International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 2, Issue 1, January 2015, PP 22-28
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
www.arcjournals.org

Gaps of Cryptography and Their Automatic Treatments with Reference to Classical Cryptography Methods

Dr. Mozamel M. Saeed

Salman Bin Abdul-Aziz University Collage of Science
Dept. of Computer Science, KSA
mozamel8888@gmail.com

Abstract: *The subject of security in the automatic information system is highly considered as an interesting subject in the view of researchers and workers who are dealing with those systems. The world wide spreads of computers have had direct impact on the development and efficiency of automatic information system. But still there is a continuous fear towards the security aspects and possibility of dependency of computers in directing and handling the automatic systems in permanent image and minute, and its ability to protect secrets and privacy from assault and snooping. The main objective of this paper is the exposure to gaps of coding systems with focus on classical encryption methods , designing mechanisms and scientific methods, to help in raising the security efficiency , and to provide the entire protection for data by using different methods with a special focusing on sensitive data.*

Keywords: *Cryptography, classical Methods, Information Security, sensitive data, Automatic Treatments.*

1. INTRODUCTION

Cryptography is the study of mathematical techniques for a number of information security aspects such as Confidentiality, data integrity, entity authentication and data origin authentication. So the Cryptography is not a way for doubling the security information only, but it is a set of techniques.

The idea of Cipher System is how to hide the authoritative information in a way not to be understood by any unauthorized person. The interceptor is the person who intercepts and obtains the words from the cryptographer. The purpose of the cryptography is to maximize. The aim is to conceal information, thus reducing the number of possible choices by monitoring bilateral unacceptable models tend to have a kind of arrangement.

The information security is resulting from the need for exchanging public and private information. Computer systems and networks have been used in worldwide. Therefore, the security concepts are not clear. During the period of first computer, the physical security along with the appropriate policy of choosing staff, were sufficient to provide security. But now it became insufficient and inflexible after the discovery of time – sharing computer systems, which is consisting of several terminals spread across a wide geographical area.

When the safety and security of electronic communications started to appear, it did not seem important. Because, most of the stored information was not of great sensitivity. As it seems today. The more valuable stored information in the computer, the greater desire of some people to access it for vandalism or graft by selling to those who are willing. For this reason, the information security has become of great importance.

There are many issues, regarding the time – sharing computer systems. And computer networks have strong link with the protection of communication channels. The networks not only link the terminals to the corresponding computers, but also have a vulnerability in network connection with host computer (Host). Due to the natural property of any channel of communication, the enemy may have connection center access. Therefore, physical protection is not significant and the only way to strengthen protection in communication channels is the application of Cryptography.

2. CRYPTOGRAPHIC OBJECTIVES

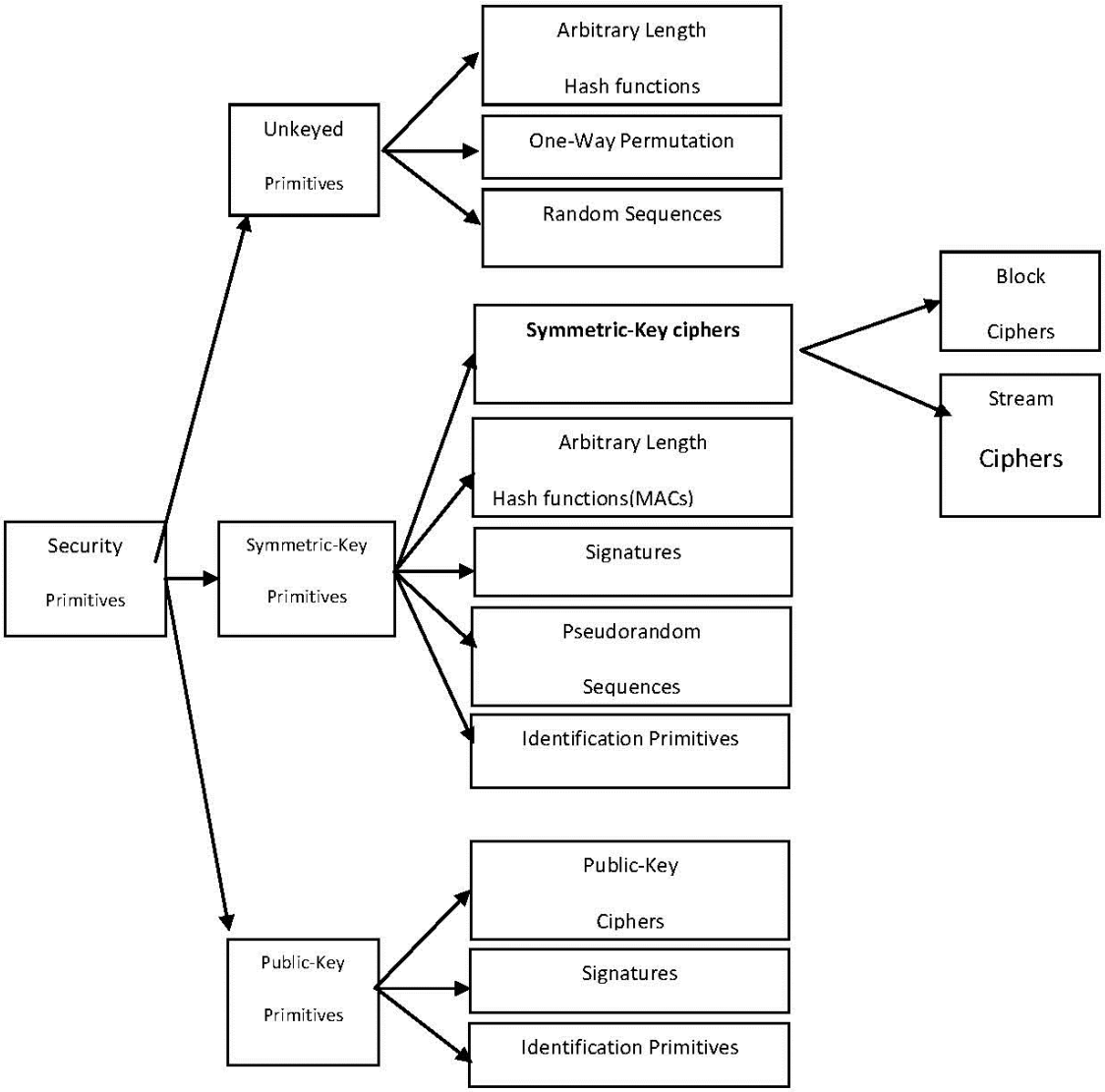

Fig1. *The classification of encryption objectives*

The information security goals can be placed in four frames:

- Confidentiality: is a service through which knowledge prevents the contents of information about all participants, except the authorized persons who are allowed to have possession of such information. The concept of Secrecy is synonym of Confidentiality and privacy.
- Data Integrity: is a service targeting changes for unauthorized data. In order to achieve this goal you must possess facilities to detect unauthorized data. The processing of data should include operations such as: Insertion, Deletion, and Substitution. The receiver of the message must be able to prove that the term has not been altered during the sending process. And the enemy should not be able to bring a false statement instead of legitimacy.
- Authentication: Is a service or function to do the Identification. It is applied to all participants in the communication and information. All parties involved in communication should try to know each other. As for the information received it should match the original information sent as well as the date of sending, its contents and transmission time.
- Non-Repudiation: is a service or function that prevents any Entity from denying a commitment or previous work done. So when such a dispute occurs between parties involved, there should be a mean for resolving it. The mean can be through involving a trusted third party. The sender must not be able to make a false denial after a period, claiming that he has sent a word.

In addition to that, the purpose of encryption is to make the message or record not perceived by the unauthorized people. Any attempt to re- encipher the same message – correctly, is considered as a significant security risk. Such cases must be seriously prevented.

Furthermore, there are encryption tools which sometimes are called primitives. They have been used in the provision of information security. They can be evaluated through several aspects such as:

- Level of Security: it is difficult to be expressed quantitatively. And often is given a vocabulary concept number of required operations (using the best currently known ways) to frustrate those goals. Sometimes, the level of security is called Work Factor.
- Functionality: The primitives need to be integrated in order to achieve a number of security objectives .And the primitives are chosen according to its efficiency. And the most effective characteristics will determine the main effective primitive that will be chosen.

3. SECURITY AND PROTECTION OF INFORMATION SYSTEMS

The ideal system is defined as a system that has a flat distribution for each statistical properties of the code, which means the properties of natural language.

Security is linked directly to the difficulties for the reverse conversion or cryptographic transformations for any system. The protection granted can be evaluated through lack of accuracy (Uncertainty), that facing the enemy (Opponent) to specify the allowed keys. The goal of any decoder is to identify the key (k), clear text (p) or both. After all, he can be convinced about the potential information about (p). Is it a text or data table (Spreadsheet) or anything else.

It is obvious that the full security is a desirable objective in encryption. And full security means that, if the parser code cannot obtain additional information, he will not be able to obtain any information from the text objector, meaning that it is an unbreakable system.

4. CRITERIA OF ENCRYPTION POWER

There are several criteria, called attacks which have been used for the purpose of determining the suitability of any cryptographic system. Its capability in attacking the encrypted text only and attack Known-Plain text. Any system able to resist the cipher text is taken as a reasonable indicator for system security. There is a third attack which is called the selected clear-text attack. We realize that it is actually impossible to design a system of encryption to prevent every possible attack. But the experience is able to build systems which balance security with functional, cost, and time. In addition to the three basic types of attacks there are other ones such as: The attack of brute-force. It is known as a clear text. It is not hard to obtain it. Therefore, the brutal-force has become the standard for the security code. Cryptographic systems that look perfect are often vulnerable to the brute force attack if certain processors are applied. As for the system which prevents the violation when subjected to the chosen plaintext attack, can certainly be a secured system. Then it is considered as an efficient system. If its actions (Procedures) never enlarge or maximize the accuracy of the small key, until it seems like it is too large in length.

5. THE ENCRYPTION AND CRYPTOGRAPHY ANALYSIS

The encryption and code analysis are two manifestations of studying cryptology; each depends on the other and causing a certain effect on it in a certain interaction. With the aim to develop improvements to strengthen the security code by designing more efficient attacks. The success in achieving safe code rarely happens, since the failure is common in this area.

From the attacks that face the encryption methods, it is noticed that, the enemies have numerous options for any encoding method. The reason is that, most of the enemies have been trying to get part of the encrypted text, which is available for all the enemies. And then examine the relationships in this text in order to discover the key security system. If the enemies could not get a clear text, they will continue trying and searching for any information, whatever the contents of the clear text. Because they will certainly be useful in the analysis of the cipher text.

6. GAPS OF ENCRYPTION SYSTEMS

6.1. General Gaps in Encryption Systems

- Most applications support the encoding method for a long period of time which helps the analyst to focus on this way until he is able to acknowledge the key or designing a way to know the key, each time it is changed.
- The key change is a complex process, due to the overlap of key management and distribution factors. Especially when increasing the number of participants and then, some departments remain using the key for a long period. This will enable the analyst to discover it.
- Even if the key has been changed, still its distribution through the networks will lead to objections by enemies.
- All the cryptographic systems increase to be vulnerable as time passing, this is due to the attacks. And the breed encryption methods that have been evaluated in a certain period as strong, they will definitely become weak in later periods. For example, the classic methods were often reliable in data encryption.

6.2. The Gaps of Classical Encryption Methods

- Homophonic: Can easily be broken. And cannot conceal the statistical characteristics of the clear-text and language. Subject to the clear-text attack. It takes only few seconds to be broken in the computer.
- Running-Key Cipher: Although this code has a Period that is equal to the length of the text. But can be easily broken.
- Simple replacement blades: These codes are subject to violation, due to the statistical attacks which include code blocks, and the holsters that are designed by the analysts. In order to explain the clear text blocks, and the encrypted text in contrast.
- The flow Blades: easy-flow mathematical analysis.
- Blades of the blocks: it works in a typical special unit smaller than the clear text, (usually binary) and then the encryption of any clear text in block blades will produce the same cipher text when using the same key.

7. HIGHLY SECURE MECHANISM OF SENSITIVE DATA

It is noted that all encryption methods are prone to breakage by different means. There is a perpetual conflict between designers and developers of cryptographic systems. Also between the enemies and intruders, especially those analyst of the code. The computer is a new factor in weakening the cipher. The cryptographic methods that were strong in a certain time period become weak in the future period, due to technical development in the designing of computers, especially the methods that rely on gaining strength on computational and mathematical capacity. These methods have been subject to breakage, due to technical development in terms of speed, size store and the processing power of computers. Also it is noted that, the breaking of certain encryption methods lead to attempts that can strengthen them, by adding some of the complicated steps. But after a period it will be broken again and so on.

A number of different mechanisms, each with special specifications have been proposed to address the gaps from which the encryption methods suffer, during the security of data protection. In term of:

7.1. Using the Switch Mechanism of Cryptographic Methods to Strengthen Data Security

This mechanism uses many cryptographic methods for data protection in various ways. The aim of the mechanism is to deceive and hide the information. From the enemies, and confuse them, when they try to get any of the cryptographic methods which are implementing the encryption process.

This mechanism provides a complex way to fool the enemies. Using multiple encryption methods, secret encryption keys, and many ways to check these methods. If we suppose for example that there are four ways that revealed the key for first method is x_1 , duration of key detection for the

second method x_2 , for the third method is x_3 and for the fourth method is x_4 , the time it takes to discover keys all together will be through collecting these time periods, with the addition of extra time to know what kind of methods were used. So the probability of detecting the key will be very low.

This mechanism requires the storage of tables containing the names and numbers of methods used for encryption; you can use the name of the method or manner. Using the number of the method is far better for security than using the name. Therefore, we have used numbers of methods. And the numbers of the methods should be swapped either periodically or by agreement of the beneficiaries so that, for example, method number 5 become 10 then give other number for method number 10 and so on. So that we don't allow any opportunity for the enemy to discover the switch mechanism during his monitoring the numbers.

In order to increase the security of this mechanism, the one message can be encrypted, by using more than one encryption method, after dividing into several sections. Each section of the phrase with different encryption method. In this mechanism many choices have been placed to the beneficiary for the protection of his data. Thus, we believe there types of data that are of utmost importance worthy to deserve this kind of attention, complexity and develop obstacles for the enemies. No matter the time or size, or quality of user complexity. Only the important is data protection.

7.2. Multi- Level Authentication

Most applications of authentication depend on one level of authentication. These applications rely on encryption as best method for authentication. The methods of encryption generally get broken. The result is that the methods of authentication will also be subject to breakage.Therefore, we try develop a more restrict mechanism to the authentication, depending on the kind of user authentication and message authentication. With especial consideration for the sensitive applications.

In this mechanism the required recipient's personality has to be verified in more than one authority level, through passing various stages. Using in each stage certain authorization method, the beneficiary will not shift to any level, unless he has passed the previous level successfully. The traversal mechanism has been designed in several styles. There are levels that must be met in full, and others met in certain ratios. This mechanism has been designed so that it faces the beneficiary on the first level, the authentication method known and characterized by its strength. And when passing that level successfully then moving to the second level, which has been designed so that the recipient faces a series of questions with confidentiality and privacy. Any information concerning the beneficiary himself or other beneficiaries involved with him, and then moves to another level. Facing an authorization method also known and so on. You can also put different methods of authorization in each level by the parties involved the purpose is an identification of beneficiaries.

7.3. Mechanism of Integrating Encryption With Coding

In many of the protection methods used, we found little use for the encoding method in data protection. And most of the encoding methods prefer the encryption in those processing. The encoding means, replacing the whole words or phrases of the clear text with specific elements consisting of groups of letters, shapes, numbers or a total combination of them. There are several methods for encoding which shows that there is a link between call origin and colour-coded such as cheque book, but the encoding objects that is required for data protection is the need to code book it does not indicate that there is any relationship between the original and the encoded word. The lack of any relationship between the words and phrases is necessary for putting obstacles in front of the enemies.

7.4. Using the Authorization Method in the Verification of the Physical Entity Parts

Such as a floppy disk that contains unwanted information like viruses. This proposal requires some sort of change in the CD-RW disc, as well as the auditing procedure.

7.5. Using the Methods of Modeling in the Simulation Methods of the Enemy

By analyzing the key length used and the method of its selection and management. On the other hand, a predictive measure can lead to knowing that there is an attempt to uncover the key by the enemies and its type, then issue a warning to the participants about the attempt so that they can take precautions and change the key used. The action must be designed accordingly to give enough time to take those precautions.

7.6. Using the Concept of Natural Language in the Science of Artificial Intelligence (AI)

With written symbols merge mechanism supports encoding with encryption and fill gaps, where the written symbols contain words contrasting symbols. And these words will be fixed on the one hand, and may sometimes using another word by authorized participants giving the same meaning of the original Word, but are not installed in the book icons and this gap could be addressed by using the natural language for the purpose of providing synonymous with equality, this could lead to freedom available to authorized users, and those words will be added to words that aren't in the code book.

7.7. The Equality of the Equalizing Cipher Text With Clear Text in Some Values of N

Through which the enemy could discover the relational ties between cipher text and plaintext. It is a point of weakness that the specialists could not be awared of. Even in the event of some who referred in the RSA algorithm regarding it as a weak point in this algorithm. That will minimize the importance of the small probability of its occurrence, but we believe that there is a major weakness, particularly in sensitive security information. Therefore, we propose a designing through which the values can be discovered and dealt with. So that it will not appear as equal when sending.

8. CONCLUSION

This paper reflects the importance of encryption as necessary mean in the process of protecting transmitted information that has been stored, and should not be reached by such unauthorized who can make violation. The paper has reviewed some of the encryption methods and their limitations (gaps), and concluded the provision of mechanisms and methods of specification for addressing these gaps from which the encryption suffer, in order to provide high security protection of sensitive data and computer information systems.

REFERENCES

[1] A. J .Menezes, P. C. vanOorschot, and S. A .Vanstone, “Handbook of Applied Cryptography “, CRC Press, 1997.

[2] Al- Kadi I.A., Origins of Cryptography: the Arab Contribution, CryptologiaVol X VI, 1, 1992.

[3] Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 1996.

[4] CzeslawKoscielny, MiroslawKurkowski and Marian SrebrnyModern Cryptography Primer: Theoretical Foundations and Practical Applications , Dec 3, 2013.

[5] Deley. D.W. Computer generated random numbers, hrrp//dehyed@netcom.com, 1999.

[6] Diffie W.D. and Hellman M. New Directions on Crytography, IEEE Transactions on Information Theory, vol. It 22 no. 6, 1976.

[7] E .Biham, “Cryptanalysis of multiple modes of operation “, Advance in Cryptology – ASIACRYPT ‘ 94 (LNCS 917) , 278 – 292 , 1995.

[8] Fred Piper and Sean Murphy, Cryptography: A Very Short Introduction , 2002.

[9] Hans Delfs and Helmut Knebl, Introduction to Cryptography: Principles and Applications (Information Security and Cryptography) , Nov 2010.

[10] Helen F. Gaines, Cryptanalysis: A Study of Ciphers and Their Solution , Apr 1989.

[11] Jason Andress, The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice by Jun 2011.

[12] Jonathan Katz and Yehuda Lindell ,Introduction to Modern Cryptography: Principles and Protocols (Chapman & Hall/CRC Cryptography and Network Security, Aug 2007

[13] John R. Vacca ,Computer and Information Security Handbook, Second Edition , Jun 2013.

[14] Kaufman C., Periman. R and Speciner N. Network Security-Private Communication in a Public World, Prentice- Hall 1995.

[15] Keith M. Martin , Everyday Cryptography: Fundamental Principles and Applications ,May 2012.

[16] Menezes A.J. Vanorschot. R.C. and Wanstone. S.A. Hand book of applied Crytography, crc press,1997.

[17] Michael E. Whitman and Herbert J. Mattord,Principles of Information Security , Jan 2011

[18] M .Matsui, "The first experimental cryptanalysis of the Data Encryption Standard " , Advance in Cryptology – EUROCRYPT ' 94 (LNCS 839) , 1- 11 , 1994 .

[19] Niels Ferguson, Bruce Schneier and Tadayoshi Kohno, Cryptography Engineering: Design Principles and Practical Applications, Mar 2010.

[20] OdedGoldreich , Foundations of Cryptography: Volume 1, Basic Tools , Jan 2007.

[21] Rhee M.Y, Crytogaphy and Secret Adat Communication, MC Gray- Hill 1994.

[22] Schneier B. Applied Crytography, John Wiley and Sons 1995.

[23] S.K. Langford and M.E Hellman , " Differential –linear cryptanalysis " , Advance in Cryptology – CRYPTO ' 94 (LNCS 839) , 17- 25 , 1994 .

[24] Wade Trappe and Lawrence C. Washington,Introduction to Cryptography with Coding Theory , Jul 2005, 2nd Edition

[25] William Stallings , Cryptography and Network Security: Principles and Practice 6th Edition, 2013.

[26] William Stallings, Cryptography and Network Security: Principles and Practice, 5th Edition, Jan 2010.

AUTHOR'S BIOGRAPHY

Dr. Mozamel M. Saeed is the head department of Computer Science at Faculty of Science, Salman Bin Abdul Aziz University. I've published some papers internationally.