The Use of Cryptographic Techniques RSA-m to Protect the Information in Real Time

Balabanov Anatolii, Agafonov A., Izvoreanu Bartolomeu, Fiodorov Ion, Cojuhari Irina,
Moraru Dumitru

Technical University of Moldova, Department of Automation and Informational Technologies
Stefan Mare Av., 168, Chisinau, MD2012, Republic of Moldova
Tel:(37322) 292836; E-mail: bbalsoft@gmail.com

ABSTRACT

In this paper the authors propose an advanced algorithm of RSA (modernized "kriptolock"). This algorithm is proposed to use for encoding the information with a short term of secrecy, when the attack are encrypted blocks of discrete analog signal, whereby the decoding of the information flow in real summer time is almost impossible.

Keywords: cryptographic, systems, asymmetric, algorithm, RSA, information, secrecy, signal

1. ASYMMETRIC CRYPTOSYSTEM

The effective systems of cryptographic data protection are asymmetric cryptosystems that called cryptosystems with public-key. In such systems for encryption the data is using only one key, and for decryption another key (thus the name of asymmetric). The first key is public and can be published for using by the all users of system that encrypt data. Decryption data with a public key can not be done.

The recipient decrypts encrypted data using the second key that is secret. Of course, the decryption key can not be determined from the encryption key. Generalized scheme of asymmetric cryptosystems with public key is presented in the Figure 1.

In this cryptosystem is used two different keys: K_B - public key of subscriber B; k_B -secret key of subscriber B. The subscriber key generator is always placed on the subscriber side. The values of keys K_B and k_B depends on the initial state of the generator keys.

Disclosure of the secret key k_B from the known public key K_B should be difficult problem.

The characteristic features of asymmetric cryptosystems are:
The public key K_B and cryptogram C can be send by the unsecured channels, if it is known to the enemy the K_B and C. The algorithms of encoding and decoding

$$\mathrm{E_B} : \mathrm{M} \to C,$$
$$D_\mathrm{B} : C \to \mathrm{M}$$

are the public.

The security of information in asymmetric cryptosystem is based on the secret of key k_B.

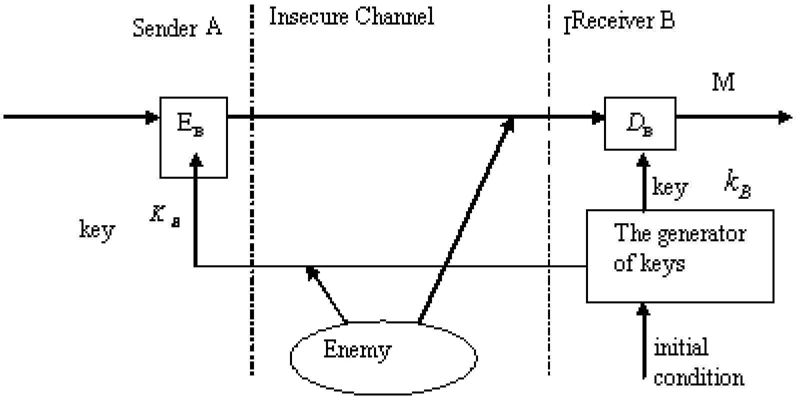

Figure 1. The general scheme of asymmetric cryptosystem.

Asymmetric cryptosystem with public key are based on the applying the one-direction functions. One-directions function can be defined as follows. Let X and Y some arbitrary sets, function

$$f: X \rightarrow Y$$

is one direction function, in case if for every $x \in X$ can be easy calculated the value of function

$$y = f(x),$$

where $y \in Y$.

But for the most $y \in Y$ it is so hard (need more time) to receive that value of $x \in X$, that we have $f(x) = y$.

The basic criterion for inclusion f function to the class of one direction function is not existents of effective algorithms of inverse transformation $f^{-1}: Y \rightarrow X$.

2. THE PRESENT OF RSA SYSTEM

Nowadays, the RSA system is the most used asymmetric cryptosystem with an open (public) key, providing such protection mechanisms as encryption and digital signature [2, 4, 7,10]. The RSA algorithm was proposed by the three researchers-mathematicians Ronald Rivest, Adi Shamir and Leonard Adlmanom in the years 1977-78, is one of the most reliable and often called the de facto standard in the practice of modern cryptography [4,10] . Regardless of the official standard the existence of such standard is extremely important for the development of the electronic commerce and in general economy.

Unified workflow system with the public key implies to use the digital signatures between users from different countries, that use different software on different platforms; The system RSA has so big quality that it takes into account and when is creating new standards. In the developing of the standards for the digital signatures in 1997, was developed the standard ANSI X9.30, supports Digital Signature Standard (DSS). A year later, was introduced ANSI X9.31, which focused on the digital signatures RSA [4,10].

2.1 Algorithm of determination public and private keys

1. It is chosen 2 primes *p* and *q*;
2. It is computed *N = p * q*;
3. It is computed the value of Euler's function *f (p, q) = (p-1) * (q-1);*
4. It is chosen the prime number e, coprime with *f (p, q);*
5. It is selected the number of d, satisfying condition *e * d mod f (p, q) = 1;*
6. Pair *[e, N]* - public key encryption;
7. Pair *[d, N]* - private key encryption.

2.2 Advantages of the RSA system

- The advantage of asymmetric ciphers to symmetrical is no need to pre-transmission of the secret key in the secure channel.
- In symmetric cryptography - only one key and it is kept secret by both sides, but in an asymmetric cryptosystem - the are two keys, but only one key – is a secret, and it is known only by one side.
- In the symmetric encryption to increase the reliability of the system the secret key it should be updated after each session of transmission information, whereas in an asymmetric cryptosystem pair (e, d) can not be changed for a long time.
- In large networks the number of keys in an asymmetric cryptosystem is much lesser than in the symmetric systems.
- Asymmetrically cryptography system has been successfully working to establish the authenticity of digital signatures and mailing secret key.

2.3 Disadvantages of the RSA system

- The advantage of symmetric encryption algorithm to the asymmetric is that in the first it is relatively easy to make changes.
- Although the messages are securely encrypted, but it is known the recipient and sender with fact of sending encrypted messages.
- Asymmetric algorithms use longer keys than symmetric.
- The RSA algorithm is much slower than DES and other block encryption algorithms. Thus, the process of encryption / decryption using the key pair is two to three order slower than the encryption-decryption of the same text in the symmetric algorithm. And the encryption is faster than decryption and signature verification - faster than signing. Because of the structure of the algorithms in the system with open -key speed the processing of a single block of information is usually ten times lower than the performance of systems with a symmetric key block with the same length. To increase the efficiency of public key is often used mixed methods, implementing cryptographic algorithms of both types.
- In its pure form asymmetric cryptosystems require significantly greater computational resources, so in practice they are used in combination with other algorithms.

For the digital signature (DS) previously the message exposed to be hashed, and using an asymmetric key is signed by only a relatively small result of the hash function.

The asymmetric cryptosystem is used in the form of hybrid cryptosystems, where large amounts of data are encrypted symmetric cipher for the session key, and using an asymmetric cipher is transmitted only the session key.

3. THE EXTENDED ALGORITHM RSA-m

As it is known, asymmetric cryptographic system uses the properties of RSA one-direction functions for integer argument, satisfying the conditions of existence of one of the types of solutions of diofantine equation with *a* = 1. Under the extended algorithm of the RSA (modernized "kriptolock") refers to the following diophantine equation relating to the open *(e, n)* and closed (*p, q, d*) RSA keys

$$e \cdot d = k \cdot \varphi(n) + a = k \cdot \varphi(p) \cdot \varphi(q) + 1 = k \cdot (p-1) \cdot (q-1) + a, \qquad \text{where } \ a > 1 \tag{1}$$

When *a*=1 the expression (1) is a kriptolock usual classical RSA. If you keep a secret from potential enemies (at least for a while) and use the value of *a* parameter other than 1, then we have an extended algorithm RSA, then this upgrade will ensure high reliability even with low RSA key length.

Possible opponents in Moldova can be ordinary programmers crackers (hackers) encrypts the encoded information flows in the inter-bank transactions, "experts" in the forgery of credit cards (smart-card) individual account holders ATM or conventional car hackers.

Generally speaking, if a professional person who specialize in various areas of cryptanalysis and cryptotehnique, are limited in their intellectual and / or technical resources, the RSA c advanced algorithm creates them or compelling or significant obstacles (mostly temporary) when they try to disclose keys. Under limited resources should be understood not sufficiently familiar with the theory, small financial and time parameters, which in turn reduces the possibility of organizing a serious attack on the cryptosystem used locally (with RSA keys within a $64 \div 512$ bit, that is the use value $n = 10^{20} \div 10^{150}$).

Example 1.

The following example shows the difficulties facing the enemy in his attempt to uncover the keys to RSA. It is assumed that the enemy does not yet have the information regarding the proposed upgrade. Suppose we have RSA-m with the following parameters: *p* = 1181, *q* = 1193, *n* = 1,408,933. Then

$$17d = 1406560 \cdot k + a \tag{2}$$

If $k = 1, \ then \ \grave{a} = 3 \to \ d = 82739$.

The enemy, finding the decomposition *n* = 1408933 = 1181*1193 and, assuming that he is dealing with a classical system RSA, will, of course, to "attack" kriptolock form:

$$17d_1 = 1406560 \cdot k_1 + 1 \tag{3}$$

Thus, $d_1 = 496433 > 82739 \ and \ k_1 = 6 > 1$ that is, it seems, is much higher than the values in the real system. This fact will require greater operational capacity to implement the algorithm and cryptanalytic drives, so the enemy beyond the capabilities of the limited resources of its computers.

Example 2.
This example illustrates how, in spite of the knowledge of the expansion of the number *n* of factors, the opponent is faced with another problem - with unsolvable diophantine equation. Here, as in the previous example, it is assumed that the enemy does not know about the use of the upgraded algorithm RSA.

If in (3) the left and right sides multiplied by 5, we get kriptolock form:

$$85d_1 = 1406560 \cdot k_2 + 5 \tag{4}$$

The enemy is knowing that *e* = 85 (the public key) and easy laying, as in Example 1, the number of the factors $n \rightarrow$ p = 1181 and *q* = 1193, receives a diophantine equation in the form:

$$85d_3 = 1406560 \cdot k_3 + 1 \tag{5}$$

Equation (5) is not solvable in general.

At the time, as RSA (m) to the algorithm (4) is quite normal working range of numbers of species $N < \sqrt{n}$. Indeed, taking the message *N* = 13, we get:
first residue (or open connection) $N_1 = N^{85} \bmod 1408933 =$ 1,262,521
second residue (decrypted message) $N_2 = N_1^{496433} \bmod n = 371 \cdot 293$, which is 13^5, or $N = \sqrt[5]{N_2}$ r.

Example 3.
This example illustrates the simplicity of key generation in RSA (m):
At RSA (m), working with kriptolock *p* = 11, *q* = 17, we have a diophantine equation of the form:

$$9d = 160 \cdot k + 2 \quad ; \quad (d = 18,\ k = 1) \tag{6}$$

Suppose now that we need to change keys ($e = 9 \Rightarrow e = 11$).

In the classical RSA in this case requires two prime numbers, sets new public key *e*, then solve the diophantine equation using the extended Euclidean algorithm, which is not easy and will take time.
For example, if we have *n* = 187, and the need to move to a new key, then choose, for example, *e* = 11, *p* = 5, *q* = 7 and solve the equation

$$11d = 24 \cdot k + 1 \quad (d = 11,\ k = 1)$$

In the case of RSA (m), the transition from *e* = 9 to *e*=11, with the same numbers *p* and *q* takes one procedure: division with remainder (negative), i.e. get kriptolock

$$\begin{cases} 11d = 160 \cdot k + 5 \\ (d = 15 \left[\begin{array}{r|l} 160 & 11 \\ \hline -\dfrac{50}{55} & 15 \\ \hline -5 & \end{array} \right]) \end{cases} .$$

Example 4.

Now take kriptolock, where *p* = 461, *q* = 439, *e* = 77. It corresponds to the diophantine equation

$$77d = 201480 \cdot k + 1$$

To find *d* do the following with the release of fission integral part and remainder. When divided (according to Euclid's algorithm) number (201 480:77) have a whole part and the remainder in 2616 and 48 respectively. Further procedure division gives respectively:

Table 1. The integral part of the dividend divider Balance

The integral	part of the dividend	divider	remainder
201480	77	2616	48
77	48	1	29
48	29	1	19
29	19	1	10
19	10	1	9
10	9	1	1
9	1	9	0

Based on the Table 2, the top of which are integral parts of previous divisions, we find (by the rules) the values of *k* and *d*.

Table 2. Presentation of the integral parts of previous divisions

-	1	1	1	1	1	2616
1	1	2	3	5	**8**	**20933**

k=8, d=20933.

Indeed, by substituting these values into the original equation, we get

$77 \cdot 20933 = 201480 \cdot 8 + 1$ or 1611841 = 1611840+1 or 1611841 1 = 1611841.

At the same time, to find the value of *d* ***for kriptolock RSA-m*** at these same values of *p*, *q* and *e* need to do ***only one operation of division*** with the release of a whole part and a remainder.

When divided (according to Euclid's algorithm) number 20148077 have a whole part and the remainder in 2616 and 48 respectively. (See Table 1), which means that in kriptolock RSA-m the private key d has *a* value of 2616, the parameter is 48.

Example 5.

This example shows how to use the algorithm of RSA (m) you can find keys for conventional algorithm RSA.

Need d_1 to find kriptolock

$$7d_1 = 60 \cdot k_1 + 1 \tag{7}$$

There kriptolock RSA-m

$$7d_2 = 60 \cdot k_2 + 3 \quad \text{or in general } 7d_2 = 60 \cdot k_2 + a \quad (d=9,\ k=1)$$

Establish the relation between d_1 и d_1 and d_2.

Of diophantine equations known that between the equations:

$$ax_1 = by_1 + 1$$

and

$$ax_2 = by_2 + c$$

there is a connection

$$x_2 = cx_1 \text{ and } x_{2m} = x_2 \pm mb.$$

Then

$$cx_1 = x_2 \pm mb$$

or in the notation for kriptolocks RSA $ad_1 = d_2 \pm m\varphi(n)$.

In this example $a = 3,\ d_2 = 9,\ \varphi(n) = 60$

Then $3d_1 = 9 \pm m60$.

The possible values d_1 are the natural numbers $d_1 = \frac{9 \pm m60}{3}$, that is 23, 43, 63, 83 ...

Direct substitution d_1 in (7) that $d_1 = 43$ satisfies this equation.

Consequently, $d_1 = 43$ - there is a secret key of this system RSA.

In the literature, sometimes quite correctly points out that the determination of an RSA key should ask prime numbers p and q, and the numbers *e* and *d* are sized according to the equation:

$$ed = k\varphi(n) + 1$$

But for large values of $\varphi(n)$ this procedure is reduced to finding the keys hard to solve the problem in cryptography - the factorization problem.

4. THE DESIGN OF DEVICE ENCRYPTION

4.1 The functional block diagram of data communication system

The developed equipment represents the equipment that was elaborated using the electronic circuits, microcontroller, etc. This device will encode the signal that was obtained from the microphone and it is transferring to another computer via internet and the decoding is made use the another device.

The device has the following functions:

- Capture voice signal from the microphone; Signal amplification; Converting analog to digital signal; Coding data; Data transmission to PC; Receive data from the computer; Decoding data; Convert digital signal to analog; Signal amplification; Transmission signal to the speaker.

In the Figure 2 is represented the functional block diagram of data communication system with two capturing blocks of data processing and communications (DCPCD) that are connected to the two different computers and the computers are connected with each other via the Internet.

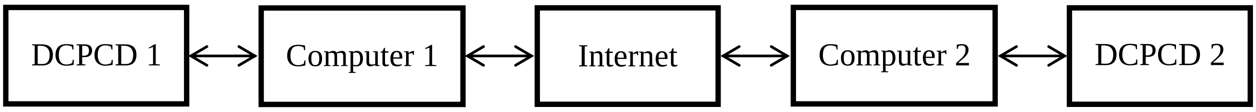

Figure 2. Functional block diagram of the data communication system.

In the Figure 3 is represented the block diagram of the capturing device, processing and communication of data, as goal this device captures the sound signal through the microphone and the signal will be transmitted to the operational amplifier (AO). The captured sound signal from the microphone is low power, therefore we need use the operational amplifier. After signal amplification, the signal is sent to the analog-digital converter (CAN). We need this converter to encode with a high level of data encryption. The microcontroller will processing the data, encrypt them and then the data will be sent to the computer (PC). The encrypted data will be transmitted via the Internet at the other place of the line where the other device will decode and reproduce the original signal. The using such device has the advantage of protection the data transmission through the communication path by hackers that use special programs to capture data packets.

After processing the data, they are transmitted to the digital-to-analog converter (CNA). After converting the data, they are transmitted to the power amplifier (AP). After amplification the signal is sent to the speaker.

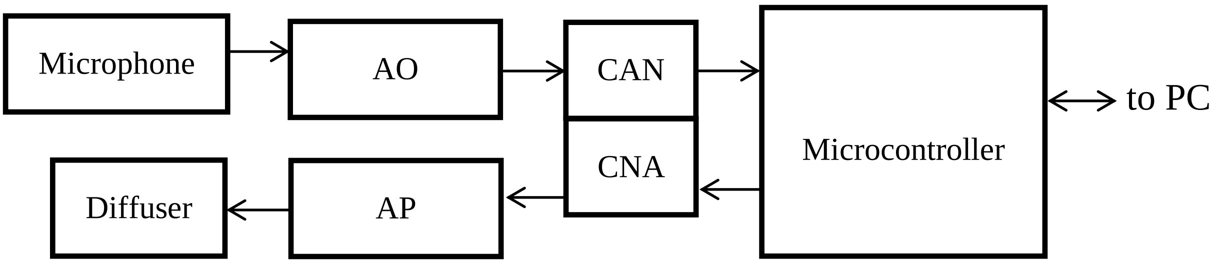

Figure 3. Block diagram of the capture device, data processing and communications.

4.2 The electrical device's schematic diagram of the capture, processing and data communication

In the Figure 4 is represented the principle diagram of the designed device that is composed from the following components: Microphone; Operational Amplifier; Analog-digital converter; Digital-to-analog converter; Microcontroller; Audio power amplifier; Speaker.

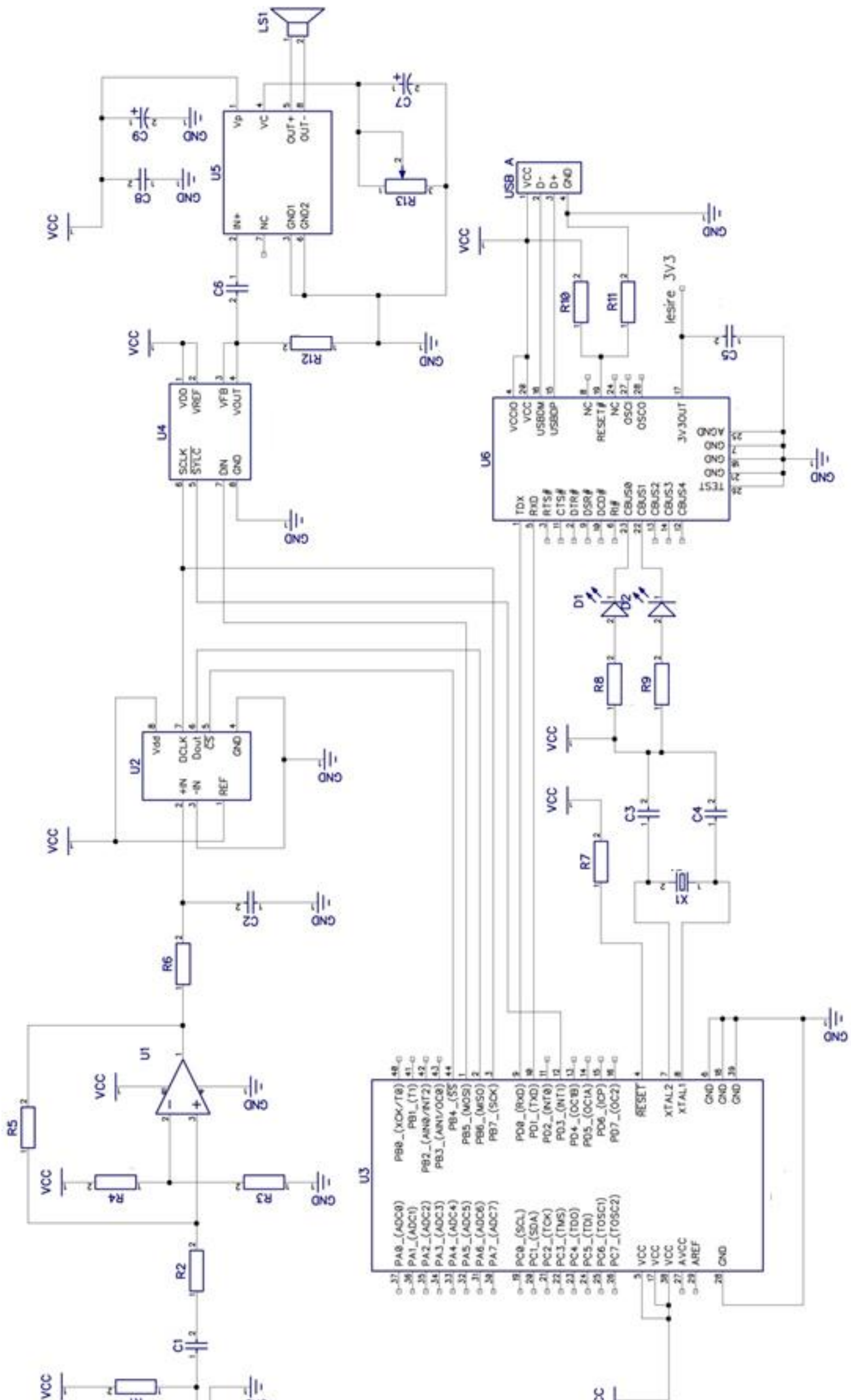

Figure 4. Principle diagram of the designed device.

4.3 The block of capture and signal amplification

The microphone amplifier is an amplifier based on the LM358 chip. The factor of amplification is given by R5 and R2. The R1 is used to limit the current applied to the microphone and C1 blocks all continuous components arising from the microphone. Voltage divider R3 and R4 form the reference level. R6 and C2 form a high frequency filter.

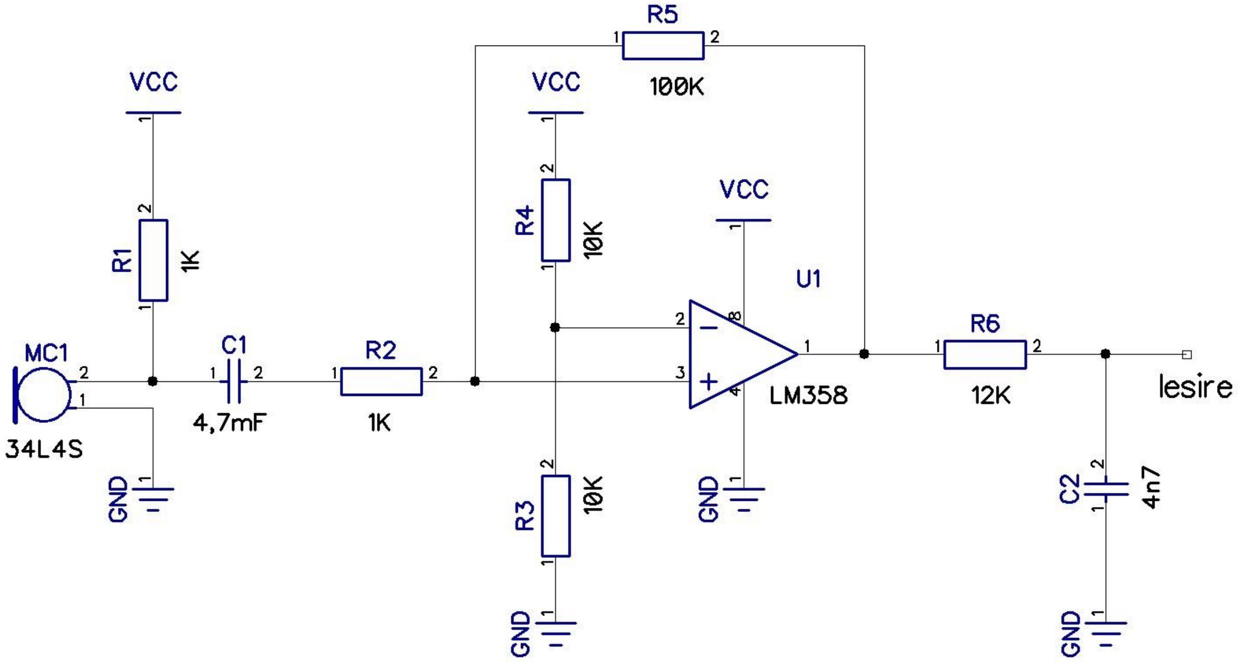

Figure 5. Principle block diagram capture and signal amplification.

4.4 Digital-analog converter

The digital analog converter (DAC) is an electronic circuit that provides at the output the analog quantity (voltage or current) proportional to the number being applied to the input as a combination of binary variables, that implements function of digital-analog conversion. DAC includes the circuits for generating reference voltage or current, the electronic switches controlled by input signal bits, network of resistors and capacitors of precision and circuit of summation currents. The main characteristics of digital-analog converters are:

- Input code;
- Resolution;
- Accuracy;
- Speed;
- Temperature stability;
- Nature and scope of the output signal.

4.5 The block of data processing

Generally the controller is now on electronic structure controlling a process or, more generally, a specific interaction with the environment, without the need for human operator intervention.

The flash memory program with the entire block of extracting instructions, decoding and execution communicates through its own bus, separate of data bus. This type of organization is following the principles of a Harvard architecture and allows the controller to execute instructions quickly.
Power-down mode saves the contents of registers, but blocks the oscillator, disabling all other chip functions until the next External Interrupt or Hardware Reset.

Power-save mode, the asynchronous timer continues to run, allowing the user to maintain a time basis while the rest of the device is off.

Standby Oscillator is running while the rest of state off. This allows very fast start combined with low power consumption. In standby mode extended (Extended Standby Mode), so the main oscillator as well as asynchronous timer continues to run.

Flash memory (on-chip) allows programming by the SPI serial interface.

5. CONCLUSIONS

Doing the research presented in this paper, it can be presented the following conclusions:
1. Application is an extension of the RSA algorithm introduces additional uncertainty parameter to be determined, potentially increases the "hacking" in the case of short-encryption (for privacy) of information can serve as a means to improve the reliability of the system (for example, operational negotiation).

2. Advanced RSA algorithm can significantly reduce the time to generate new keys for the "kripto lock" and thus allows for the process of ***rapid transition from one key to another as many times,*** also complicate the operational work "cracker"

3. With advanced cryptanalysis algorithms RSA opponent (even knowing about the application of the modernization of the algorithm) or face insurmountable fundamental difficulties (Diophantine equation has no solutions), or he needs at this time, beyond the limits of its technical capabilities.

4. Doing this research and implementation of the hardware product, the obtained device is able to capture the voice, encrypt the processing data and decrypt the data in the real time, but it is not excluded that at this moment of the development exist the small delay of the signal.

REFERENCES

1. Agafonov A.F. "Lectures on the comparative analysis of the theory of numbers", Kishinev: samizdat. - 2003, 2006.

2. Oleinik V.L. "Methods for prime numbers - the current state», Chişinău: Akta Akademia All, 1999.

3. Agafonov A.F., "Improved probabilistic algorithms for determining primality", Chisinau: Proceedings of the II International Conference on Informatics, 2002.

4. "Introduction to Cryptography" / Ed. Ed. VV Yashchenko. Izd. MSU 2000.
5. Cheremushkin A. "Lectures on the arithmetic algorithms in cryptography", MCCME 2002.

6. Agafonov A.F, Balabanov A., Shegeva C.H. "A method for the experimental evaluation of the operating capacity of randomized algorithms and the reliability of the conclusion of the simplicity of" Chisinau: Proceedings of the International Conference of Information Technology BIT 2004.

7. Results of science and technology. Problems in mathematics. Number Theory, Volume 49, VINITI, 1990.

8. Shegeva C.H. «A Generation block of prime numbers», Kishinev: Materials Science and Technology Conference of Young Scientists, 2004.

9. Vasilenko O.N. "Number-theoretic algorithms in cryptography", - M. MCCME, 2003.

10. Handbook of Applied Cryptography by A. Menezes, P. van Oorschot and S. Vanstone, CRC Press, 1996.

11. Balabanov A.A, Agafonov A.F. Perspective, the problem of information security in commercial and reliability of fire-alarm systems. Report on the section of Informatics and Cybernetics, direction: "Problems informatsiionnoy security" Moscow, January 23, 2008.

12. Agafonov A.F, Balabanov A., Shegeva C.H. A method for the experimental evaluation of the operating capacity of randomized algorithms and the reliability of the conclusion of the simplicity of the number. Chisinau: Proceedings 3rd International Conference on Informatics, 2003.

13. Agafonov A., Balabanov A. Properties solvability of Diophantine equations of the second degree, and their use in problems of cryptography. Chisinau: Proceedings 4th International Conference on Informatics, 2005.

14. Niculescu G., John L. Techniques and communication systems. - Bucharest: Matrix ROM 2001. - 504p.

15. Mateescu A., Davies, N. signals and telecommunication circuits. - Bucharest: Teaching and pedalogică - 319p.