions. A typical product of this class is FireWall-1 software from Check-Point Software Technologies, installed on Sun workstations and filtering inbound and outbound streams. Unlike routers, Fire Wall-1 is able to dynamically open data paths according to Internet protocols, such as FTP.

In addition, this package is equipped with a user-friendly graphical interface, security alarms and network access loggers that generate reports of unusual activity. Such products generally provide better protection than routers, but are of high cost.

The firewall router and products of the FireWall-1 software just reviewed do not have some features that increase the security against intrusion. For example, when transmitting a data stream, they do not analyze its content and are unable to validate access to network resources.

Such capabilities are firewalls – dedicated computers with active functions of filtering information flows at the point of communication of the local network with the outside world. The main task of systems in this category is to isolate the network from outside encroachments by viewing data packets, blocking suspicious traffic, and using special means of acknowledging access privileges.

Thus, the firewall acts as a watchdog, which does not miss any input or output that does not meet explicit criteria. Today there is a wide variety of firewall-based data security tools on the market.

REFERENCES

1. Библиотека Сетевой Безопасности URL: http://securitv.tsu.ru.

2. An Introduction to Computer Security: The NIST Handbook. Draft. – National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 1994. 310 c.

Information about the author:
Domnich V. I.
Candidate of Technical Sciences, Professor,
Head at the Department of Automated Process Control
of the V. I. Vernadsky Taurida National University