Secure Voice Data Transmission Based on the Formant Analysis Algorithms

Cunev Veaceslav,
Chisinau, Republic of Moldova

***Abstract* — This report examines the features, differences and advantages of the formant analysis for building on its base and using of enhanced RSA-m encryption algorithms for crypto security of the voice communication of short- and long-term secrecy in online conversations.**

Index Terms*—Component, formatting, style, styling, insert.** ***(key words) crypto security, permanence, RSA cryptosystem, fast encryption algorithms, RSA – m, online mode, protection, information, security, theory of numbers, comparative and formant analysis, cryptography.

I. INTRODUCTION

Nowadays cryptographic protection of the transferred and archival digital (bit) information is very demanded in modern computing and information systems, radio communication systems, data management complexes, in systems of mobile (cell) telephony and confidential telephone digital communication, on the state, commercial, security-signaling enterprises, financial structures, and in factory automation systems. This cryptographic protection became an active component of the listed systems. Cryptographic protection of the transferred and archival digital (bit) information is done with the goal of this information closure and security of its exchange and use, in the communication channels as well as at the places of transfer, reception, processing and temporary or permanent storage. There are already invented various special vocoders, autonomous or embedded intercom stations, telephone handsets or facial voice headsets, provided with wired or wireless connection with transmitting-receiving component of mobile, telephone or other radio equipment

The distinctive features of such devices are the methods and ways of encryption, which allow encoding bit information in real time without significant delays. However the bottleneck of such offers is the low durability of crypto protection, which is provided for online communication by these devices. To hide the information when it is transmitted through the open channel authors suggest, unlike the traditional scheme, to transfer not the original information, but some not obvious data about it, which are known only to receiving side (or internal software of encryption device). The information should be easy recovered on the basis of this data. This can be for example a one- or multidimensional formant [1] of a number or mathematical expression, whose parameters value varies from time to time by changing of the base p of formant according to some function, or from the value of the digital representation of the protected information. The formant itself is transmitted in an encrypted form, for example, using one of the $RSA - m$ algorithms or any other, for example hybrid algorithm [3].

The algorithms and device, suggested by the authors, differ from well-known ones, for example from Lucifer system of IBM Company and from the encryption data standard of the National Bureau of Standards, or RSA cryptosystem. They differ by the way of open data binary information compression (reduction) and the subsequent possibility of its bit-to-bit encryption with the use of well-known algorithms, such as RSA, but using not known to cyber-spies and rather short crypto keys and other necessary parameters of encryption. This enables the use of such encryption method in online mode. This makes this method convenient even for use in radio systems.

For this purpose there is used its adequate transformation through bit-by-bit encryption of each discrete of compressed digital signal on the base of the formant analysis algorithms with the following batch transmission in the form of the protected information block. On the receiving side there are realized the restoration of encrypted code batches (blocks), decomposition of the block into informational and auxiliary parts, information bits decryption on the base of formant analysis algorithms with the restoration of the continued analog voice signal using vocoder, that converts the decoded digital signal into analogue one.

II. ADVANTAGES, LIMITATIONS AND NEW OPPORTUNITIES OF RSA CRYPTOSYSTEM

As it is known, the RSA asymmetric crypto-encryption method is used for information protection by encrypting large messages, divided into 64-bit blocks. Two keys are used for encryption – public and private, one-side functions properties and arithmetic of large numbers [2], more than 10^{12} and more, i.e. $10^{60} \dots 10^{150}$, finding dividers of which in a reasonably short time meets considerable difficulties.

Comparatively low speed of RSA system, but its high crypto durability (resistability) gave authors the idea to look for new possibilities of the use of this system in information protection in the usual flow transmission, for example, voice, in online mode. The suggested method (way) of encryption is based not on the transmission of the information itself, but on the transmission of some special information, the broadcast volume of which will be significantly less than the original and, therefore, can be transmitted in encrypted form in real time (online) with the required degree of crypto durability on the base of ideology of RSA algorithms.

The essence of the considered method is in the use of the properties of so-called numerical formants, introduced and described by the authors in [1], with the help of which any number can be represented in the only way by means of the finite number of small decimal (and therefore binary as well) numbers, which are significantly smaller in absolute value than the original large number. Whereas the time of encoding of the formant of a large number, encryption and decryption of its parameter of the declared *RSA-m* algorithms, are substantially less than encryption and decryption time of the original large number, which is a 64-bit block in the classical RSA cryptosystem. Each sending of the block s_i $(i = 1 \ldots 409600)$ of the open message is processed by a pair of randomly selected crypto-keys. As it is known [1], linear formant uses only 3 parameters, from which only 2 are encrypted, and in some modifications of the RSA-m algorithm – only one! The advantage of the formant number representation is in the fact, that the base of the formant can be any number, both simple or composite, which significantly increases the size of the number set, as for selection of the formant base in encryption (which increases crypto durability of the algorithm), and for its hacking in cryptanalysis (which complicates the task of the attacker).

The known standard of data encryption encrypts information by 64 bit blocks, which requires preliminary accumulation of 64 bits of information, and while decrypting it requires additional synchronization for extracting of the beginning of each block of encrypted information. Besides, the process of the next block encryption consists of 16 cycles, which creates a certain delay in encryption of the information blocks. The listed features of the well-known data encryption standard make it inconvenient for online mode use and in radio communication systems.

III. Advanced Algorithms of RSA-m cryptosystem

For the realization of the formant approach for public message encryption there are preliminary formulated K matrices with the size of $n \times n$, where will be stored randomly computed (but according to the Fermat's algorithms on the base of simple numbers p' and q') modules $N = p'q'$ crypto conversion $RSA - m$ and preliminary matched pairs of crypto-keys with different length $\mu(s_i)$ bits, and also - bases p, cores k and remainders q of the "image" formants, corresponding to the public message code.

In one of the variants of the RSA algorithm $- m$ in the process of conversation broadcasting through the communication channel (radio, mobile phone, internet etc.) each discrete with amplitude $m(t_i)$ of bits at the output of the ADC of vocoder is considered, as an address of crypto-keys location, placed in read-only memory (ROM) with a capacity of 2^{32}, whereas crypto-keys are distributed to the addresses randomly.

Encryption is carried out in two stages: 1) finding of the formant parameters– core k and remainder q – by dividing of the discrete amplitude on the formant base p; 2) encryption of the formant numbers-parameters k and q on module N with its individual crypto-key e.

After each communication session the key addressing in ROM changes. Thus, encryption method is almost equivalent to encryption with one-time key with a random length, equal to the length of discrete bits of the message, which corresponds to the Shannon theorem conditions about decryption impossibility. The use of hardware and not software implementation of the microprogram automaton would ensure an increased encryption speed.

A. RSA-m Algorithm of Bit Information Encryption

Authors have developed several variants of formant algorithm use for encryption with secrecy of different short- and long termness with significant reducing the encryption and decryption operation time in comparison with the classic RSA algorithm.

Thus, as one of the directions of use of classical RSA cryptosystem advantages, authors suggest bit-by-bit encryption of the information with the use of short crypto-keys, which length is sufficient for providing of short-term level of conversation security (1-3 min.). And for increasing of the time of urgency (up to tens of months) it is foreseen the change of their lengths to the values, which provide higher crypto durability.

The process of the binary information encryption consists of several stages, fig.1:

1) On the first stage there are determined the formant parameters - core k_i and remainder q_i – of each discrete D_i public message S_O in the form of $F_p(D_i) = k_i p + q_i$, which are further
2) Encrypted by the unknown to users key e, located in ROM at the address, which is defined for example according to AB1 algorithm, amplitude of the current discrete, by performing a set of operations, which include on the transmission side division by module p (formants base) 32-bit number S_O, after that – functional decomposition of the received 32-bit sequence on the core k_i and remainder q_i,
3) Then it is converted turn by turn by the data encryption block into coded encrypted message (block), which is directed into the communication channel and on the input of the 32-bit forming register (8) as an adder on module 2 of the output of the block (6) and 32-bit random number, read from the ROM (4),
4) And on the receiving side, on the 1-st input of 32-bit forming register (10) there is directed encoded and encrypted binary packet from cryption-

block (unit) (9) of the communication channel, and on the 2-nd input of the adder – 32-bit random number, read from ROM (4);

5) The output of the register (10) is fed to the decomposition in the block (11), where auxiliary and information parts are allocated, which after that

6) Encrypt and restore the formant in block (12) as a fragment of the speech block on the output of the daisy-chained DAC (13) and vocoder (1).

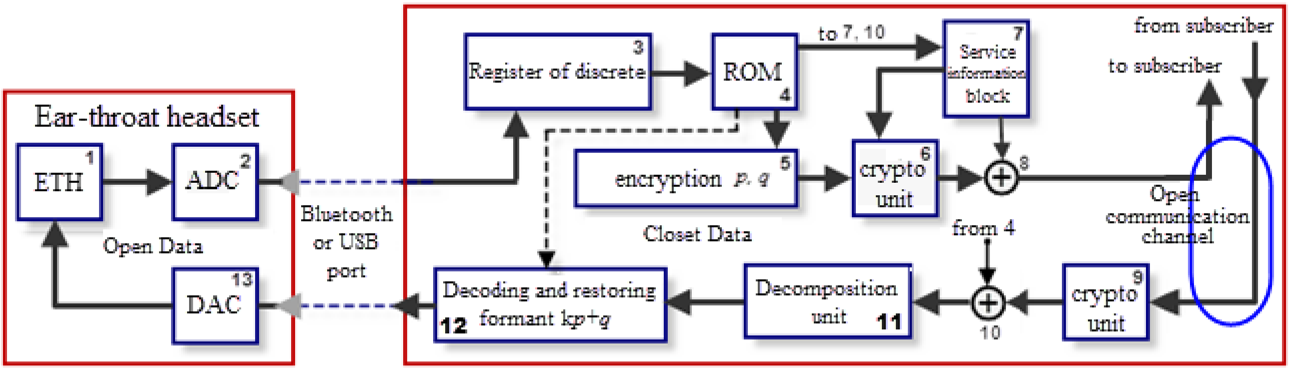


Fig. 1 Block diagram of the encryption and decryption device

Fig. 1 represents block diagram for implementation of the described procedure of the binary information encryption on one of the conversation place. Encryption and decryption devices contain: ear-throat headset (1) with built-in ADC (2) and DAC (13), connected to the encryption/decryption device through the USB port or Bluetooth wireless port, 12-bit register of discrete (3) for receiving, processing of each discrete of voice signal (they arrive at a rate of 4096 discrete/sec) and transmitting of its value into ROM (4) for calculation with the help of built-in software of the corresponding formant $F_p(D_i)$ on the current base p_i, value of which is located at the address, defined by the software of the ROM (4) by the value of the current discrete. After that encryption block (5) of the parameters k_i and remainder q_i of the current discrete with the help of ROM program resend encrypted data about formant parameters into cryption–block (6), that forms 64-bit packet of the encrypted message with the addition of auxiliary, additional information and symbols from the block (7) in order to organize the process of the transmission into the communication channel.

B. RSA-m algorithm of discrete encryption/decryption

The process of encryption of each 12-bit discrete of the open information is carried out in the following way: $m -$ digit bit number of the register of 3 discrete is sent to the calculation subroutine (4) of the formant of current discrete D_i by the formula$F_p(D_i) = k_i p + q_i$. Current value of the formant base p is retrieved by the program from the cell of the active data matrix for the current formant. The address of the needed cell of one of 32 matrices of encryption/decryption parameters storage, located in ROM, is found by the program according to the value of the current discreteD_i. Calculated by the program parameters of the current discrete - core k_i and remainder q_i, are encrypted according to formulas

$$k_i^{\text{ш}} = k_i{}^e modN; \quad q_i^{\text{ш}} = q_i{}^e modN \qquad (1)$$

Where $e, N -$ are respectively the 1st key (in asymmetric cryptosystems it is called "public") and encryption module, taken from the cell $D_i^{S_i}$, whose values change for each discrete or transmission session (depending on the chosen regime or encryption method). The result of encryption is sent to Cipher-block (6), to where from the Master Information Block (MIB) (7) auxiliary, additional and special symbols are added. These symbols form 64-bit cipher-packet, which is sent to the open communication channel, after its mixing in block (8) with the random 64, 32 or 12-bit number depending on the bit size of the chosen ADC and on the length of the cipher-block package.

Transmission of the information to the communication channel is carried out sequentially by "portions" of 64 bits (digits), and each portion of the message is additionally converted by adding the bits, which define the beginning and the end of the package, address bits for initiation of the program of search of necessary matrices and addresses of cells, which store values of the parameters $p_i, k_i, q_i, P, N, e, d, A_{na}$ for encryption/decryption of 64-bit packets, their decomposition and restoration of the discrete value by its restored formant, and address of the cell A_{na} of a matrix of random numbers for the operation of blocks 8 and 10. Besides, from the cell of matrix A_{na} on module 2 a random sequence "1" and "0" is added as 64-bit functional conversion of the output package information for its protection from distorting action and possible statistical analysis in case of intentional attacks. The address of a random number is also identified by the contents of the cell D_i, thus the number of digits of registers 8 and 10 is (12, 16, 32 or) 64-bits, and number of digits of random numbers from block 4 and 7 of ROM - 32 bits, which are summed on module 2 with outputs 6 or 9, beginning with any undefined position of the bit sequence from outputs 6 or 9 so that after masking the packet sent to open channel was sufficiently discharged with zeros.

The decryption of discrete of encrypted information is carried out in the following way. 64-bit content of Chiper-block 9 is summed on module 2 with the number, extracted from the cell A_{na} . The sum received (the original cipher-packet) is converted by block 11 into encrypted values of formant parameters of the next discrete. These values possess in block 12 their original values

$$D_i = F_{p_i}(D_i) = k_i p_i + q_i, \qquad (2)$$

$$k_i = (k_i^{ш})^d modN = k_i,\ i.e.\ (ed)modN = 1;\quad q_i = (q_i^{ш})^{ed} modN, \qquad (3)$$

where $\{d, N\}$ – 2-nd crypto-key (usually is called “private”).Decrypted in the block 12 values of the formant parameters , according to (2) restore the value of the current discrete, which is sent to vocoder from the output of DAC (13)

IV. Operation description of the encryption and transmit data protection device

In case when there are written the absolute values of amplitudes, the digitized signal in the form of a set of sequential discrete is called *writing format* of type PCM (Pulse Code Modulation).Standard audio compact disk (CD-DA), used from the beginning of 80-s of the 20th century, stores information in PCM format with sampling frequency 44.1 kHz and 16-bit quantization rate. According to Nyquist–Shannon sampling theorem, in order to unambiguously restore the original signal, sampling frequency should be twice higher that the maximum frequency in the signal spectrum.

Since the upper limit of hearing is 20 kHz, the sampling frequency should ideally be not less than 40 kHz. That is why standard sampling frequency, used in the CDs recording, is 44,1 kHz (so called CD-quality). However, the sampling frequency can be even higher, but such quality of sound is used only in sound-recording studios and by extra demanding music lovers.

The sampling frequency of 44,1 kHz — is not always an achievable ideal. When data is transmitted over a network with low data through-put, the quality of sound has to be sacrificed in favor of its recording format size. In practice there are usually used sampling frequencies in two, four and eight times smaller, than 44,1 kHz:

- 22,05 kHz — is so-called radio-quality. It is used for sound encoding at FM radio stations. In case of Flash it suits well for creation of wallpaper music and event-related sounds. It is even a little redundant for the human voice transmission;
- **11,025 kHz — telephone quality. The sampling frequency, which is optimally suitable to the transmission of the human voice. It is used in в IP −telephony;**
- 5,5 kHz — the sound is close to the loss of information component. This sampling rate can be used for the transmission of low sounds and voice (but with very low, mediocre quality).

So, the sampling frequency is chosen equal to $2f_{max}$ in the frequency spectrum of the voice channel. Considering that the border frequency of the sound channel of cell communication is 40 kHz, we shall accept for a model variant the sampling frequency 12 $kHz \rightarrow T_{selection} = 12\ 000\ \text{discrete/sec}$.

During the speech or sound transmission there is encrypted each discrete of the digitized amplitude of the analogue signal, for example with a rate till 4000 or 12 000 discrete/ sec (at the sampling of the analogue signal with frequency 4 kHz or 12 kHz).

When ADC number of digits is 12 bit or $2^{12} = 4096$ of numbers and frequency (rate) of discretization is $4 \ldots 50Hz$, the period of selection is within the range from $250\ \text{microseconds till}\ 20\ \text{microseconds}$, which sets heightened requirements for the processing of numerical information when working in real time.

Thus, at a sampling rate of 12 kHz the values of discrete of the speech sound in IP −telephony and 12-bit ADC represent a random set of natural numbers in the range of numbers from 1 till $4096 = 2^{12}$, and at 16-bit – is from 1 till $2^{16} = 65\ 535$. Thus, for example, for the 3 minute conversation could not be interrupted by the forced “pauses of silence”, spent on the processing of billions of bits, the processing speed and data through-put of the communication channel of microcontroller or computer equipment should be very high.

Indeed, the information is transmitted through the accumulation buffer, where packets (blocks) of 32(64) bites or 4(8) bytes are formed. These blocks will always contain also the information about restoration of the real information and about the method of its reproduction in real time (or it can be recorded as encrypted or restored information in memory). The format of the data block contains also the service bits about the composition and structure of the transmitted information package.

A. Variant of encryption

1 variant – *encrypted cell address is transmitted* through the open channel. The first variant (the simplest and the most unprotected!) – the address of the cell, where the value of the next discrete is located in the form of formant parameters (*p, k, q*), encrypted with the help of RSA algorithm, is transmitted through the closed channel. It is clear that due to the limited number of possible discrete (they are only 4096) all they can be systematically displaced in memory. The first method – the value of discrete – is its address in ROM of the receiving or transmitting devices.

The further main task is to encrypt this address, for example, by some mask or with the help of RSA-m.

1.1. Encryption by simple mixing. The initial state – the value of the cell content is the storage address of this content in matrix. For example, the number 3253. It should be stored in the cell №3253. Mix the addresses of discrete matrix randomly. For example, №3253 became №1900. The last address is encoded in the system of formants (*p, k, q*) using

$RSA - m$ and is transmitted to the open channel. Although the discrete is the same, its value is still 3253, but it will be stored in the cell №1900, which depends on the formant of numbers 1900 (or 3253, depending on what is mixed

1.1.1. addresses

1.1.2. or the content of the addresses.

2 variant. ***Each formant of discrete*** (i.e. base and remainder) *is encrypted* using $RSA - m$, which is transmitted online in the open channel.

2.1. Encryption of 4096 possible values of the sound discrete

For each discrete we will select, for example, 100 different key pairs (matrix10×10). For each discrete we create its cipher-text or cipher-discrete. That is why for 4096 real discrete we will 4096x100=409600 memory cells to store cipher records of discrete..

2.2. Storage of encrypted discrete (matrix M1)

Let's there be a matrix **M1** $300 \times 300 = 900\,000$ cells, which is twice more, than is necessary for allocating of $409600 \approx 410\,000$ numbers with the length up to 32 binary bits ≈ 9 decimal bits + 2 more. They shall be arranged in that way, so the search time of a random number in this range was minimal.

2.3. The content of the M1 cells is the formants of discrete. Speaking more precisely, these are their parameters: core k, remainder q and base p in "pure form" or encrypted by any cipher.

2.4. The length of the RSA-m keys.

The length of the keys is chosen from the calculation of the minimum time spent on the crypto-processing. That is why the lengths of the public and private keys are almost equal, but not larger than 14-15 binary digits from16383 ... to 32767, i.e. the numbers ≤ 32 767 of the decimal number, and to the

$$N < 10^9 = 1\,000\,000\,000_{decimal} = 111011100110101100101000000000_{binary}.$$

The public key is often chosen by order or even 2 orders less than the private key: $e \approx 12 - 14$ bits, $d \approx 15 - 17$ bits while using the transmitted data package of 32 bits and about 2 times more- for the packages of 64 bits. In short-term secrecy systems keys can me chosen in a range up to one byte.

B. Preliminary work with memory

1. To create the set of matrices: $MAD -$ matrix of discrete addressess , $MP -$ matrix of the formant basses , $MADE, QE -$ matrix of crypto-keys. To fill them, i.e. to write in ROM memory in the form of integers all values of discrete from possible 4096, i.e.: series $\overline{1,4096}$ for MAD, series $\overline{1,409600}$ – for encrypted discrete values of matrix $MADE$, series of base value for matrix MP
2. To calculate the formants of all discrete on 100 simple bases and to write the matrix 1 2 3…… 5000/1 2 3….100. Totally about 500 000 o formants on 100 different formants.
3. The sequence of discrete arrangement in cells of matrix 5000x100 shall be encoded by mixing (10x10 of variants: 10 on lines and 10 on columns. Totally, 100 mixing of the variants of discrete arrangement in matrix). There will be 100 matrices of M1 type.
4. Encryption of all discrete by three formants p, q, m and their writing in memory in the form of indexes of matrices M1. Thus, one and the same discrete in ROM will have 100 different index-addresses.
5. The same ROM arrangement is formed on the receiving side as well.

C. Work on the transmitting side

1. Speech sampling using ADC.

2. Work with the next formant – writing to the buffer (discrete register)

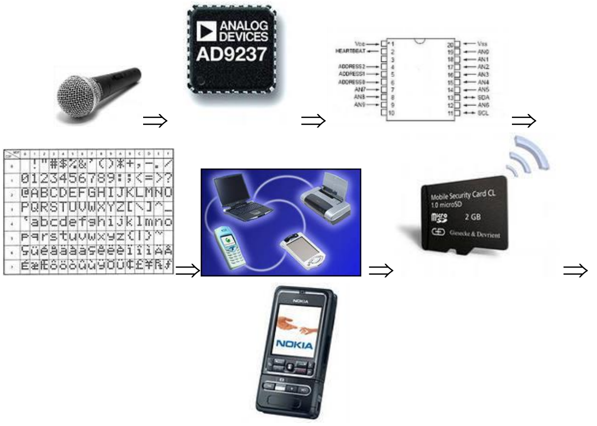
a) The conversion of the discrete value into an integer;

б) Formant evaluation (or searching for such number in ROM and writing of its address in RAM memory – at this address in ROM there are located all the data about the current integer)

3. Generation of the signal-text of a package: 1) 4 encrypted addresses are transmitted: 3 addresses for p, q, m and the 4th address to control the transmitted information in the control cell ; 2) there is transmitted only 1 address (random) ,where all the information about the formant of the current discrete is stored (for the information of mini time-bound secrecy) and the 2nd address to control the transmitted information in the control cell;

D. Work on the receiving side

1. Reception of the signal and its analysis. Reading of the addresses p, q, m and comparison of their values with the data in the control cell.
2. Signal assembly by the discrete addresses.
3. Signal Playback.



Microphone ⇒ ADC ⇒ Calculation of formant of the next discrete (in the form of an integer) ⇒ identifying the address of the next formant cell ⇒ Writing to the memory (Buffer) ⇒ Formation of the signal-text package: ⇒ Over-the-air transmission of the encrypted cell address . The example of the practical use of the declared method of information closing.

V. Systems of the Mobile (Cellular) Communication Using Cryptoprotecton Methods on the Base of RSA-m System

There exist a strong opinion, that it is very irrational to use public keys in the systems of flow encryption (speech digital closed channel are an example of flow encryption). Since other equal conditions in asymmetric systems require a large length of the key comparing with the symmetric encryption systems. That is why asymmetric encryption is mainly used as an auxiliary procedure and **only in service channels,** where there is a need to change (replace) symmetrical keys, used in the closing of the speech information directly.

The expounded in the report approach to the use of RSA ideology in such (broadband) communication channels **as the main cryptosystem of information closing** is based on the use of **a small length of encryption key,** compensable with its quite frequent and fast change.

Since voice communication though the protected line must be provided in real time, the information protection is based on the **flow encryption (in distinction from RSA, when information blocks are formed and encrypted).** Thus the analogue signal is discretized on time with the period of discretization Td/2 (Td – the period of oscillations of the highest harmonic of the analogue signal, determining the period of the repetition period of the impulse sequence of the formed discrete), after what each discrete is encrypted individually and separately.

The advantage of the suggested by the authors method of voice communication channel cryptoprotection is not in the use of large keys, which while "hacking" require a lot of time on the factorization of a very large number. The advantage is in the frequent change of the relatively short keys, each of which is designated to separate discrete encryption. The opening of such keys will require additional machine time spents on the decryption of each discrete separately. Let's note that "hacking" of the speech discrete significantly differs from the hacking of the textual information. In the latter case text decryption allows omitting not only separate letters, symbols, but even words, nevertheless hidden text can be restored, considering it as some meaningful information. There is another situation with the sound!

The procedure of information comprehension "by ear" is very similar to the popular telegame "Guess the Melody", when participants try ti restore some melody by singing a "piece" of it, in the form of musical phrase, or even by its first 2-3 sounds. The sound is a set of discrete of digital exposition or "description" of the speech or sound information. If the sound has constant intensity and frequency – this is monotonous sounding. And human voice has a huge number of overtones and tones (discrete, belonging to different frequency components) etc. This is the circumstance, which creates difficulties in disclosing of such private information "by one discrete". The difficulties are caused by the base of high cryptoresistability of such encryption method.

As an example, let's estimate the work of the model system with concrete numbers. Let's assume, that discrete "stand" from each other on the time axis at the distance of Td =167 μs. In this case, if we use quickly changing keys, the length of each is 38 decimal digits; system will ensure the safety of a 24-hour negotiation session for a period of three years.

A. *Description of the operation of the fully open and closed RSA-mAB cryptosystems:*

In classic RSA public key is sent to the receiving side and can be accessed by crypto-analytics. Public key of the sender will be used by the recipient for encryption of the response message by the RSA algorithm. After encrypting of the message by the sender, it won't be possible to open it with the public key (principle of encryption using public key, for example RSA system). The owner of the private key can easily decrypt the received message.

Before the communication both sides of negotiations will start the generator of public keys, which will be stored in their data bases and will be used throughout the whole communication session. The quantity and parameters of the generated keys for the proper protection are determined (calculated) below:

When the connection is established, "initiator" (A) sends to the receiving side (B) the first encrypted message, which contains randomly chosen public key $\{e, N\}$ from its data base (preliminary having generated the private key $\{d, N\}$). The public key received will be used by the side (B) doe encryption of its message, that contain, in its turn, a pair of its public crypto-keys for side (A). **Thus, the main idea of the organization of secure information transmission between negotiation sides is in the constant change of the public keys (short enough in length for the flow data transmission). This is the alternative for the use of long keys, because it requires from the crypto-analytics permanent machine time spent on the definition and factorization of the base number N for new keys compromise.**

In another alternative variant **(fully closed RSA-mF system)** keys won't be transmitted in encrypted form. There will be transmitted only code information about keys, for example, about the addresses of their locations on some servers, or in ROM receiver, or in the form of some digital-code information, that allows to form the necessary keys on the receiving side. This variant was considered by the authors in the present report.

References

[1] Balabanov. A.A., Agafonov A.F. Сопоставительный анализ и его приложения. Классические и современные задачи теории чисел и криптографии. (Comparative analysis and its applications. Classical and modern problems of the theory of numbers and cryptography.) - pub.Lambert, Germany, 2016, 197 p., INN 978-3-659-92621-1

[2] Balabanov.A.A., Cunev V.V. Защищённые IT-системы на основе алгоритмов формантного анализа (Protected IT-systems based on the formant analyses algorithms) /- pub.Lambert, Germany, 2016, 215 p., ISBN 978-3-659-94826-8

[3] Balabanov.A.A., Cunev V.V. Способ шифрования двоичной информации и устройство для его осуществления (Method of binary information encryption and application for its implementation) / - patent of RM, http://www.findpatent.ru/patent/209/2099885.html