International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 10, 2020
ISSN: 1475-7192

The cryptography by identifying the different cryptographic algorithms in the sequence of their temporal existence and importance

[1]MSc Waseem Saad Nsaif, [2]MSc. Wisam Mahdi Abas, [3]MSc. Abdullah Farhan

Abstract

This research consists of basic concepts and principles of cryptography, then it moves to identify the different cryptographic algorithms in the sequence of their temporal existence and importance, to begin with, traditional cryptographic algorithms, then it turns to the corresponding cryptographic algorithms where it discusses a number of algorithms including DES, AES, Triple DES, and others. Then proceeds to identify cryptographic algorithms using the public key, and also discusses a number of them such as RSA and ECC. Although the list presented previously does not cover at all the possible possibilities for network penetration, it does clarify the area of network security concerns. Network security is complicated by some fun. Here are some of the reasons for this observation:

1- Issues of achieving security related to networks and communications are not as simple as they seem to newcomers to this field. The requirements appear quite clear, and indeed, most of the basic requirements for security are evident through their names: confidentiality, identity verification, refusal to recognize, perfectionism. However, the mechanisms used to achieve these requirements can be very complex, and their understanding may require solid logic.

2- When a person develops a protection mechanism or algorithm, he must consider all possible types of attack on his system. Often times, the resulting attack is based on a different view of protection, allowing for the exploitation of unexpected vulnerabilities in protection mechanisms.

3- In light of the previous item, we see that the procedures used to provide a service are often unclear and intuitive. At first glance, it is not clear that these measures are necessary to fulfill the security requirement for which they were set. However, the picture becomes clear after all the procedures and possibilities for breaching the established security requirement have been studied.

[1] College of physical education and sport science - Diyala University- Iraq
[2] Presidency of the University of Diyala, Diyala University, Iraq
[3] College of Agriculture, Diyala University, Iraq

Received: 15 May 2020 | Revised: 5 Jun 2020| Accepted: 20 July 2020

4- When designing the various mechanisms to achieve security, a decision must be made about where to use these mechanisms, from two perspectives: physical, that is, what are the network points that need this mechanism. Boolean, i.e. in which layer or layers should this mechanism be used.

5- Most protection mechanisms include more than one algorithm or one protocol. Most subscribers must possess some confidential information (for example cryptographic keys), which leads to questions about how this information is generated, distributed, and protected. In addition, there is a reliance on communication protocols, which sometimes complicate the development of the protection mechanism. For example, if the correct work of one of the protection mechanisms assumes that there are time limits for the transmission of the message from the sender to the receiver, then any protocol or network that offers the ability to change this time interval will make the limits imposed by the protection agent a meaningless amount, and thus the mechanism will lose Protection takes effect.

We see from the above that there are many things that must be taken into consideration. This chapter provides an overview of the topics on which this thesis will be built. A general discussion will begin with network security services and mechanisms, and potential attack types that have been identified. For these mechanisms. The overall model is then developed to review network security mechanisms and services.

Keywords: *cryptography, algorithms, network security*

I. Introduction

The director responsible for system security in an organization (which is often called the system security director) needs a clear way to define the security requirements for his system, in order to plan the protection used and to acquire the products that provide this protection.

One of these methods requires awareness of the following three points related to information security:

• Methods of attacking the security of the system: These are activities that lead to exposing the protection of the institution's information.

• Security Service: These are the mechanisms designed to detect and prevent the attack on information and its recovery in the event of certain dangers.

• Security Service: It is the service that improves the security of data processing systems and data exchange systems in the organization. These services aim to nullify attacks on the organization's information, using one or more protection mechanisms. We will try to clarify these three points from the last point

Services

Let's look first at the security services usually associated with regular physical documents. The activities of the human race depend on various fields, such as trade, foreign policy, and military hopes Etc. to use and exchange documents while securing the confidentiality and completeness of these documents. Documents usually have dates

and signatures, and these documents often require some kind of protection against exposures, forgery, and smuggling, such as whether they are documented somewhere, stamped with a seal, officially registered, and so forth.

The large penetration of information systems in various areas of life, especially professional affairs, has led to the replacement of regular paper documents with electronic information or documents, and therefore these electronic documents must perform the same functions as normal paper documents. However, the features related to electronic documents made achieving these functions or services difficult:

1 - It is usually possible to distinguish between the paper document and any copy of it, but it is impossible to distinguish between the electronic document and any copy of it because the electronic document is in one way or another a specific sequence of digital cells only.

2- The change in the paper document can leave a physical effect that reveals this change or amendment. For example, the eraser can leave a small white spot within the limits of its effect. In the case of electronic documents, changing the content of a khan or signal will leave no physical impact.

3- Any verification or proof process related to paper documents is based on the set of physical properties of this document (for example, the form of a manual signature, or the author's seal of justice). As for the verification of the authenticity of the electronic document, it must be based on an internal effect contained in the information.

Table 1 shows some of the common traditional document-related functions whose counterparts are required to implement electronic documents. These functions can be considered as requirements that must be met by security or protection services.

The list listed in Table 1 is relatively long, and it alone cannot be a guide for organizing the protection service. Instead, computer security and network security research have focused on some general security services that include most of the jobs required to secure information security. These services will be reviewed in the next paragraph:

. Table 1 **a partial list of public jobs to ensure data integrity**

the definition
Authorization
License and/or coincidence
Signature
Testimony (writing with justice)
Matching

legal responsibility
The receipt
Authentication of the original and / or receipt
Sign a check
Entry (Exit)
Validate validity
Time of occurrence
Authenticity - for programs or files
Polling or voting
Property
Registration
Approval/disapproval
Privacy (confidentiality)

Mechanisms

There is no single mechanism that implements all the functions listed in Table 1. We will see in the context of this research many mechanisms that integrate into achieving the various parts of this tour, but we can mention that there is one element that enters into the structure of many of the protection mechanisms used: Blinding techniques. Blindness, or diversions similar to blinding, are actually the most common mechanisms for achieving security. Therefore, this book focuses on developing, using and managing these technologies.

Attack

Information security, as contained in many books, means how to prevent an attack, and if that does not happen, how to detect an attack on systems that depend on its work for information, and then how can the information

that was attacked be recovered, without interfering in the sense of information with a limit Itself. Table 2 includes a list of examples of the attack, each of which appeared in one of the actual cases. These examples are special cases of attack that the organization or people are trying to address or prevent. As for the nature of the attack in which an organization is concerned, it varies from case to case. Fortunately, you can understand the issue by looking at the general types of attacks from different perspectives, which is the subject of the next paragraph.

. Table 2 **Examples of attacks**

1- Owning illegal access to information.
2- Impersonating another user to shift responsibility or to use other people's license to:
A- Generate fraud or fraudulent information
B- Modifying real information.
C- Using a fraudulent identity to obtain illegal entry.
D- Fraudulent confirmation of information transfers.
3- Disclaim responsibility for information generated by the fraudster.
4- Claiming to receive information from another user, while the impostor himself actually generated it.
5- A claim that information was sent to a receiver (at a specific time) while in reality it was not sent (or was sent at another time).
6- Disclaiming the fact of receiving information already received or claiming to have received it at a different time.
7- Extending the fraudster's powers (to enter, generate information, distribute, ...)
8- Modifying the licenses of other people (without having the authority to do so).
9- Hide the existence of some information or withhold it from other information.
10- Intrusive communication between two parties in the form of an effective communication node.
11- Collecting information about the people who accessed the information (files, databases ...) and when this access was made, in order to analyze this information and extract what is useful of it.

Received: 15 May 2020 | Revised: 5 Jun 2020| Accepted: 20 July 2020

12- Weakening confidence in the data integrity protocol, by exposing information that the article is supposed to keep confidential (according to the terms of the protocol).
13- Corrupting software functions by adding hidden or secret functions.
14- Have others violate the sanctity of the protocol by providing incorrect information.
15- Weakening confidence in the protocols, as a way to cause a clear system flaw.
16- Preventing connections between users, especially confidential interference, in order to reject trusted connections as untrusted communications.

OSI security architecture

The security manager, as mentioned earlier, needs an organized and specific method for determining the requirements, and thus assessing the various security products and policies and selecting the necessary ones. This is fundamentally difficult enough in a central data processing environment, but when using LANs and WANs, things get more complicated. In its Recommendation X.800 H, or "Security Architecture for OSI", the World Telecommunication Union (ITU) identified this regulated path. The OSI security architecture benefits these managers as a way to streamline security provisioning. Moreover, computer and communication manufacturers have developed security features for their products in line with this regulation, as it has become a recognized global standard. The OSI security architecture provides a useful overview of many of the concepts used in this book. It focuses on services, security mechanisms, and possible types of attacks.

Protection services

Recommendation X.800 defines protection services as those services provided by the open system communication protocol layer, which ensures adequate security of the system or the transferred data. The following definition given in RFC 2828 documents may be clearer: processing or communication services provided by the system to provide a special type of protection for the resources of this system. Security services implement honest policies that depend on security mechanisms. The X.800 Recommendations divide these services into five classes and fourteen special services (as indicated in Table 1.4). We will explain each one separately.

Authentication

Authentication services focus on making connections reliable. In the case of a single message, such as a warning or alert signal, the authentication service function is to provide a guarantee to the recipient that the message that you have received is actually coming from the source it claims to be from. In the case of reciprocal messaging, as is the case between the terminal and the host computer, the matter includes two things. First, when starting a call, the service must ensure that both parties are reliable or in a more precise sense, that is, they are actually the ones who call

themselves. Second, the service must ensure that no interference occurred during the communication process, such as if a third party is disguised under the name of one of the parties and thus has an illegal transmission or reception process available to it. There are two authentication services that are defined in this field:

• Peer entity authentication: Provides identification or verification of the identity for both parties. This service works at the time of communication or during the messaging phase. It tries to secure confidence in one of the parties in the event that this party does not try to secure it, either because it is impersonating another person or when the illegal return of the previous contact.

• Data origin authentication: This service aims to confirm the source of the data. This service does not provide protection against data copying or modifications. This type of service supports similar e-mail applications, in which case there is no previous interaction between the parties connected to each other.

Access control

Access control is understood in the context of network security as the ability to control and limit access to the host system and its applications through the communications provided. To achieve this, the party wishing to access must first be identified and then assigned access authorities will be defined.

Data confidentiality

The confidentiality or privacy of data means the protection of the transferred data from negative (ineffective - which will be explained later). Depending on the content of the transferred data, several levels of protection can be determined. The most widespread services protect data transmitted between users over a period of time. For example, if a TCP connection is established between two systems, then general protection prevents the release of any user data transmitted over the TCP connection. Narrow forms of this service can also be defined to ensure the protection of a specific message or even a specific field within a message. These challenges are less beneficial than the general pattern, in addition to being more complex and more costly during the application's work. Another part of confidentiality is protecting the information stream from analysis. This is accomplished by not leaving the attacker room to monitor and know the source, fate, frequency, length, and other characteristics of the mobile information stream during communication operations.

Data integrity

As in the confidentiality of data, data integrity can be applied to a chain of transmitted messages, to a single message or to a specific field within a message. In this case, we also see that a useful pattern is a case of applying data integrity to the entire data stream. The connection-dependent data integrity service, which is the service that deals with all threads, ensures that the message is received exactly as it was sent, without any multiplication, implantation, modification, rearrangement, or forwarding. This service also provides treatment for data destruction operations as well. Consequently, the contact-dependent perfectionism service covers both modifying the message chain and permanently rejecting the service. On the other hand, non-communication services, which deal only with specific

messages regardless of their overall context, generally provide protection against message modification only. We can distinguish between services that provide recovery functions and those that do not. The luxury services are affiliated with effective anti-attack activities, and therefore are more concerned with detection than they are with prevention. If any violation of the data integrity is revealed, then the luxury services will somehow express that, then other programs or the investor will manually retrieve the data that was attacked. Instead, there are special mechanisms in place to recover from the loss resulting from the loss of data integrity, and we will see that later. The embodiment of automated recovery mechanisms is one of the best alternatives available.

Non-repudiation

Denial means that the sender or recipient is prevented from denying the transmitted message. Consequently, when the message is sent, the recipient can prove that the message was actually sent by the alleged sender. Similarly, upon receiving the message, the sender can confirm that the message was actually received by the alleged recipient.

Availability service

Both programmers X.800 and RFC 2828 define availability as a system feature or system resource that is accessible or used upon request by any person defined and defined in the system, depending on the performance specifications of this system (i.e. the system is available if the service is provided Consistent with its design when requested by the user). Various types of demolition can result in loss or reduction of availability. Some types of attacks can be repelled by automated countermeasures, such as confidentiality and cryptography, while others require physical action or interference to prevent them or to recover from the loss of some distributed system elements. X.800 documents treat availability as a feature associated with many security services. However, it is sometimes helpful to sort out a service for availability. Availability service is the service that protects the system to ensure its availability. It is specifically directed against an attack that leads to unavailability of services. It depends on the resource management and control of the system and therefore depends on the access control service and some other security services.

Table 3 **Protection services (according to) X.800**

Data integrity	**Authentication**
Ensure that the received data is exactly that which was sent by the licensee (that is, does not contain any modifications, additions, or responses).	**Ensure that the calling party is the same person claiming its identity.**
Communication integration with the ability to restore	**Peer authentication**
Ensure the integrity of all user data on contact, and discover any changes, insertions,	**Use with a logical connection to secure the identity assurance of the calling party.**

deletions, or responses to any data within the entire data sequence with an attempt to recover the original data.	
Communication integration without the ability to restore	**Data origin authentication**
As described above, however, with detection only, with no possibility of recovery.	**During a transmission connection, it ensures that the origin of the data being received is the person who claims its identity.**
Integration of selected fields with connection	**Access control**
Ensuring the integrity of some of the fields chosen within the user data for a block of data that is transferred over the connection, and it takes the form of making sure that the chosen fields have been modified, inserted, deleted, or answered or not.	**Preventing unauthorized use of resources (that is, this service controls who can have access). To a particular resource and under what conditions this access can take place and what can be done by those who use this resource).**
Non-contact integration	**Confidentiality of data**
Secure single data block integrity offline, and can take the form of detecting any data modifications. In addition, a limited form of response detection may be provided.	**Protecting data from unauthorized disclosure.**
Integration of selected fields offline	**Confidentiality of contact**
Ensuring the integrity of selected fields within one offline block takes the form of determining the probability of a change in these fields.	**Protect all user data on a specific connection.**
Failure to decline commitment	**Confidentiality of the selected fields**

Received: 15 May 2020 | Revised: 5 Jun 2020| Accepted: 20 July 2020

To provide protection against the refusal of one of the participating parties to contact, to know about its participation in whole or in part.	**Confidentiality of selected fields within user data within a given connection or within a single block of data.**
The original is not rejected	**Data flow confidentiality**
It provides proof that the letter was sent by the designated authority.	**Protecting the information that can be extracted by**
The destination is not rejected	**monitoring the flow of information through communication.**
Proof insurance that the letter has been received by the designated authority.	

Protection mechanisms

These mechanisms are clearly divided into two parts: mechanisms that can be applied in the special protocol layer and mechanisms that are not dependent on any protocol layer or security service. These mechanisms will be covered in the appropriate places of this book and therefore we will not expand on them now, and we will suffice to comment on the definition of the cipher. X.800 documents distinguish between reversible encryption mechanisms and non-reversible encryption mechanisms. Reverse encryption mechanisms are simply encryption algorithms that allow data to be encrypted or encrypted, and then retrieved or decrypted. Non-reversible encryption mechanisms include Hash Algorithms and message identification codes used in digital signature and message authentication applications. Table 6.1 based on X.800 documents between protection services and protection mechanisms are presented.

Security attacks

The X.800 and RFC 2828 and security attacks documents were categorized in a useful way, in which they divided these attacks into two basic types: passive attacks and effective demolitions. A passive attack tries to know or use the information, but without ever having to finalize the system's resources. As for an effective attack, it tries to change the system’s resources or influence its work.

Negative attacks

Passive attacks are by their nature part of eavesdropping or transmission control. The aim of the aggressor in this case is to obtain the information transferred. Two subtypes of these attacks can be distinguished: obtaining message content and analyzing information flow. The first type - which is to get the message content - can be easily understood, as a phone conversation, email, or file transferred can contain sensitive and sensitive information or confidential information. Naturally, we try to prevent infringement from accessing this content. The second type of

passive attack - information flow analysis - is more ambiguous. Suppose we have some way of disguising the content of messages or other information that constitutes the flow of information, and therefore the aggressor will not be able, even if he obtains it, to reveal its content or understand its content. A common way to camouflage content is to encrypt. But even if we use encryption protection, the aggressor will still have the ability to monitor message patterns. Thus, it will be able to determine the location and identity of the connected host computers, and it can also estimate the transmission and length of these messages. The attacker can use this information and analyze it to guess what the connection is. A negative attack is difficult to detect because no change is made to the data. However, it is useful to prevent the success of this type of attack, usually by using cryptography. Therefore, the emphasis on preventing a negative attack must be more than exposing it.

Table 4 p**rotection Mechanics (X.800)**

Unspecified protection mechanisms	**Specific protection mechanisms**
Mechanisms that are not part of any OSI security services or protocol layer	**It may be included within the appropriate protocol layer to secure some OSI security services.**
Reliable work	**Encryption**
A work that can be verified to be true with respect to some criteria (for example: according to the criteria specified by a security policy).	**Use mathematical algorithms to convert data into an unreadable form directly. This conversion and the restoration of data to its original form depend on a certain algorithm and a number of encryption keys (maybe equal to zero).**
Security patch	**Digital signature**
The tag associated with a resource (which may be a data unit) that defines or specifies the trustworthy attributes of that resource.	**Data appended to, or a cryptographic transformation of, a data unit to allow the receiver of the data unit or verify the origin and integrity of the data unit and to protect it from distributions (three times by the receiver).**
Discovering events	**Access control**
Discover events related to security.	**A set of mechanisms that define access laws for resources.**
Impact of security notation	**Data integrity**

The data collected can be used to facilitate the codification of security operations. Which constitutes an independent review or test of the system's records and activities.	**A set of mechanisms used to ensure the integrity of a data unit or stream of a data unit.**
Restore security	**Authentication exchange**
Dealing with requests from mechanisms, such as juvenile handlers and management functions, and carrying out restoration work.	**A mechanism that is supposed to include the identity of a party by exchanging information.**
	Paste traffic
	Insert bits within voids in a stream of data to thwart traffic analysis attempts.
	Routing control

Table 5 **the Mechanism**

the service	**Encrypt**	**Digital signature**	**Access control**	**Data integrity**	**Authentication exchange**	**Paste traffic**	**Routing control**	**Documentation**
End point authentication	**yes**	**yes**			**yes**			
Data origin authentication	**yes**	**yes**						
Access control			**yes**					
Confidentiality	**yes**						**yes**	

Received: 15 May 2020 | Revised: 5 Jun 2020| Accepted: 20 July 2020

Traffic flow confidentiality	**yes**					**yes**	**yes**	
Data integrity	**yes**	**yes**		**yes**				
Failure to decline commitment		**yes**		**yes**				**yes**
Availability				**yes**	**yes**			
	yes	**yes**			**yes**			

II. Conclusion

An effective attack includes making some adjustments to the data flow or creating a false data flow, and it can be divided into four categories: stealth, redundancy, message modification, and service blocking. Masquerade is when someone introduces themselves as someone else. A hidden attack usually includes another type of effective attack. For example, the identification sequence can be captured and retransmitted after a real identification sequence has occurred, enabling a defined and legitimate person with few privileges to obtain higher privileges by impersonating the characteristic of the one with the highest privileges that has just been identified. Replay involves simply changing or delaying part of a legitimate message in order to produce an illegal effect. For example, the message can be modified allowing Zaid to read the secret accounts file, to read "Omar is allowed to read the secret accounts file." Denial service is prohibited or discouraged from the normal use or management of telecommunications services. This type of attack can have a special purpose. For example, a person can block all messages to a destination (for example, the identification service). This type of attack can take another form, disrupting or disrupting the total link, either by deactivating this network or by overloading it with messages, which leads to a noticeable decline in its performance. An effective attack has properties that are exactly the opposite of a negative attack. While a negative attack is difficult to detect, but there are procedures available to prevent it from happening successfully, on the other hand, we note that it is very difficult to fully efficient attack because in order to do this it is necessary to place physical obstacles on all communications and services and on all ports. Instead, we resort to uncovering this type of attack and work to stop it completely and then restore any sabotage or delay caused by it. Since detection has a disabling effect, it can also contribute to prevention.

Received: 15 May 2020 | Revised: 5 Jun 2020| Accepted: 20 July 2020

References

1. Dr. P. K. Deshmukh, Mrs. V. R. Desale, Prof. R. A. Deshmukh, “Investigation of TPA (Third Party Auditor Role) foe Cloud Data Security”, International Journal of Scientific and Engineering Research, vo. 4,no. 2,ISSn 2229-5518, Feb 2013.
2. T. Good and M. Benaissa, “Hardware performance of eStream phase-III stream cipher candidates,” the State of the Art of Stream Ciphers Workshop (SASC’08), Lausanne, Switzerland, Feb. 13-14, 2008.
3. D. Hwang, M. Chaney, S. Karanam, N. Ton, and K. Gaj, “Comparison of FPGA-Targeted Hardware Implementations of eSTREAM Stream Cipher Candidates,” the State of the Art of Stream Ciphers Workshop (SASC’08), Lausanne, Switzerland, Feb. 13-14, 2008.
4. Atallah M J, Blanton M, Fazio N, 2009, Frikken KB, “Dynamic and efficient key management for access hierarchies” ACM Transactions on Information and System Security, pp.18:1–43.
5. D. Shrinivas, “Privacy-Preserving Public Auditing in Cloud Storage security”, International Journal of computer science and Information Technologies, vol 2, no. 6, pp. 2691-2693, ISSN: 0975-9646, 2011.
6. Wallner D, Harder E.Agee, 1999, “Rfc2627:key management for multicast:issues and architectures”, pp56.
7. Wong CK, Gouda M, Lam SS, 1998, “Secure group communications sing key graphs”In: Proceedings of theACM SIGCOMM’98 conference on applications, technologies, architectures, and protocols for computer communication, pp.68–79.
8. C wang, Sherman S. M. Chow, Q. Wang, K Ren and W. Lou, “Privacy-Preserving Public Auditing for Secure Cloud Storage”,IEEETrasaction on Computers I, vol. 62, no. 2, pp.362- 375 , February 2013.

Received: 15 May 2020 | Revised: 5 Jun 2020| Accepted: 20 July 2020