UDC 004.056.53

A.V. KHODAKOVA, A.S. GUBKA

National aerospace university named after N.E. Zukovsky “KhAI”, Ukraine

THE SYSTEM OF THE DATA PROTECTION FOR THE CRITICAL COMPUTER SYSTEMS IN ENERGETIC

The system of the data protection for the critical computer systems (Atomic Power Plant) which is transferred through network Internet, between the atomic power plants and National Committee of the Atom Energetic is developed. It is based on the new developed method, which combines symmetric and asymmetric algorithm enciphering of the data, such as electronic digital signature, based on RSA (Rivest Shamir Adleman) technology, and GOST 28147-89 algorithm. Due to this protection of the transmitted confidential information in critical computer systems in energetic is essentially improved.

data protection, critical computer system, atomic power plant, electronic digital signature

The introduction

The state of the Atom energetic is one of the most important characteristics of the national economy of the country. The increase of the number of the APPs (Atomic Power Plant) among the general electricity is typical to the modern stage of the development of the world power engineering. Because of the increase of the single capacities of the power units and because of the fact that the heat shames become more complicated and the cost of the equipment is height and the conclusive meaning has got the problem of the creating of the modern control system, the main aim of which is to provide the required regime of the exploitation of such a complete objects as APP. The advance increase of the “information loading” of the control systems is compare with the increase of their single capacities is one of the characters of the development of the energetic. Of the late 30 years the common volumes of the incoming and outcoming information in the control systems of the APPs have increased on average from 300 to 1500 units per APP [1].

The problem of the protecting of the information, especially on the strategically important for the people objects (to which we can refer and APP) exists always. The development of the system of the protecting of the information for the critical computer systems is shown in this work. All this is shown on the example of the APP. The urgency of this topic follows from the following aspect: it is daily necessary to send the reports from the APPs to the NCAE (National Committee of the Atom Energetic). This information is very specific. The access to it is maximally limited. That is why the heightened safety requirements are made to this information. These reports contain the information about some kind of the characteristics of the block that are hand over, they also contain the information about the regimes of the work of the units. About the experiments that are carried out on the station. If some not established situations take place – all this is written down into the report [2].

Over the list of the reasons nowadays the delivering of the information from the APP is organized using the open commutation channels. The documents are send in the paper way. That is why the required security level can not be reached. The adaptation of the new technologies and the achievement of the human ideas allow solving this problem in the following way. The reports that are send are protected with such a methods of the information protecting like the encoding algorithm GOST and electronic digital signature (EDS). The information that is stored in the report is at first encoded with the help of the encoding algorithm and then it is signatured with the EDS. All these allows not only to increase the speed of the delivering of this reports from the APP to NCAE but also to increase the reliability of their delivering.

1. The aim of the work

The aim of work is to increase the level of the protection of the information that is delivered from the APP. The increase of this level is made with the help of the encoding algorithm GOST and EDS. To reach our aim it is necessary to solve the following problems: the analysis of the present technology of the data protecting and delivering from the APP; the analysis of the EDS technology and of the encoding algorithm; the developing of the algorithmic structure of the subsystem of the data protecting with the help of the EDS and encoding algorithm. The developing of the software of the data protecting subsystem the purpose of which is to protect this information in process of the delivering it from the APP.

2. The analysis of the present technology of the data protecting and delivering in process of sending it from the APP

In the present time there are 4 APP in Ukraine. The usage of them caused some fear by the people because the protection of them is not very high. But the world begins to understand that the hydrocarbon energetic is near to its end. And its growth will stop. There is not enough storage of the fuel to satisfy the world's necessity in the energetic. In this situation there is no alternative to the developing of the atom power energetic. The new technologies allow to make APPs safe and allow to control all parameters and if it is necessary to undertake measures which help to prevent the possible extraordinary situations. Today the reports from the APPs are sending as a paper documents. It is made in two ways: with the help of the special post or with the help of the commutating channels. In the both cases it is needed too much time to send this information. And everybody understand that this information is very special and it must be delivered very quickly. Today the speed of its delivering and the protection of it do not satisfy the requirements.

To remote these shortcomings the method that is shown in this work is developed.

2.1. The analysis of the EDS technology and of the encoding algorithm technology. As it was said, the aim of this work is to develop the information protection method for the critical computer systems in the energetic. To make this the encoding algorithm GOST and EDS are used. It is necessary to tell some words about the work of these two algorithms.

2.2. The encoding algorithm GOST 28147-89. GOST includes the description of the algorithms of the several levels. On the top level the practical algorithms are situated. They serves to encode the arrays of the data and to working out of them the imitation insert. All they are based on the three algorithms of the lower level that are called “cycles”. These fundamental cycles will be called “basic cycles” in order to distinguish them from the rest of the cycles. They have the following names and symbols:

– the encoding cycle (32-3);

– the decoding cycle (32-P);

– the cycle of the imitation insert elaboration.

Each of the basic algorithms is the multiply repentance of the single procedure that is called “the main step of the cryptographic transformation”.

In GOST the main information consists from the two structures of the data. Besides the key itself that is necessary to all the keys it includes also a table of the replacements. The main characteristics of the keys structures of the GOST are shown below.

1. The key is an arrow from the 8 32-bites elements of the code K: $K = \{Ki\}$, $i = (0 .. 7)$.

2. The table of the replacements can be shown as a matrix which size is 8_16, it includes 4-bites elements that can be shown as integer from 0 to 15.

The lines of the replacement tables are called the units of the replacement, they must include the different values. This table is denoted with the symbol H.

The main step of the cryptographic transformation. It is an operator that denoted the transformation of the 64-bits data unit. The additional parameter of this operator is the 32-bite block. The scheme of the main step algorithm is shown below.

Step 0. Determines the begin data for the main step of the cryptographic transformation. N – the 64-bit data block which is transformed, during the elaboration of the step its younger ($N1$) and older ($N2$) parts are worked over as a separate integer number with out comma. That is why we can write $N=(N1, N2)$. X – 32-bites element of the key.

Step 1. The summering with the key. The younger part of the transformed block is added mod 2 with 32 element of the key which is used on this step. The result is transferred on the next step.

Step 2. Block replacement. 32-bites number, that we have got on the previous step is interpreted as an array from the 8 4-bits blocks of the code:

$$S = (S0, S1, S2, S3, S4, S5, S6, S7).$$

Step 3. The cycle shift for the 11 bit to the left. The result of the previous step is cyclically shifted for the 11 bit to the side of the younger classes and is delivered to the next step.

Step 4. The bitwise adding: the result from the step 3 is bitwise added mod 2 with the older part of the transformed block.

Step 5. The shift in a line: the younger part of the transformed block is shifted on the place of the older part and on the it's place the result of the work of the previous step is placed.

Step 6. The value of the transformed block that we have become returns as a result of the work of the algorithm of the main step of the transformation.

2.3. The algorithm of the electronic digital signature (EDS) in the RSA system. In the RSA system each subscribe X has a pair of the keys – open key (N_x,E_x) and private D_x, which knows only X and nobody else. In such a way every person can use the algorithm of the encoding E_x of the subscribe X but only he has the algorithm of the decoding $D_{x.}$

It is important to carry out such a correlations to the arbitrary message M:

$$D_x\,(E_x\,(M))= E_x(D_x\,(M))=M.$$

The aim of the subscribing is to guarantee the authenticity. Such a system is described with the scheme that includes the following elements.

- The probabilistic algorithm of the key generation. Each subscribe A become the pair $(K_{A,}K'_A)$, where K_A – open, a K'_A – private key.
- The algorithm of the signature $SIGN$ which makes the word $S= SIGN(M,\ K'_A)$ that is the subscribe of the subscribe A on the message M.
- The algorithm of the checking of the signature CHECK is given to every person who wants to check that the subscribe S of the message M belongs to the owner of the open key K_A. The checking can be named successful if $CHECK(K_A,\ M,\ S)=1$ for each message M and each pair of the keys (K, K') the following correlation is true:

$$CHECK(K,\ M,\ SIGN(M,\ K')) = 1\,.$$

It means that the system of the EDS is correct.

3. The development of the algorithmic structure of the system of the protecting information with the help of the EDS and encoding algorithm GOST

As a result the method of the data protecting for the critical computer systems in the energetic was developed (fig. 1). This method is a result of combination of the named above algorithm with the purpose of the increase the level of the protection of the object. The high stability of this method was got because not only the symmetric but also asymmetric algorithms of the encoding were used. In such a way it is not only impossible to intercept the information it is also impossible to use the information during the term of its actuality.

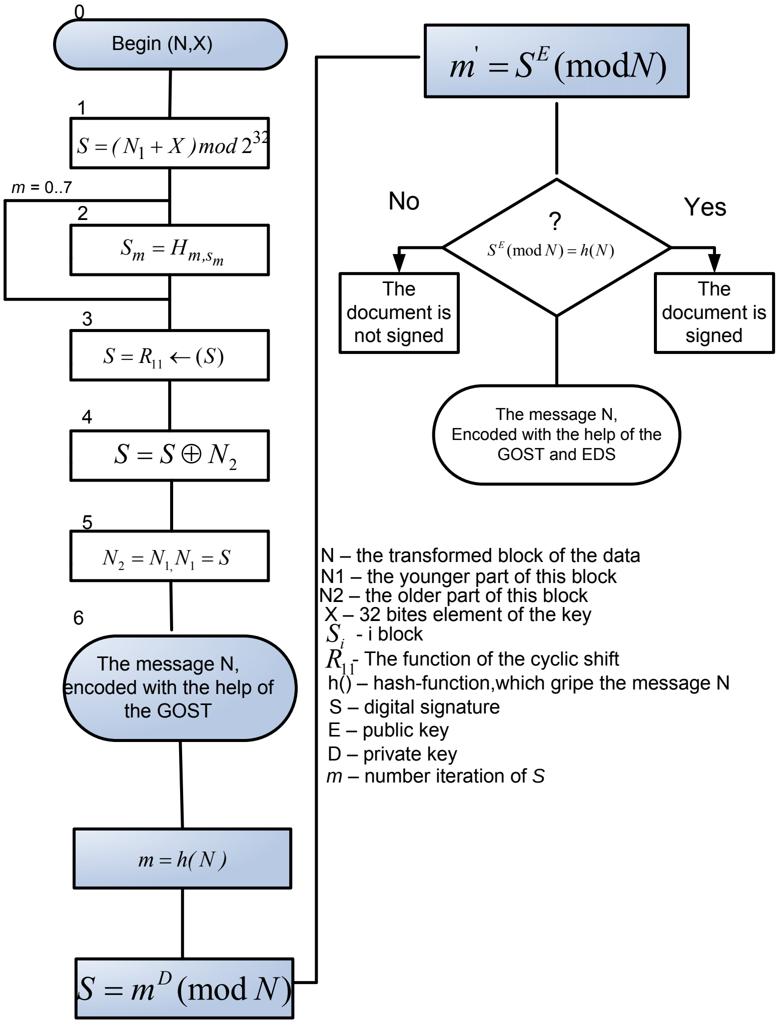
0
Begin (N,X)
1
$S=(N_1+X)mod\,2^{32}$
m = 0..7
2
$S_m=H_{m,s_m}$
3
$S=R_{11}\leftarrow(S)$
4
$S=S\oplus N_2$
5
$N_2=N_1,N_1=S$
6
The message N, encoded with the help of the GOST
$m=h(N)$
$S=m^D(\mathrm{mod}\,N)$
$m'=S^E(\mathrm{mod}N)$
No
Yes
?
$S^E(\mathrm{mod}\,N)=h(N)$
The document is not signed
The document is signed
The message N, Encoded with the help of the GOST and EDS
N – the transformed block of the data
N1 – the younger part of this block
N2 – the older part of this block
X – 32 bites element of the key
S_i - i block
R_{11}- The function of the cyclic shift
h() – hash-function,which gripe the message N
S – digital signature
E – public key
D – private key
m – number iteration of S

Fig. 1. The scheme of the developed method of the data protecting

It is well-known that the actuality of the delivered from the APP information is about some hours and the decoding of it in some days or month has no sense.

The algorithm of the developed method is shown on the fig. 1.

On the base of this method the soft ware was developed that helps to protect the delivered information with the EDS and GOST.

The algorithm of the work of the program is the following: the user loaded from the file or inserts with hands that information that he wants to protect that he generates the key, encodes the information and in the window he can see the result of the encoding. On the first form of the program the encoding with the help of the GOST take place.

Then the user opens the next form where he can make EDS on his message. He checks the control sum and sends the document.

Literature

1. Горелик А.Н. Автоматизированные системы управления технологическими процессами АЭС. – К.: Техника, 2005. – 425 с.

2. Топольницькій М.В. Атомні електростанції. – Львів: APS, 2005. – 524 с.

Поступила в редакцию 6.02.2008

Рецензент: д-р техн. наук, проф. А.Ю. Соколов, Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Харьков.