Qassim University جامعة القصيم

Search for IT221 Information security

" DIGITAL SIGNATURE "

Group names:

Ruba Alharbi. 362216679

Khozama Alsalim. 371201334

Thekra Alsuhaibani. 362206020

Ghadah Aldubayan. 371201914

Under the supervision of:

Dr.Nada Alruhaily.

TABLE OF CONTENTS

Basic concepts of digital signature

Safety:

The possibility of sending messages safely to the future of the message without exposure to any third party, and that security includes the protection and confidentiality and security of communications systems and infrastructure.

Identity:

Identifying the sender and distinguishing it from any other unique electronic identity of the sender, prevents any change or tampering with the document signed on it.

Reliability:

The document sender or recipient of the document may need to confirm or trust that the content has not been compromised or manipulated during the transmission process, and that the encryption process hides the content of the message, it cannot be changed.

Confidentiality and Privacy:

Encryption of Information Sent To protect the information from unauthorized access, it is recommended not to send sensitive information via e-mail if the user is forced to send it. This information can be stored in a separate file, then encoded using encryption software such as "Truecrypt".

Credibility:

It is used to validate the content of the file signed on it, which misses the document or message, that the messages contain information about people or sensitive content, must be digitally signed to authenticate the source of the message and know that this information is accurate. "In the sense of proving the validity of the sender and not the validity of the data".

Integration of information:

Ensure that the data has not undergone any change or manipulation since it was digitally signed.

AC (A certification authority):

Independent communications that verify identity and grants the certificate.

CSR :

Before you can order an SSL certificate, it is recommended that you generate a Certificate Signing Request (CSR) from your server or device.

SSL certificate :

An certificate consists of a public key and a private key. It uses the public key to encrypt information and uses the private key to decrypt it.

Chapter 1:

In this chapter we will cover the overview of signature in general .

1.1 Introduction

This era is characterized by rapid scientific progress in various aspects of knowledge, as well as in the number of discoveries and inventions in various aspects and applications. The technological and social revolution created by the Internet in the past 20 years has put it at the top of the list of factors affecting the lives of human beings and many of the traditional services to electronic services to meet the needs of beneficiaries and governments.

The proliferation of technology in the world and the expansion of its fields have shown us modern technology as a double-edged weapon facilitated us a lot of things such as the ability to exchange and discuss ideas electronically, but the harmful side is the emergence of electronic crimes, which tension many of users of these devices. As we know that it is one of the most important ways to maintain the integrity of information from modification and distortion and to prove its owner we have to insert the signature on it.

A **signature** is a distinctive written sign of the person who issued it, or a special mark of a particular person used to announce his name and express his consent to the work, including the name of the signatory and his family or title, and may be abbreviated to a specific symbol indicating his name, it indicates satisfaction and acceptance of the document signed with the full contents. It can be said that signing is a social phenomenon or a necessary phenomenon protected by the law, a personal mark through which the identity of the signatory can be distinguished. The signature is a signature so that it is legible and visible. It will not be so unless it is placed on the document so that its effect remains clear.

1.2 General signature characteristics:

1- The signature must be linked to the person who is the source thereof.

2- Specific and specific to the personality of the signatory distinct from other people, the signature is a safe means of identifying a person after following certain procedures.

3- The signature leads to the approval of the information contained in the document or intended by the signature owner.

4- Enhances the level of safety and privacy for online clients, especially in the field of electronic commerce.

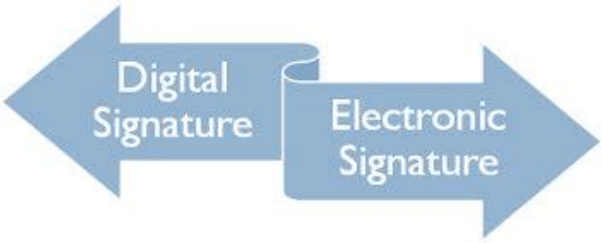
5- Linked to the information contained in the electronic document in such a way as to detect any modification.

6- Helps companies or institutions protect themselves against counterfeiting and forgery of signatures.

7- It conducts teleconferences without the presence of contractors, thus helping to develop and ensure e-commerce.

Chapter 2:

In this chapter we will discuss about electronic signature and compare it with digital signature.



2.1 Electronic Signature

The electronic signature is a procedure performed by those who want to sign an electronic document, such as contracts, agreements, orders for sale and purchase or private correspondence and others, and in light of the spread of electronic information processing systems and invasion of companies and departments and banks .Subsequently, to rely entirely on manual signature is a problem that is impossible to adapt to modern systems of management and accounting. Therefore, Science turn to the search for an alternative to the traditional signature can perform the same function on the one hand and adapt to the modern management methods on the other. This alternative can be considered as "a process of encryption consisting of symbols and numbers issued by one of the specialist and recognized internationally or legally, and these codes do to document the files of all kinds" This is known as electronic signature. As an important part of this process, the document recipient can validate the signature conclusively and immediately. The electronic signature process does not require manually signing as it does on paper signature. Instead, a person often clicks a button and then enters a secret statement to sign the file, message or other. In addition, the electronic signature ensures the integrity of the message so that there is no change in it during the transmission process. Also verify the identity of the sender and not repudiation the message because the private key cannot be with anyone else.

2.2 Types of electronic signature:

1- Signature of electronic pen:

Here the sender of the letter to write his personal signature using a special electronic pen, through a specific programs and this programs to capture the signature and ensure its validity, but this type needs devices with special specifications and is less secure and does not guarantee the authenticity of the proof.

2- Biometric electronic signature:

This signature depends on the human characteristics of the person, such as fingerprinting or tone of voice, and is confirmed by the signature of the person by entering the information to the computer and stored in an encrypted way in the memory of the computer to be matched later.

3- Electronic digital signature:

This type is which we will address in this research, is a set of numbers to be compositions in a code to be signed, and it relies on algorithms or mathematical calculation to ensure the confidentiality of information and communications in a safe way by converting it to form incomprehensible only from the owner Relationship. Where the signature of the electronic using a specific key to encrypt the document,

and then the receiver of that message to decrypt with another key to get the information sent, if the message appears after the decryption clearly and legible, the signature of the sender is true.
This digital signature is based on the use of two key technology, one public and the other private. The private key is used by the owner of the electronic signature. The public key can be used by everyone to verify the authenticity of the signature and to verify the identity and personality of the signature.

2.3 Difference between digital and electronic signature:

Digital signature is a kind of electronic signature, but distinct. A digital signature is more secure, encrypts the document and ensures that documents are not altered or manipulated. As for the electronic signature, it can be said that it is similar to the handwritten signature, but it is electronic. Customers can sign documents online with a click of the mouse or using their fingers to track a handwritten signature on a document.

The most important differences can be summarized:

- An electronic signature can be considered an electronic "fingerprint" that is encrypted and authenticated by the person who has already signed it. An electronic signature is a symbol or photograph, attached to the document indicating the signatory identification.
- The digital signature is used to secure a document. As for the electronic signature is used to verify the document.
- As for the validation, the digital signature should be through trusted certificate authorities or trust service providers. In contrast, the electronic signature does not have a specific verification process.
- In addition, considered a digital signature is more secure than an electronic signature.

Chapter 3:

In this chapter we will start cover the most

important topic in this search (digital signature)

3.1 Digital Signature

As we said earlier, digital signature is a mathematical code, consisting of symbols and numbers, which includes the accuracy and validity of contracting between parties in business transactions, companies and institutions. It can also be considered as a good alternative to manual signing, since it will in turn sign the document to prove the personal signature and ensure access to the data without modification or falsification. Also, it ensures that data is not compromised by the signature, because this type of signature is based on the principle of encryption.

There are two ways to sign encryption, either by signing using a single encryption key: in this case one key is used by the sender and the receiver.
The sender of the document encrypts it using the encryption key and then sends it to the other party that has the same encryption key. He uses this key to decode the message so that he can read it and understand its content. Therefore, no one other than the sender and receiver can understand the message.

The other way: is to sign using the public and private key: where the sender of the message sign using the private key, and then send it to receiver where he can through the public key to decryption document and understand its content. This type provides a high degree of safety. Thus it can be said ,The use of digital signature technology is evidence of the validity, integrity and completeness of electronic contracting, if any party changes any part of the document signed digitally, the process will be revealed and notice the change. If the signature is from a source or not, the person can identify himself from his personal signature the company can verify the validity, authenticity, integrity and confidentiality of the signature of the customers electronically with the company.

3.2 Here are some of the milestones in the history of digital signature technology:

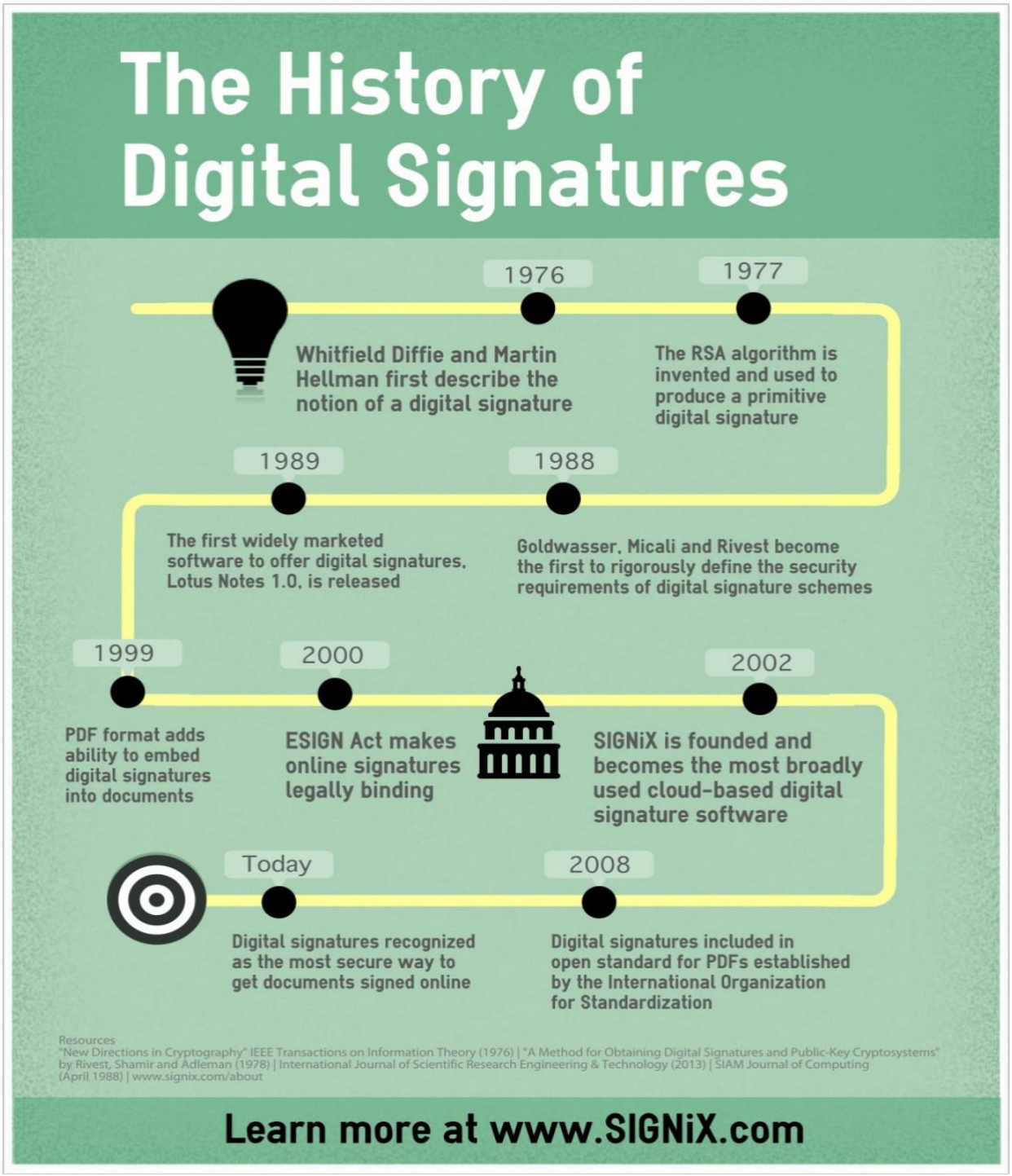


Figure 1. (www.signix.com)

3.3 Characteristics of Digital Signatures:

1- The signature must use certain symbols or marks for the sender to prove his credibility.

2- Must prove the sender and the date and time of signature.

3- It must be unique.

4- It should be easy to distinguish and prove.

5- It is more accurate and efficient than manual signature.

6- At most cannot be forgery or fraud.

7- Also, digital signatures cannot be constant.

3.4 Advantages of digital signatures:

-Authentication:

The digital signature helps to verify the authenticity of the source, and the confirmation of the sender.

-Integrity:

If a message is digitally signed, any change to the message after signing invalidates the signature. This helps data integrity.

-Not repudiation:

This means that when an entity signs some information, it cannot later deny its signatures.

-Time & cost saving :

Digital Signature can sign documents anytime and anywhere instantly without having to wait or be bored. Also, may save a great deal of money, instead of having to travel or attend to sign a contract or document. In addition, save for ink, paper, shipping / delivery… etc.

- Stamping Date :

In the digital signature is proved by the date and time which will automatically verify the sender .it does not need to be authenticated by the other party because it is a basic source.

-Workflow efficiency:
Many digital signature features help speed up the work process. It follows documents more easily and effortlessly. It also ensures better efficiency in the workflow.

-Add security:
Digital signatures guarantee the verification, authentication and legality of signatures. It also reduces the risk of duplication or changing the document itself. The security features included in digital signatures also ensure that documents do not change without permission.

-Legal validity:
Digital signatures can stand in any court of law like any other signed paper document. Because it provides authenticity and ensures that the signature is verified.

3.5 Problems and difficulties of digital signature:

- Digital signature issuers may not have the necessary license or comply with consumer protection laws.
- The cost, time and resources required of the consumer to move to a digital signature system that relies on encryption and entering into an agreement with the licensing and auditing authority, so the digital signature is slow.
- Difficulty keeping pace with the development of software and electronic technologies.
- Lack of awareness raising using digital signature.
- User does not follow the procedures required for digital signature carefully.
- Information can leak and reach the third-party causing security problems in the system.

3.6 Types of digital signature:

- **Direct digital signature**

In this type there are only two parties involved n the passing of the signed information: "sender, receiver". Assumed that receiver knows public key of sender. The sender also trust that the receiver's will not be able to change the document.

Signature may be formed by:

1- Encrypting entire message with sender's private key.

2- Encrypting hash code of message with sender's private key.

- **Arbitrated digital signature**

In this type of signature there must be a third party called "trusted arbiter". The role of the trusted arbiter is usually:

First, verify the integrity of the signed message or data.

Second, verifying receipt and the passing on of the signed document to its intended final destination.

3.7 Does a digital signature achieve a paper signature function?

The digital signature is the identity of the person who signed on document. Thus, it is able to achieve paper signature function.

The paper signature is known a drawing made by a person. It can be considered an art rather than a science. You can easily fake it or imitate it. A digital signature is a small encrypted part of the data added to the e-mail, such as mail or documents. It can be said that science is not art. It is therefore difficult to falsify, as it provides more security and credibility for higher documents. Some may think that a digital signature is only a copy of a paper signature made by a scanner. This is a misconception. As we said earlier, encrypted data is attached to the e-mails to ensure that they are not modified or manipulated.

It can be said that the most important difference between them, that in the paper signature, the presence of the person is required to sign, and may result in an increase in cost and loss of time. As someone who travels only to sign on his paper and prove his identity. Or as someone waiting for a manager or boss to sign a contract or document. Instead, the digital signature can be done with this task as little as possible. For this reason, mostly prefer digital signature on paper.

Chapter 4:

In this chapter we will show the digital signature

and its impact on our lives

4.1 Areas of use digital signature:

- The signing of letters for applications of financial and commercial transactions and various transactions is a legal signature.
- Encrypt messages to a person or group of people, check the sender's identity and verify his signature.
- Signing of checks and individual transactions with the sales and purchases through the international Internet.
- Make and sign cash transfers.
- Issuing certificates that serve the citizens, such as banks, universities, institutes, real estate documentation, selling and buying sites, are documented with certificates and legal certification.

4.2 Human and financial resources needed to support digital signature

The technology in the digital signature is the safety of electronic contracts that require digital signatures which requires a strong resources and financial resources to maintain the confidentiality of the information and ensure the correctness of the information. It lays back layers to protect them from breaking or hacking, so as not to lead to hacking problems or theft and plagiarism.

The rules for digitizing these technological resources are established and built for several factors:

1. Algorithms, code.

2. Implementation.

3- key.

Algorithms:

There are three algorithms:

- Produces private key, contains secret key for user or private key.
- Output signature and give private key.
- Validate the key then accept or reject.

Implementation:

Algorithms are Implemented and applied in a correct manner so it will not lead to severe problems and cannot be broken .it must be recognizable so it will not be difficult to decode.

The key:

Create a key for the user which is linked to a document or identity, issued by a responsible party and it will become the identity of the user. It must be saved and remain confidential to prevent theft of copying it.

Therefore, secure algorithms must be developed, expertise programmers should be assigned to prevent any breakthroughs. The password or key for this code, algorithms, must be kept with a trusted person. Therefoe the information is kept high secure and cannot be for the benefit of the sharing.

Human resources:

It requires programmers with experience, honesty, and sincerity. The source of the digital signature must be checked to have licenses in consumer protection law, so that the company is protected from any breaches. The white hat hackers needed to detect the gaps in the company firewall to save company form any falsifying of its digital signature.

Financial resources:

Setting up a high quality digital signature tools. Setting a salary for programmers responsible of the company digital signature .setting up a special regular maintenance of digital signature.The financial loss that the company puts in all of the above will limit the damage and breakthroughs that may face the company. A singing a high quality security will come with a high cost to the company but it will save the company information. The financial resources that we put to save the company information will help us to minimize the loss of information security.

Chapter 5:

In this chapter we will discuss how related IT with digital signature specially in informatics crimes.

5.1 Informatics crimes

is an illegal act or activity carried out by a group of people called hackers.In order to achieve specific goals of their own as stealing private information or funds or achieving other political and social objectives.

5.2 Types of informatics crimes:

1- Crimes targeting individuals or personal cybercrime:

Include impersonation Electronically, by stealing an email, a person's password, or private information about access to various social networks.

2- Crimes targets property:

This type of crime will target governments, private institutions or individuals, it focuses on destroying some information about the victim whose information has been controlled.

3- Crimes targeting governments:

Are crimes of a political nature, which are applied to the electronic systems of governments to destabilize and destroy their various systems and programs.

4- Crimes of fraud:

Aimed at fraudulently deceiving many people financially, or with the aim of taking private information through fraud.

5.3 Objectives of information crimes:

-To access information illegally, to steal or access certain information, or to delete or modify it in a way that achieves the goal of the hacker.

-Access to confidential information of some technology users, such as government agencies, banks, institutions and individuals, and then blackmail them.

5.4 The most important ways of preventing informatics crimes:

- Take caution and not believe all of the ads and make sure their credibility by the famous search engines.

- Avoid opening an anonymous e-mail and even speeding it down.

- Put the password code in accordance with the good specifications that make it difficult to hack it, from these specifications: to contain more than eight characters, to be varied letters, symbols, languages, etc.

- Take care of personal information and personal computer by setting appropriate protection programs.

5.5 Digital certificate

For get powerful and secure network we will need to install many services, such as: certificate service this service is based on SSL (Secure Sockets Layer).

Definition of digital certificate:

A digital document that contains a set of information that leads to the verification of the identity of the person or organization or website and encrypts the information contained in the server through the so-called SSL (Secure Sockets Layer). We can compare the digital certificate with a passport or digital credentials when communicating between the server and the client. When the client wants to send confidential or sensitive information, the Internet browser automatically accesses a server to verify the identity of the entity Which wants to send information to it and the following ensures a secure connection channel.

5.6 The contents of the digital certificate:

The digital certificate contains many information, but the most important of these information is the following:

- The name of the owner of the digital certificate (whether a person or a company).

- Serial number of digital certificate plus expiration date.

- A copy of owner's the public key the digital certificate.

- Electronic signature of the authorities that issued the digital certificate.

5.7 How to obtain a digital certificate?

Must be Request an electronic signature of the digital certificate from a trusted & specialized in digital certifications, that called: CSR (Request Signing Certificate).

5.8 Public key and Private key:

When requesting an electronic certificate (CSR), the server issues two keys: one public and the other private.

The public key:

Is included in the digital certificate and is available to all and is used to encrypt messages sent to the owner of the digital certificate.

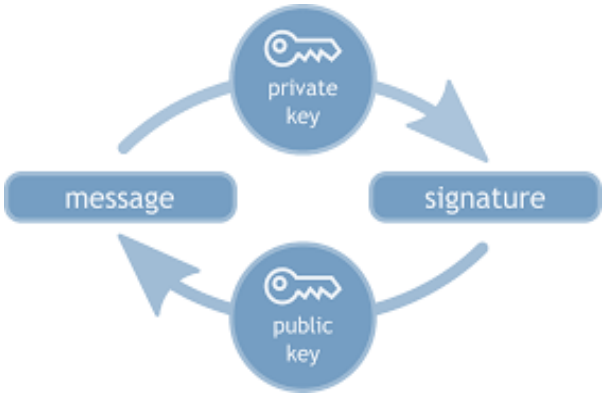
The private key:

Is stored in the computer local and is used to decrypt the received messages and to make a secure connection via an encrypted communication channel. The browser web sends a request to the server web server to verify and link the private key and the certificate.

the server is the only one that has access to the private key and is able to decrypt the information sent over the encrypted communication channel.

Chapter 6:

In this chapter we will cover on some types algorithms used in digital signature.



6.1 Cryptography

Cryptography is the science of keeping information by transforming it into a secure form. This process, called encryption, has been used for centuries to prevent hand written messages from being read by unintended recipients. Today, cryptography is used to protect digital data.

6.2 Symmetric encryption (conventional encryption)

This encryption depends on the key secret used, since the person who has the key can decrypt and read the text.

The symmetric encryption contains five components:

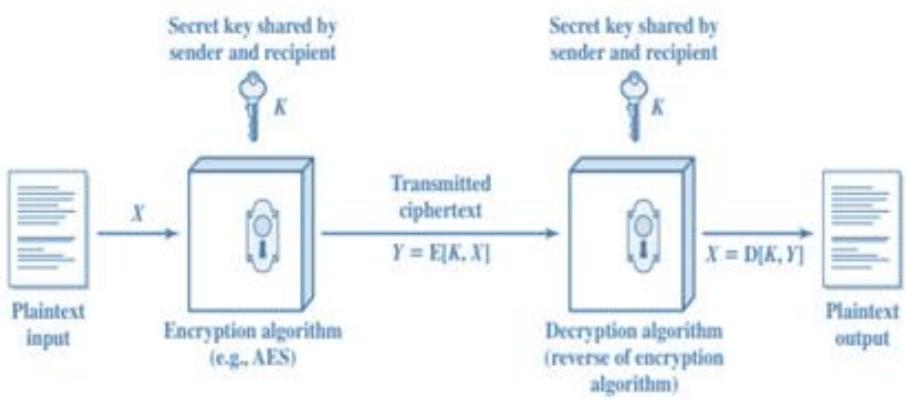


Figure 2. Simplified Model of Symmetric Encryption (Stallings,2011)

Plain text: Is the original message or input data for the algorithm as input.

Encryption algorithm: The encryption algorithm transformations on plain text, e.g. AES, DES, triple DES

Secret key:

Cipher text : Is an encrypted message.

Decryption algorithm: The Cipher text and the same as the secret key produces the original plain text.

There are two requirements to configure secure symmetric encryption:

1. We need a very powerful algorithm so that the opponent is unable to decrypt encrypted text or pause the key
2. It is necessary that the sender and receiver have the same secret key in a safe way

6.3 Asymmetric encryption (public key)

The same importance of symmetric encryption is also important asymmetric encryption.

This encryption depends on two keys, public key and private key, as the public key for encrypting messages and private key for decryption.

The public key is sent to all the people either in private in which the owner maintains the message.

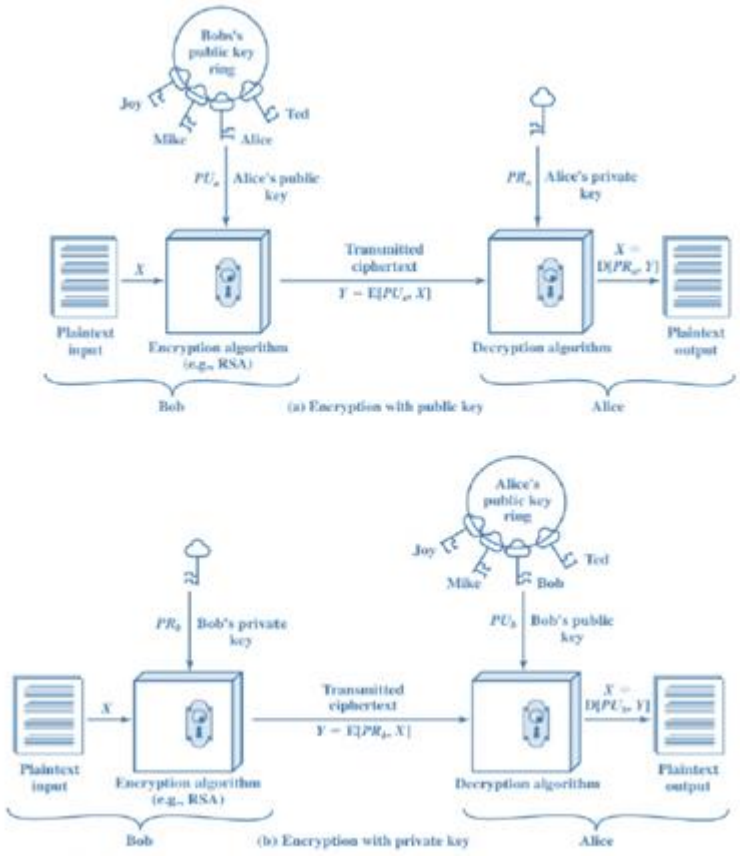


Figure3. Public-Key Cryptography(Stallings,2011)

Plain text: Is the original message or input data for the algorithm as input

Encryption algorithm: The encryption algorithm transformations on plain text, e.g. RSA, DSA, Elgamal.

Public and private key: Is a pair of keys that are selected so that one is for encryption and the other is for decryption

Cipher text: Is an encrypted message , it will produce two different keys and two different cipher text .

Decryption algorithm: This algorithm takes encrypted text and matches the key and produces the original text.

6.4 Types of Symmetric encryption algorithm :

1- The Data Encryption Standard(DES).

2-Advanced Encryption Standard(AES).

6.5 Types of Asymmetric encryption algorithm:

1- Rivest–Shamir–Adleman Encryption(RSA).

2- ElGamal Encryption .

Algorithm	Asymmetric Algorithm	Symmetric Algorithm	
Factors	RSA	Data Encryption Standard(DES)	AES
Encryption	Slower	Moderate	Faster
Decryption	Slower	Moderate	Faster
Security	Least Secure	Not Secure Enough	Excellent Secured
Deposit of keys	Needed	Needed	Needed
Inherent Vulnerabilities	Brute Forced and Oracle attack	Brute Forced , Linear and differential cryptanalysis attack	Brute Forced Attack
Key Used	Different key used for Encrypt and Decrypt	Same key used for Encrypt and Decrypt	Same key used for Encrypt and Decrypt
Rounds	1	16	10/12/14

Stimulation Speed	Faster	Faster	Faster
Trojan Horse	No	No	Not proved
Hardware & Software Implementation	Not Efficient	Better in hardware than in software	Faster
Ciphering & Deciphering Algorithm	Same	Different	Different

Table1. Comparison between Symmetric and Asymmetric Algorithm (Mahajan and Sachdeva,2013)

6.6 Comparison between Asymmetric encryption type:

6.6.1 Rivest–Shamir–Adleman(RSA) Encryption:

One of the oldest and most popular algorithms used for public-key encoding is RSA.The algorithm is named after its creator Ron Rivest, Adi Shamir and Leonard Adleman, who issued it in 1977 while working at MIT. (Stailing,2014). It depends on the integer factorization problem.

Key generation

1. Choose two different large random prime numbers p and q.
2. Calculate the $n = pq$.
3. Calculate the totient $\varphi(n) = (p-1) \times (q-1)$
4. Select for public exponent an integer e such that 1 < e < φ(n) and $gcd(\varphi(n), e) = 1$
5. Calculate for the private exponent a value for d such that d = e^{-1} mod φ(n)
6. Public Key = [e, n].
7. Private Key = [d, n].

Encryption

We give our public key numbers to the person that wants to send us their message. They will encrypt the message with the formula$C = m^e mod n$. C is our encrypted Message

Decryption

In order to decrypt the message we need our private key n and d .

we don't give anybody our private key.

We use the formula:$M = c^d mod n$

Numerical Example

Here is an example of RSA encryption and decryption. (Stailing,2014)

Choose two random prime numbers.

1. p=61 and q=53 Compute n=p*q
2. n=61*53=3233
3. Compute the totient $\varphi(n) = (p-1) \times (q-1)$
4. φ(n) = (61 − 1) × (53 − 1)=3120
5. Choose e>1 coprime to 3120
6. e=17
7. Choose d to satisfy $d=e^{-1}$ mod φ(n)
8. d=2735.
9. 17 * 2753=46801=1+15 * 3120.

The **public key** is (n=3233,e=17). For a padded message m the encryption function $C = m^e mod n a^{xA}$becomes:$c = m^{17} mod 3233$.

The **private key** is (n=3233,d=2753). The decryption function $M = c^d mod n$ becomes:$M = c^{2735} mod 3233$

For example, to encrypt m=123 , we calculate$C = 123^{17} mod 3233 = 855 a^{xA}$

To decrypt c=855, we calculate

$M = 855^{2753} \text{mod} 3233 = 123$

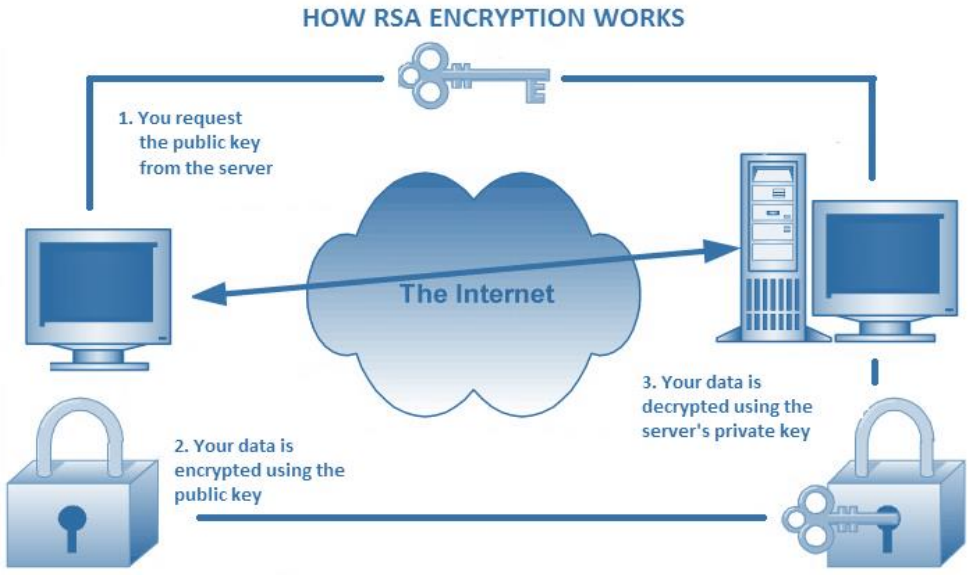


Figure4. RSA Encryption Work (Stailing,2014)

6.6.2 ElGamal Encryption:

ElGamal Algorithm is a public key encryption scheme submitted in 1984 by Tather Elgamal(ELGamal, 1985). It depends on the Discrete Logarithm problem.

Key Generation

A sender A generates the public/secret key pair by

1. choosing large prime p and generator g of the multiplicative Group $Z^* p$of the integers modulo p.
2. choosing a random integer a, $1 \leq a \leq p - 2$, and compute $g^a mod p$.
3. Then A's Public key is (p, g, g^a) and A's secret key is a .

Encryption

B encrypts a text m to A

1. uses A's public key (p, g, g^a). 4.calculate

2. appear the text as integers m in the range $\{0, 1, \ldots, p-1\}$.

3. choose a random integer k,$1 \leq k, 1 \leq k \leq p-2$.

4. calculate $\gamma = gkmodp$ and $\delta = m * (ga)k$.

5. send encrypted text $c = (\gamma, \delta)$ to A.

Decryption

A receives cipher text m from B

1. Use secret key a to calculate $(\gamma^{p-1-a})modp$

   Note: $\gamma^{p-1-a} = \gamma^{-a} = a^{-ak}$

2.Recover m by calculating $(\gamma^{-a}) * \delta modp$.

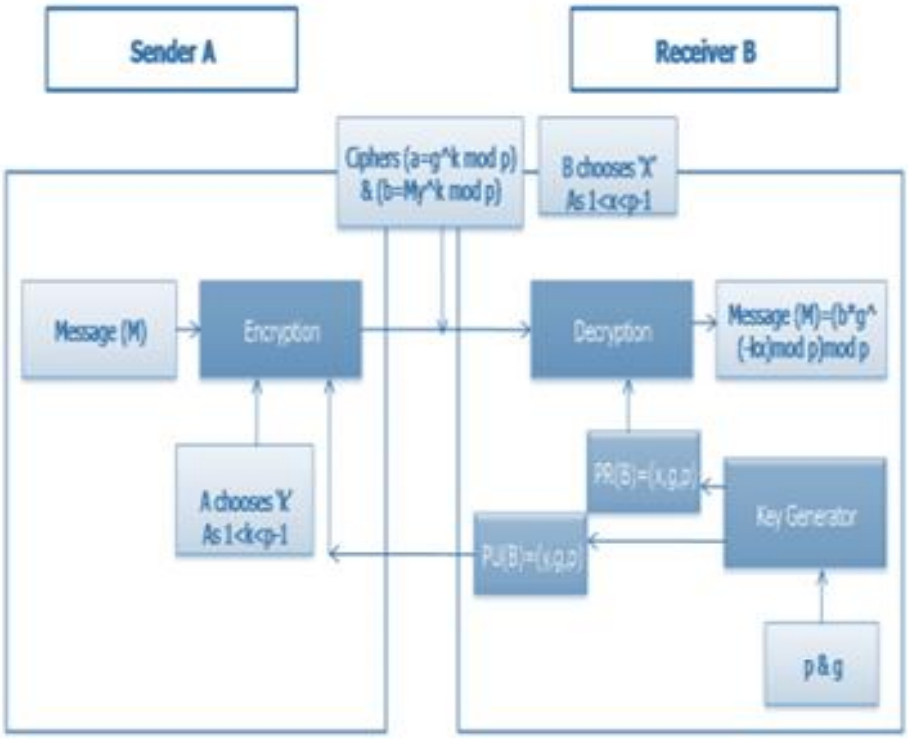


Figure 5. ELgamal Algorithm (Singh,Kumar, 2012)

Numerical Example

This is a numerical example shows Elgamal Algorithm (ELGamal, 1985).

Alice selects her public key (17, 6, 7):

• Prime p = 17

• Generator g = 6

• secret key part a = 5

• Public key part $gamodp$ = 6 5 mod 17 = 7

Bob encodes his message m = 13:

• He selectes a random k = 10

• He computes $\gamma = gkmodp$ = 610 mod 17= 15

• He encodes $\delta = m * (ga)k$ = (13 * 710) mod 17=9

Bob sends γ = 15 and δ = 9 to Alice.

Alice receives γ = 15 and δ = 9 from Bob.

• Her public key is (p, g, g^a) = (17,6,7)

• Her secret key is a = 5

Alice now decipher the message using her secret key:

• decoding factor

$(\gamma^{-a}) * \delta modp$ = 15−5 mod 17 = 1511 mod 17 = 9

• Decryption: (δ ∗ 9) mod p = (9 ∗ 9) mod 17 = 13

Alice has now decipher the message and received: 13

Characteristics	RSA Approach	ElGamal Algorithm
Number of private keys	1	1
Number of public Keys/ Group key	1	1 group key
Hard problems being solved	Large number factorization	Discrete Logarithm
Possible attacks	Chosen cipher text attack , Timing Attacks, Mathematical Attacks, , Brute Force	Plain Text Attack
Performance analysis	Signature generation and verification is very fast	More Secure
Communication Group	NO	NO

Table 2. Comparison of RSA, DSA and AlGamal (Bansal, Sharma and Mishra,2017)

Chapter 7:

Conclusion

In Conclusion, we have reached the agreement of the advantages of technology in this era covering all our lives in all respects, reached us at home or also inside the bedroom and even outside it became everything through technology happens

Those of us now do not have a device or there is no Internet in the place or a modern device bought soon We not only have devices to facilitate communication, technology has become obsessed with some we buy annually or monthly or even daily It has become a passion for many of us, using it as a public interest and also a door to profit, and a door to steal some of the hacker.

It is easy to communicate with the outside world or the virtual world. Everything is available between our hands and close to us so we can accomplish better and more quickly.

But signing up for electronic fields may be difficult, so the digital signature is found to support this problem Technology has advanced in many fields, including what we talked about, digital signature.

Help us prove the world's identity in technology and in all its fields. It is proof of a letter, certificate or document in the name of the publisher or sender. And shall be authenticated or issued by a reliable authority until all doubts in the letter have been removed as certified Not modified or fabricated.

If digital signature is a good choice for companies, founders or even individuals to validate messages And also make the user move easier to complete transactions outside the scope of work.

But what should be avoided is plagiarism, privacy and targeting of messages for sabotage, destruction or theft There is no non-penetrable chip, but the protection of messages should be increased by encryption, such as the use of a digital signature for protection, increased security within the company's circuit, and more ways to protect not just digital signature.

Chapter 8:

References

https://www.techwalla.com/articles/difference-between-direct-arbitrated-digital-signature
https://techdifferences.com/difference-between-digital-signature-and-electronic-signature.html
https://www.signix.com/blog/bid/108804/infographic-the-history-of-digital-signature-technology
https://medium.com/@KeithKrach/the-top-5-advantages-of-digital-signatures-aed3ebfdbabc
https://www.ijser.org/paper/Elgamals-Algorithm-in-Cryptography.html
https://don.p4ge.me/rsa-explained-simply/programming
http://www.startimes.com/f.aspx?t=16851952
https://books.google.com.sa/books?id=dfhQDwAAQBAJ&pg=PA366&dq=صفات+التوقيع+الرقمي&hl=ar&sa=X&ved=0ahUKEwiYx5Wd7fDgAhXF2OAKHd00AhcQ6AEIKDAA#v=onepage&q=صفات%٢٠التوقيع%٢٠الرقمي&f=false
https://books.google.com.sa/books?id=yxW5DAAAQBAJ&pg=PT92&dq=التوقيع+الرقمي&hl=ar&sa=X&ved=0ahUKEwi_v8zq8vDgAhUQfxoKHSp3BHAQ6AEIMjAC#v=onepage&q=التوقيع%٢٠الرقمي&f=false
https://books.google.com.sa/books?id=2c4nDwAAQBAJ&pg=PT58&dq=انواع+التوقيع+الرقمي&hl=ar&sa=X&ved=0ahUKEwjkkJbhifHgAhWK1-AKHTMrCxQQ6AEILTAB#v=onepage&q=انواع%٢٠التوقيع%٢٠الرقمي&f=false
https://www.mohamah.net/law/%D8%B7%D8%B1%D9%82-%D8%A7%D9%84%D8%AD%D9%85%D8%A7%D9%8A%D8%A9-%D9%88-%D8%A7%D9%84%D9%88%D9%82%D8%A7%D9%8A%D8%A9-%D9%85%D9%86-%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7%D9%84%D8%A5%D9%84%D9%83/
https://weziwezi.com/%D8%A8%D8%AD%D8%AB-%D8%B9%D9%86-%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA%D9%8A%D8%A9/
https://pdfs.semanticscholar.org/1749/6c347e05ef2681473a0648ae11696796829d.pdf
https://pdfs.semanticscholar.org/55f0/7920235c979c2e0517e8c51af33db6cea720.pdf
https://books.google.com/books/about/%D8%A3%D8%B3%D8%A7%D8%B3%D9%8A%D8%A7%D8%AA_%D8%A3%D9%85%D9%86_%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA.html?hl=ar&id=do5cnQAACAAJ
https://books.google.com/books/about/%D8%A3%D8%B3%D8%A7%D8%B3%D9%8A%D8%A7%D8%AA_%D8%A7%D9%84%D8%AA%D8%AC%D8%A7%D8%B1%D8%A9_%D8%A7%D9%84%D8%A3%D9%84%D9%83.html?hl=ar&id=yxW5DAAAQBAJ