Modern encryption texts through new applications

April 2020

***by** Panagiotis Giamvrias*

Modern encryption texts through new applications

Abstract

In this paper, a rudimentary approach is initially made to the field of cryptography and some basic cryptocurrency concepts and terminologies are analyzed. They are followed by the kinds of cryptography that exist, and in the end the most modern forms of cryptography are developed, giving a more global picture of the subject under study.

Introduction

Cryptography is a way in which two persons enable to communicate through an unsecured channel in such a way that a third party, unauthorized (an opponent), cannot interfere with communication or understand the content of messages. Post Office and Telecom Companies use widely cryptography in order to respect the confidential and privacy policy. For example, in Post Office, there is strong recommendation to protect and secure information of an envelope or parcel details such as sender and recipient data as well as its cost etc. All of these can be compressed, encrypted and this message is represented by one tracking number.

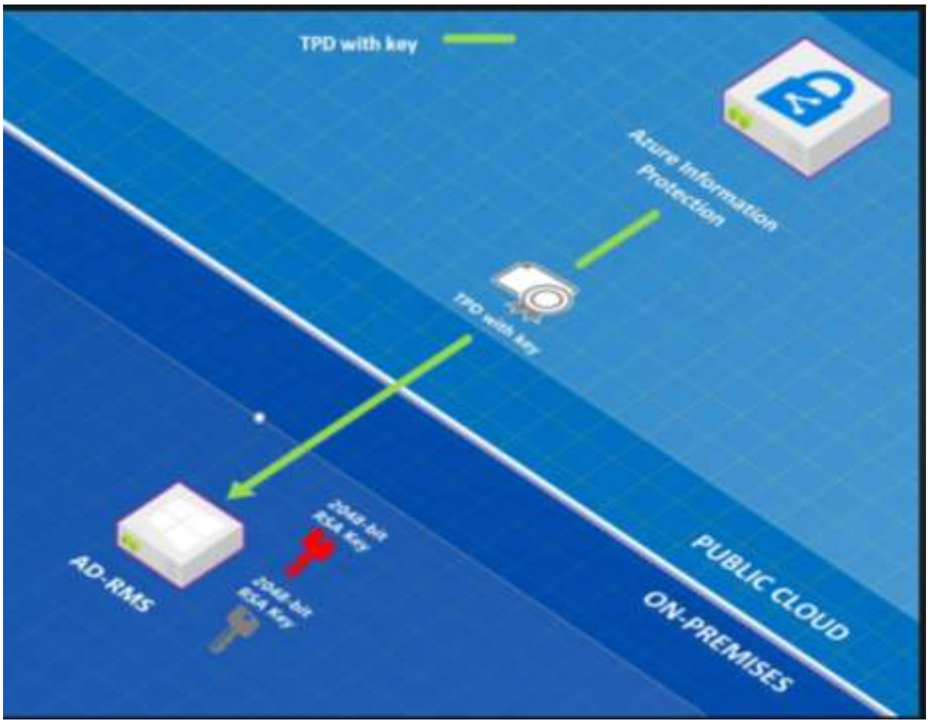


Figure1. Cryptography and keys

Historically, cryptography began thousands of years ago, when people wanted to protect a secret. The root of this word comprises two Ancient Greek words ‘hidden’ and ‘secret’. Perhaps the earliest allusion has been recorded in Phaistos Disc, 2.700 BC, which depicts symbols and ancient letters. Later during 8th century BC, Homer made reference about a cryptography form in Iliad texts. Recent decades, cryptography was used to encrypt messages, i.e. convert information from a normal intelligible form to a puzzle, which without the knowledge of hidden transformation would remain incomprehensible. The main characteristic of older forms of encryption was that the processing was done on the linguistic structure. In the newer form’s cryptography makes use of the numerical equivalent, the emphasis has been transferred to various fields of mathematics, such as discrete mathematics, number theory, information theory, computational complexity, statistical and combinatorial analysis.

1. Terminology

Let’s see few technical terminologies

Encryption is called the process of transforming a message into an incomprehensible form by using a cryptographic algorithm so that it cannot be read by anyone other than the legitimate recipient. The reverse process where the encrypted text generates the original message is called decryption.

Cryptographic algorithm (cipher) is the method of transforming data into a format that does not allow unauthorized parties to disclose their contents. As a rule, the cryptographic algorithm is a complex mathematical function.

Plaintext is the message that is the entry to an encryption process.

Key is a number of several bits that are used as an input to the encryption function.

Encrypted text (ciphertext) is the result of applying a cryptographic algorithm to the original text.

Cryptanalysis is a science that deals with the "breaking" of a cryptographic technique so that without the encryption key being known, the original text can be decoded.

A message is encrypted and decrypted using a cipher and a key. Usually the encryption algorithm is known, so the confidentiality of the encrypted message transmitted is mostly based on the privacy of the encryption key. The size of the encryption key is measured in several bits. The following rule generally applies: the larger the encryption key, the harder the encrypted message can be decrypted by would-be hackers. Different encryption algorithms require different key lengths to achieve the same level of encryption resilience.

Basic Encryption Objectives

Cryptography provides 4 basic functions (objectives):

- Confidentiality: The information to be transmitted is only accessible to authorized members. The information is incomprehensible to a third party.

- Integrity: The information can only be tampered with by authorized members and cannot be tampered with without detection of tampering.

- Non-denial: The sender or recipient of the information cannot deny the authenticity of the transmission or its creation.

• Authentication: The sender and consignee can verify their identities as well as the source and destination of the information with assurance that their identities are not fake.

Types of Cryptosystems

There are two categories in which the cryptosystem has been divided and developed, the Classical or symmetrical cryptosystems and the Modern or Asymmetric Cryptosystems. Below is a detailed diagram of the key components of each cryptographic item

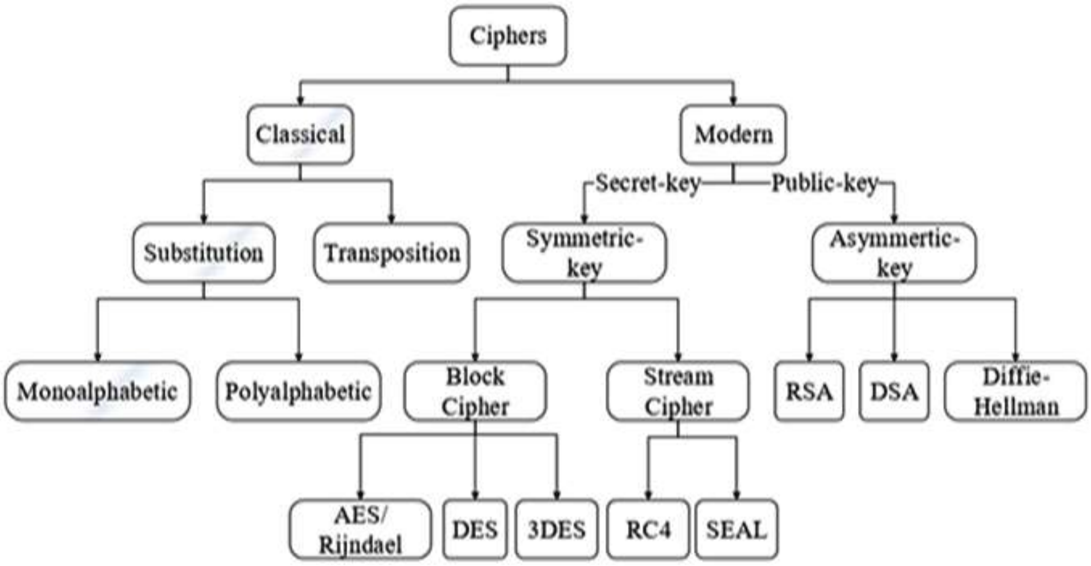


Figure 2: Classification of Encryption Methods

2. Modern text cryptography

Cryptography and DNA

Many new algorithms and techniques have been used for information security. One of recent and modern technology is DNA-using cryptography. We're going up a level above the integrity and confidentiality of data to protect information from intrusions. Mazhar Karimi's work (June 2017) proposes an encryption solution with a new model of symmetric key creation based on DNA, nucleotides, base and mutation pair and DNA conversion to mRNA. The solution proposed by Mazhar Karimi highlights the use of biological processes and the random changes identified in DNA that simulate these processes in key creation just like cryptography.

Initially DNA is simulated as a three-dimensional double propeller, like a spiral staircase. Each propeller consists of other monomerides called nucleotides. Each nucleotide has sugar and phosphate in groups and its base is nitrogen. These nitrogen bases are adenine (A), Thymine (T), Guanine (G) and Cytosine (C).

When Adleman began his research in molecular biology, he realized that these 4 letters (A, T, G and C) possess all the information needed for an organism, and in a similar way can be used to successfully calculate a mathematical NP complexity problem complete. This problem was O(n) complexity in silicon chips and itself was resolved in O(1) using DNA. This was the beginning of the use of DNA in cryptography.

DNA cryptography is a theoretical field of computing where DNA is used to hide information. The smallest DNA consists of 30 nucleotides. DNA is an information repository that is translated according to the table below.

Bits	Nucleotide
00	A
11	C
01	G
10	T

After converting the binary number to Nucleotides, the process of copying is applied if the nucleotide length is less than 60. Then if the nucleotide length is not perfectly divided by the length of a coden, the last coden is modified by repeating the last nucleotide in the sequence. Following the procedure, the single propeller is connected to its pair according to the supplementary rule. So, a complete DNA is created. This is followed by DNA conversion to mRNA. Proteins are called DNA keys. The number of DNA keys depends on how many code-based errors are found and how the tryptophan type amino acids (UGG), glutamine (CAG), arginine (CGA), alanine (GCC) and Aspartic Acid (GAU) resulting from the DNA mutation in mRNA are converted into term code or other amino acids. When all the final DNA keys are created, they are decoded in 8-bit blocks.

The following is an example to make the whole process more understandable. (Mazhar Karimi, Waleej Haider, “Cryptography using DNA Nucleotides”, June 2017)

Suppose we have the following message in binary digits:

01101101011001010111001101110011011000010110011101 100101

When these are translated into nucleotides we will have:

GAAAATAAGGCCATAAATTCATAAACATATCGGAAA
ATAAGGCCATAAATTCATAAACAT

When the mutation process is applied, and the two propellers come together we will have:

GAAAATAAGGCCATAAATTCATAAACATATCGGAAAATAAGGCCATAAA
TTCATAAACATCTT TTATTCCGGT

ATTTAAGTATTTGTATAGCCTTTTATTCCGGTATTTA AGTATTTGTA

When the transcription process begins, the sequence is done as follows:

GAAAAUAAGGCCAUAAAUUCAUAAACAUAUCGGAAAAUAAGGCCAUAA
AUUCAUAAACAC

UUUUAUUCCGGUAUUUAAGUAUUUGUAUAGCCUUUUAUUCCGGUAUUU
AAGUAUUUGUA

When the conversion to mRNA and the key proteins are created, we have:

GAAAAUAAGGCCAUAAAUUCAUAAACAUAUCGGAAAAUAAGGCCAUAA
AUUCAUAAACAC

UUUUAUUCCGGUAUUUAAGUAUUUGUAUAGCCUUUUAUUCCGGUAUUU
AAGUAUUUGUA

ACAUAUCGGAAAAUAAGGCCAUAAAUUCAUAAACAUCUUUUAUUCCGG
UAUUUAAGUAUU UGUAUAGCCU

UUUAUUCCGGUAUUUAAGUAUUUGUA

AUUCAUAAACAUCUUUUAUUCCGGUAUUUAAGUAUUUGUAUAGCCUUU
UAUUCCGGUAU UUAAGUAUUUGUA

GUAUUUGUAAAA

Which when we translate it into bits we will have:

01000000011100000010000000000011010000000111000000100000000111010101
1011010 1000101010101001111101010 11011010100010101010

000000110100000000111000000100000000011101010110110101000101010101010011
1101010 11011010100010101010

001000000000111010101101101010001010101010011111010
101101101010001010101010

010010010000

Each DNA key creates a binary block

B = {b1, b2 … bn}

In each binary block, every 8 bits of blocks are grouped in

bi = {k1, k2 … kn}

To encrypt the first 8 digits of the message are collected and shifted left by 1 bit and the XOR function is applied with each in block 1, this continues for all {k1, k2 ... kn} in b1.

$CM = (M << 1) \oplus b1kj$

The second binary block shifts the message by 2 bits and applies XOR with each key in block 2, and it also goes on for all keys in block b2.

$CM = (CM << 2) \oplus b2kj$

The general formula that arises is:

$CM = (CM << i) \oplus bikj$

Therefore, the final encrypted message is:

11101001111010011110100111101001111010011110100111 101001

Cryptography and Mobile Phones

We will refer to the escalated multiplication of elliptical curve as ECSM (elliptic curve scalar multiplication). In their article entitled "A NEW ALGORITHM FOR SIGNED BINARY REPRESENTATION AND APPLICATION IN MOBILE PHONES", authors present and propose an algorithm that can replace the elliptical curve protocol of cryptography on which our mobile phones are based, thus performing better mainly in terms of time.

The most important function in the elliptical curve is step-by-step multiplication. This can be mathematically represented as F=rG where F,G are points in the elliptical curve and r is any positive integer. Using the binary extension to represent r as it is a sum from n-1 to s=0 is considered the most common way. Here, rs is an element of a finite set of elements, the Dk.

It is therefore a question of optimising the step-by-step multiplication. This can be done by introducing fast complex methods and by using coordinates systems instead of affine coordinates. It can also be accelerated through precomputations techniques and hardware conversions.

The binary representation of the length of the staggered k and the number of "1" in it, control the performance and cost of the ECSM. Several studies have been done to find the best way to represent k, and authors in this case use the simplest of these methods, the binary method. It is therefore defined as $(k_{l-1}, k_{l-2},..., k_0)_2$ where ki ∈ (0,1), i=0, 1, 2, ..., l-4. In addition, each integer can be expressed as a sum from 0 to l-1 of $k_i\ 2^i\ P_i$ and we all call it P_2 and we have another point in the elliptical curve. The algorithm describing this procedure is presented below

Entry: $k = (k_{l-1}, k_{l-2},\ldots, k_0)_2$, $P_1 \in E(F_p)$

Exit: Q = kP

Step 1: Q = P

```
Step 2: for i = l – 1 down to 0 =>
    Step 2.1: If $k_i$ = 1 then Q = Q + P
    Step 2.2: Q = 2P
    Step 3: Return Q
```

Then, they suggest other algorithms such as the right-to-left of the Mutual Opposite Form (MOF) in ECSM, the Complementary Recognition Method (CRM), the Non Adjacent Form (NAF) of the staggered k, the unmarked binary representation of the staggered k for the direct recognition method (DRM), accompanied by examples and execution results. These four algorithms are compared according to the runtime to create unattached binary representations. The results of this comparison are summarized in the following image.

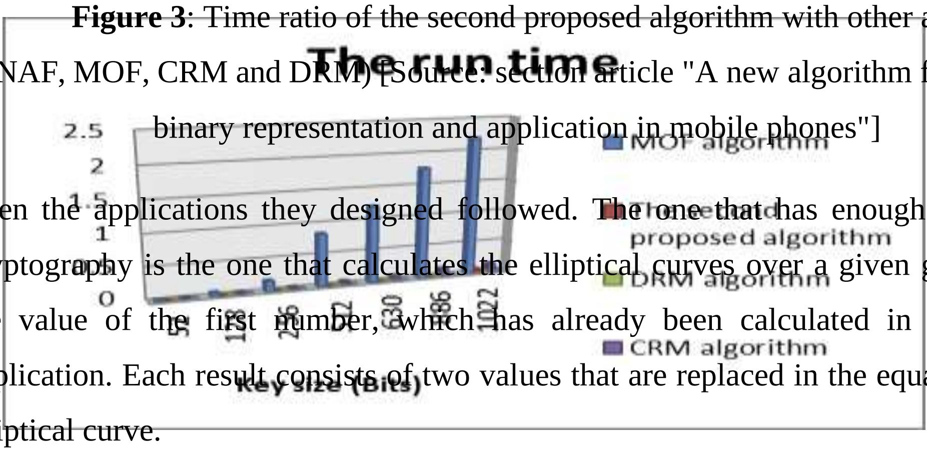
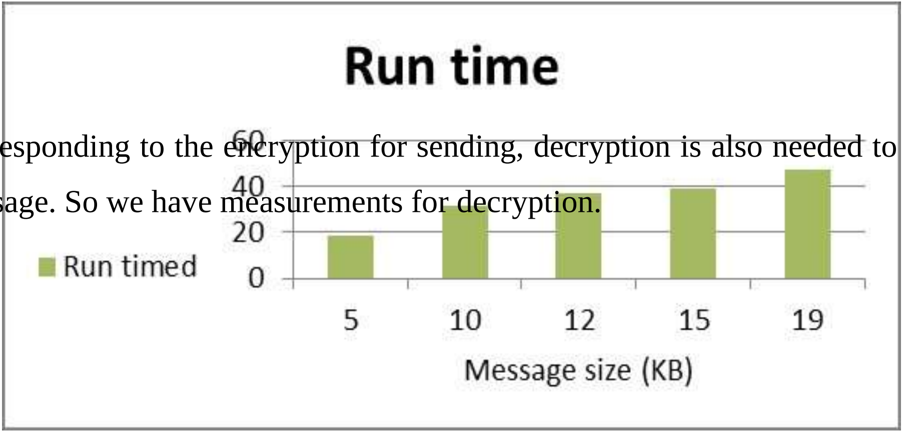


Figure 3: Time ratio of the second proposed algorithm with other algorithms (NAF, MOF, CRM and DRM) [Source: section article "A new algorithm for signed binary representation and application in mobile phones"]

Then the applications they designed followed. The one that has enough interest in cryptography is the one that calculates the elliptical curves over a given giving only the value of the first number, which has already been calculated in a previous application. Each result consists of two values that are replaced in the equation of the elliptical curve.

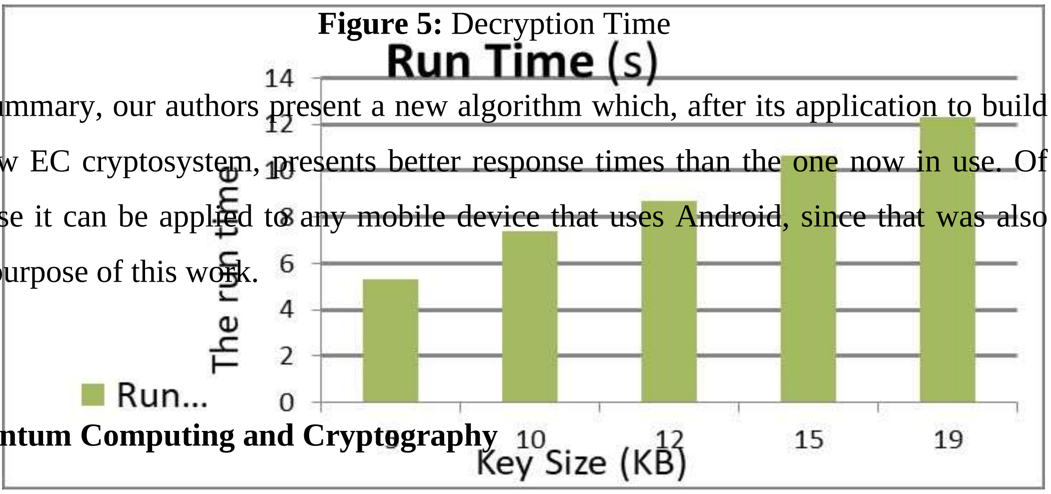
Obviously all this data needs to be encrypted to be transferred and the time it takes to encrypt is a very important factor. Below are the seconds it takes to encrypt corresponding KB.

Figure 4: Encryption Time



Corresponding to the encryption for sending, decryption is also needed to receive the message. So we have measurements for decryption.

Figure 5: Decryption Time



In summary, our authors present a new algorithm which, after its application to build a new EC cryptosystem, presents better response times than the one now in use. Of course it can be applied to any mobile device that uses Android, since that was also the purpose of this work.

Quantum Computing and Cryptography

Article "Quantum Computing and Cryptography" by Tim Moses, refers to a calculation model that exploits the strange yet wonderful properties of quantum objects. Some problems, whose difficulty increases exponentially with the size of the problem in the classic model, are scaled polynomially (or even linearly) in the quantum model, thus making a solution possible even for large systems.

In the classic computational model, the basic information unit is a "bit", which can adopt one of two mutually exclusive states, either "0" or "1". The most rudimentary function that can be performed with them is a gateway, which takes some bits at its inputs and produces a bit in its output. These gateways can be combined into circuits to perform more complex operations, such as a data processing unit.

Similarly, in the quantum computing model, the basic unit of information is called "quantum bit"or" qubit", which can exist in any of what physicists call "ideal quantum two-state system". Examples of such systems include photons (with vertical and horizontal polarization representing the two rectangular states), electrons and other spin-1/2 systems (with a rotation of top and left representing the two rectangular states) and systems defined by two energy levels of atoms or ions.

Each status corresponds to the known values of "0" and "1" bits. Qubits, however, can obtain values that are overstates of these two states. Thus, they can be assumed to occupy a state that is a combination of both the "0" status and the status "1". While quantum mechanics describeseveral interesting phenomena, it has received the most attention due to its suitability as the basis of a quantum computer.

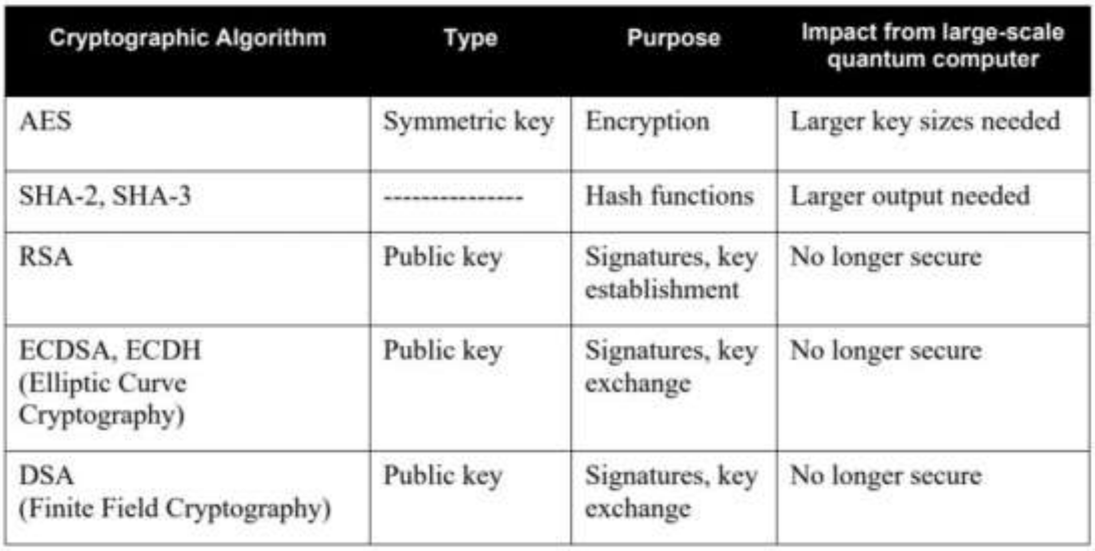
With the construction of large quantum computers, there will be at least two significant implications for information security. Quantum computers will affect the security of both symmetric key algorithms (e.g., block encryption) as well as public key algorithms (such as RSA), although the severity of the effects will be different in each case. Those who report the public key cryptography the consequences are more serious. Quantum computers can run algorithms that break all popular public key systems at trivial intervals. For example, the quantum Shor algorithm can retrieve an RSA key in polynomial time.

Quantum cryptography was created to address this problem. This is another basic distribution method that would be immune to quantum computing attacks, but in the environments where quantum cryptography is applied. This is because quantum cryptography provides "absolute security". Note, however, that there are some auxiliary functions within 26 quantum cryptographic shapes that depend on symmetric or public key encryption and these will be affected exactly as described above.

Post-Quantum Cryptography

To meet the needs of quantum computing power we have now passed to post-quantum cryptography. In academia, this new science bears the name "post-quantum cryptography.". Caution though, post-quantum cryptography should not be confused with quantum cryptography (or quantum key distribution), which uses quantum mechanics to create a secure communication channel. The following illustration shows the effect of quantum computing on common cryptographic algorithms.

Table 1 - Impact of Quantum Computing on Common Cryptographic Algorithms



Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	---------------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Then we will briefly look at the main families for which post-quantum elements have been proposed. These families include those based on grids, codes and polynomials with many variables, as well as a few more.

Grid-based cryptography

Cryptosystems based on grid problems have gained interest, for a few reasons. Exciting new applications (code encoding and encryption based on features) have been made possible using the use of encryption grids. Most grid-based keycreation algorithms are relatively simple, 29 efficient, and highly parallelized.

Code-based cryptography

In 1978, the first code-based cryptosystem (McEliece cryptosystem) appeared, and it hasn't been broken since. Newer variants have introduced more structure to the codes in an effort to reduce the size of the key, however the added structure has also led to successful attacks on some suggestions. While there have been some suggestions for coded signatures, code-based cryptography has seen more success with encryption programs.

Multiplication Polynomial Cryptography

These systems are based on the difficulty of solving multi-variable polynomial systems in finite fields. Several cryptosystems with many variables have been proposed in recent decades, while many have been broken. As multifactorial encryption systems, they are considered, as the most successful approach of signatures.

Hash based signatures

Hash-based signatures are digital signatures manufactured using hash functions. Their security, even against quantum attacks, is quite understandable. Many even of the most efficient hash-based signature systems have the disadvantage that the signer must keep a record of the exact number of messages he has signed because any error in this count will result in insecurity. An additional disadvantage is the production of a limited number of signatures. Any increase in the number of signatures increases the signature size at the same time.

Magic Square

The magic square is a sequence of numbers in an array of equal rows and columns, where the arithmetic act between the numbers in the same row or column or diagonal of the square always returns the same result. The common result is called the magic constant of the magic square. The most common arithmetic act in magic squares is to add between numbers. A characteristic magic square is the one shown in the image below and sums up to 15. In addition, there are other versions that can be reproduced in three-dimensional form and as magical rectangles, or there are modifications where shapes are used instead of numbers.

In the article we examine in this section entitled "A Research on Enhancing Public Key Cryptography by The Use of MRGA with RSA and N-Prime RSA", our authors present a methodology for using the magic rectangle to ensure greater security. As they say, the use of the magic square depends entirely on the mathematical calculation of the table. In the magic rectangle, the sumof all columns is the same as in the columns. This type of table is used and can make data another time mapping and thus create another level of security in communication. Thus, by using the magic rectangle we can enhance the public key cryptosystem and the algorithms used in cryptography

The methodology of the proposed one is described in the following steps:

(Hardik Gandhi, Vinit Gupta, Indra Rajput – "A Research on Enhancing Public Key Cryptography by The Use of MRGA with RSA and N-Prime RSA")

1) Construct a magic rectangle of even number of squares, dimensions 32x48 and use instead of the ASCII panel with 128 values. The magic rectangle contains a total of 1536 values. It has been divided into 12 quadrants, each consisting of 128 characters.

2) Each character of plain text is converted into numbers based on its position in the magic rectangle in different quadrants. The numbers are encrypted and decrypted with RSA and N-prime RSA algorithm.

Phase One: Creation of the magic rectangle

Magic rectangles are the rectangles that have a sum of all the elements in the rows equal and the sum of the column elements are also equal. We will be given the maximum and minimum values and from this we will create the 4x6 table. Two different types of register calculation will be applied. According to the tables given in the registry-1 and in the registry -2, first the 4x6 registry will be created and then we will calculate the maximum and minimum of this registry. The second type of registry will then be applied. Thus, the process will continue and alternatively the calculation will be made for a 4x6 registry. After the production of four squares 4x6 the assembly will come and create a register of 8x12. This process continues until we have four 8x12 registers thus creating a 16x24 table. Then the four 16x24 tables will be joined and 32x48 tables will eventually be created.

Phase Two: Mapping a magic rectangle

From the 32x48 registry there will be a total of 1536 values and there are a total of 128 ASCII values. We'll split this registry into 12 sub-registers so that we have 128 values in each registry. For each given message each character will be there with its ASCII value. And each character will be given a table with 128 values. Thus, 1*1 character will have 1*1 registry. The first character will go to the first registry and the second goes to the second registry and so on, so that the appearance of two identical characters will not have the same cryptographic text. Decryption will be done following the reverse procedure.

Phase Three: Encryption with RSA and N-prime RSA

The RSA template will be applied so that the mapped value is taken from the magic rectangle as an input, and then there will be an encryption process. Similarly, the decryption process will be done in reverse order. At the same time the decrypted message will be received as an input and the value of the magic rectangle will be the output of the algorithm.

1) Each user creates a public/private key pair with:

- selection of two random large samples - p, q

- calculates their system coefficient N = p.q

- note ø (N) = (p-1) (q-1)

- random encryption key option e, where $1< e< ø(N)$, gcd (e, ø(N))=1

- resolves the following equation to find the decryption key d,

d = 1 mod ø (N) and $0 \leq d \leq N$

- publishes its public encryption key: KU = {e, N}

- keeps private decryption key secret: KR = {d, p, q}

2) N-Prime RSA:

The N-Prime RSA is similar to RSA, but we can get more than two first numbers to generate keys for encryption and decryption. As shown below,

- Select two or more separate primary numbers p, q, r, and so on.

- Calculate n = p*q*r; "N" acts as the modulus value of both the public and private key.

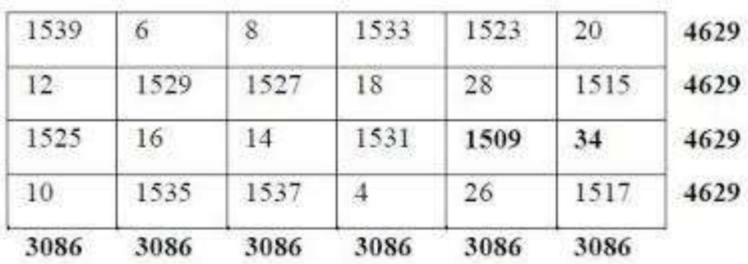
- Calculation of the Attendance function of Euler, Φ (n) = (p - 1)* (q - 1)* (r - 1) and so on.

- The remaining steps are similar to Standard RSA.

Phase Four: Possible Outcomes

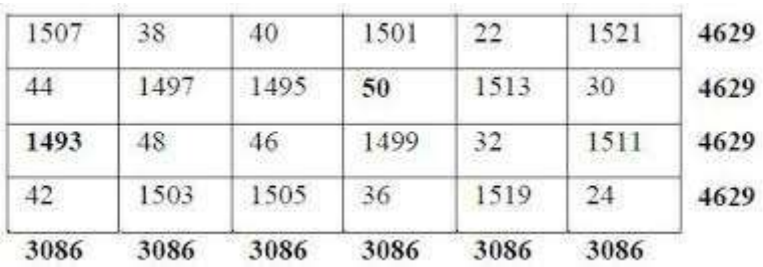
(The following tables are derived from article A Research on Enhancing Public Key Cryptography by The Use of MRGA with RSA and N-Prime RSA")

1) Magic rectangle 1 (MR _sub1): Minstart=4, Maxstart=1539, S1=0



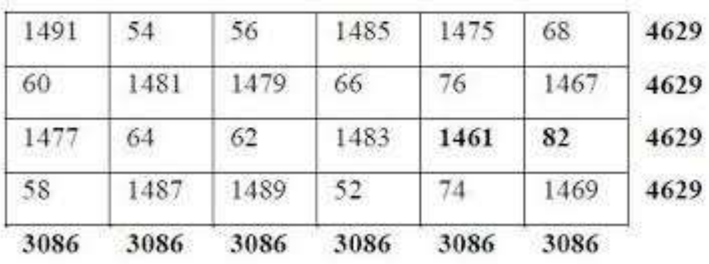
1539	6	8	1533	1523	20	**4629**
12	1529	1527	18	28	1515	**4629**
1525	16	14	1531	**1509**	**34**	**4629**
10	1535	1537	4	26	1517	**4629**
3086	**3086**	**3086**	**3086**	**3086**	**3086**	

2) Magic rectangle 2 (MR _sub2): Minstart=36, Maxstart=1507; S2=0



1507	38	40	1501	22	1521	**4629**
44	1497	1495	**50**	1513	30	**4629**
1493	48	46	1499	32	1511	**4629**
42	1503	1505	36	1519	24	**4629**
3086	**3086**	**3086**	**3086**	**3086**	**3086**	

3) Magic rectangle 3 (MR _sub3): Minstart=52, Maxstart=1491 S3=1

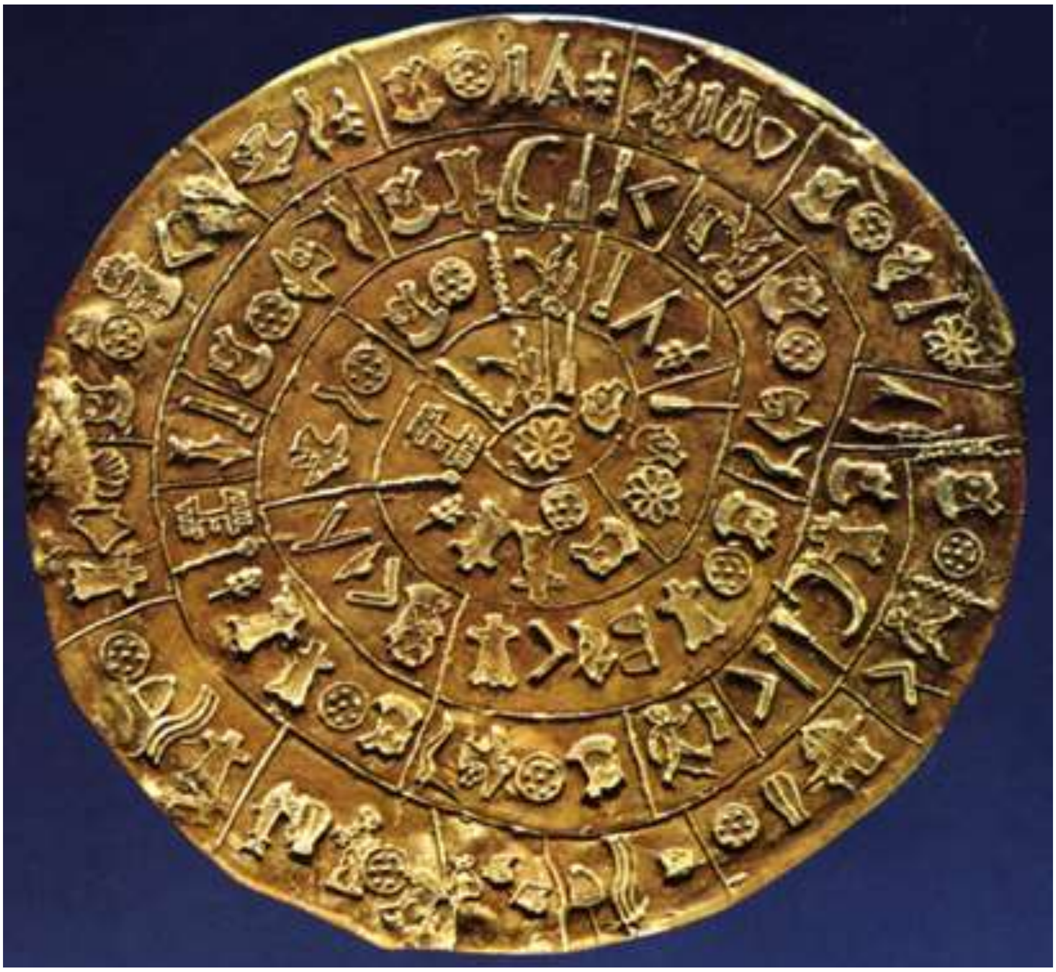


1491	54	56	1485	1475	68	**4629**
60	1481	1479	66	76	1467	**4629**
1477	64	62	1483	**1461**	**82**	**4629**
58	1487	1489	52	74	1469	**4629**
3086	**3086**	**3086**	**3086**	**3086**	**3086**	

This task prohibits each attacker from obtaining plain text in a readable format. Security is improved as there is no repeat of the values in the magic rectangle. There are several parameters used to increase the complexity of time to construct the magic rectangle such as the sum of columns, minstart, and maxstart values. Even if the attackers find the original MR values, it is very difficult to locate the order or column. It is a vital role in increasing randomness and the safety of the algorithm. The use of RSA has the problem that the first numbers used should be over 100. So they have used n-prime RSA, so that more than two prime numbers are used and this can make predicting the first numbers easier.

3. Conclusion

Today, Modern Technology provides applications in every area of our daily lives: from unlocking a car remotely and monitoring a paid satellite channel, to purchasing products using credit and debit cards, installing a software update, using a mobile network or the Internet, and exploiting a citizen's range in various countries and soon and in Greece. In the near future we expect many exciting new applications of radio frequency recognition (RFID) to combat counterfeiting and counterfeiting and smart environments.



Phaistos Disc /Material: Clay /Created :2nd millennium BC

Appendix — References

[1] Β. Α. Κάτος και Γ. Χ. Στεφανίδης, Τεχνικές Κρυπτογραφίας & Κρυπτανάλυσης, Θεσσαλονίκη: Εκδόσεις Ζυγός, 2003

[2] A. S. Tanenbaum, Computer Networks, Prentice Hall, 2003.

[3] M. Burmester, Σ. Γκρίτζαλης, Σ. Κάτσικας και Β. Χρυσακόπουλος, Σύχγρονη Κρυπτογραφία : Θεωρία και Εφαρμογές, Αθήνα: Εκδόσεις 1Παπασωτηρίου, 2011.

[4] Mazhar Karimi, Waleej Haider, “Cryptography using DNA Nucleotides”, June 2017

[5] N.M.G. Al-Saidi, M.A. Magamiss, S.F. Ibraheem, A. Kh. Faraj, “A new algorithm for signed binary representation and application in mobile phones”, Journal of Mathematical and Computational Science, Vol 8, 03 January 2018

[6] Tim Moses, Quantum Computing and Cryptography – “Their impact on cryptographic practice”, Entrust Inc, January 2009

[7] V. Dubois, P. Fouque, A. Shamir and J. Stern, Practical cryptanalysis of SFLASH, “Advances in Cryptology” — CRYPTO 2007, Lecture Notes in Comput. Sci. 4622, Springer-Verlag, 2007, pp. 1–12., http://dx.doi.org/10.1007/978-3-540-74143-5_1.

[8] Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner and Daniel Smith-Tone - “Report on Post-Quantum Cryptography”, April 2016

[9] M. Mariantoni, Building a Superconducting Quantum Computer, Invited Talk PQCrypto 2014, October 2014 Waterloo, Canada. https://www.youtube.com/watch?v=wWHAs--HA1c [accessed 4/20/2016].

[10] Hardik Gandhi, Vinit Gupta, Indra Rajput – “A Research on Enhancing Public Key Cryptography by The Use of MRGA with RSA and N-Prime RSA”, IJIRST - International Journal for Innovative Research in Science & Technology, May 2015