Survey Paper: Cryptography Is The Science Of Information Security

Mohammed AbuTaha
College of Administrative Sciences and Informatics *m_abutaha@ppu.edu*
Palestine Polytechnic University
Hebron, Palestine

Mousa Farajallah
College of Engineering and Technology *mousa_math@ppu.edu*
Palestine Polytechnic University
Hebron, Palestine

Radwan Tahboub
College of Engineering and Technology *radwant@ppu.edu*
Palestine Polytechnic University
Hebron, Palestine

Mohammad Odeh
IT and Communications Dept *mhmdodeh@qou.edu*
Al-Quds Open University
Hebron, Palestine

Abstract

Cryptography in the past was used in keeping military information, diplomatic correspondence secure and in protecting the national security. However, the use was limited. Nowadays, the range of cryptography applications have been expanded a lot in the modern area after the development of communication means; cryptography is essentially required to ensure that data are protected against penetrations and to prevent espionage. Also, cryptography is a powerful mean in securing e-commerce. Cryptography is used to ensure that the contents of a message are confidentiality transmitted and would not be altered. Confidentiality means nobody can understand the received message except the one who has the decipher key, and data cannot be changed means the original information would not be changed or modified; this is done when the sender includes a cryptographic operation called a hash function in the original message. A hash function is a mathematical representation of the information, when any information arrives at its receiver; the receiver calculates the value of this hash function. If the receiver's hash function value is equivalent to the sender's, the integrity of the message is assured .

Keyword: Symmetric Encryption, A Symmetric Encryption ,Hash Algorithm, Caesar Table.

1. INTRODUCTION

Nowadays, cryptography plays a major role in protecting the information of technology applications. Information security is an important issue, for some applications. Have the top priority such as e-commerce, e-banking, e-mail, medical databases, and so many more, all of them require the exchange of private information. For example, let us consider a person named Alice a sender who wants to send a data message which has a length of m characters to a receiver called Bob. Alice uses an unsecure communication channel. Which could be a telephone line , computer network, or any other channel. If the message contains secret data, they could be intercepted and read by hackers. Also they may change or modify the message during its transmission in such a way that Bob would not be able to discover the change. In this survey a various ways of encryption is viewed and have been compared ,a lot of examples have been provided .

1.1 Cryptography Goals

By using cryptography many goals can be achieved, These goals can be either all achieved at the same time in one application, or only one of them, These goals are:

1. Confidentiality: it is the most important goal, that ensures that nobody can understand the received message except the one who has the decipher key.

2. Authentication: it is the process of proving the identity, that assures the communicating entity is the one that it claimed to be, This means that the user or the system can prove their own identities to other parties who don't have personal knowledge of their identities. (The primary form of host to host authentication on the Internet today is name-based or address-based; and both of them are notoriously weak).

3. Data Integrity: its ensures that the received message has not been altered in any way from its original form, This can be achieved by using hashing at both sides the sender and the recipient in order to create a unique message digest and compare it with the one that received.
4. Non-Repudiation: it is mechanism used to prove that the sender really sent this message, ,and the message was received by the specified party, so the recipient cannot claim that the message was not sent [2].

5. Access Control: it is the process of preventing an unauthorized use of resources. This goal controls who can have access to the resources, If one can access, under which restrictions and conditions the access can be occurred, and what is the permission level of a given access.

1.2 Basic Terminology of Cryptography

Computers are used by millions of people for many purposes. such as banking, shopping, military, student records, etc…. . Privacy is a critical issue in many of these applications, how are we need to make sure that an unauthorized parties cannot read or modify messages.

Cryptography is the transformation of readable and understandable data into a form which cannot be understood in order to secure data. cryptography refers exactly to the methodology of concealing the content of messages, the word cryptography comes from the Greek word "Kryptos", that means hidden, and "graphikos" which means writing [3].

The information that we need to hide, is called **plaintext** (P), It's the original text, It could be in a form of characters, numerical data, executable programs, pictures, or any other kind of information, The plaintext for example is the first draft of a message in the sender before encryption, or it is the text at the receiver after decryption.

The data that will be transmitted is called **cipher text** (C), it's a term refers to the string of "*meaningless"* data, or unclear text that nobody must understand, except the recipients. it is the data that will be transmitted Exactly through network, Many algorithms are used to transform plaintext into cipher text [4].

Cipher is the algorithm that is used to transform plaintext to cipher text, This method is called encryption or enciphers (encode), in other words, it's a mechanism of converting readable and understandable data into "*meaningless*" data, and it is represented as follows:

$$C = E_{(K)}(P) \tag{1}$$

Where $E_{(K)}$ is the encryption algorithm using key k.

The opposite of cipher mechanism is called **decipher (decode)** that is the algorithm which recovers the cipher text, this method is called decryption, in other words it's the mechanism of converting "*meaningless"* data into readable data.

$$P = D_{(K^{-1})}(C) \tag{2}$$

The Key is an input to the encryption algorithm, and this value must be independent of the plaintext, This input is used to transform the plaintext into cipher text, so different keys will yield different cipher text, In the decipher side, the inverse of the key will be used inside the algorithm instead of the key.

Computer security it's a generic term for a collection of tools designed to protect any data from hackers, theft, corruption, or natural disaster while allowing these data to be available to the users at the same time. One example of these tools is the A-vast antivirus program [1].

Network security refers to any activity designed to protect the usability, integrity, reliability, and safety of data during their transmission on a network, Network security deals with hardware and software, The activity can be one of the following anti-virus and anti-spyware, firewall, Intrusion prevention systems, and Virtual Private Networks [4].

Internet Security is measures and procedures used to protect data during their transmission over a collection of interconnected networks .while **information security** is about how to prevent attacks, and to detect attacks on information-based systems [2].

Cryptanalysis (code breaking) is the study of principles and methods of deciphering cipher text without knowing the key, typically this includes finding and guessing the secrete key, It's a complex process involving statistical analysis, analytical reasoning, math tools and pattern-finding, The field of both cryptography and cryptanalysis is called **cryptology** [4,15].
Symmetric encryption refers to the process of converting plaintext into cipher text at the sender with the same key that will be used to retrieve plaintext from cipher text at the recipient. while **asymmetric encryption** refers to the process of converting plaintext into cipher text at the sender with different key that will be used to retrieve plaintext from cipher text at the recipient [15].

Passive attacks mean that the attackers or the unauthorized parties just monitoring on the traffic or on the communication between the sender and the recipient, but not attempting to breach or shut down a service, This kind of attacks is very hard to discover, since the unauthorized party doesn't leave any traces. On the other hand **active attacks** mean that the attackers are actively attempting to cause harm to the network or the data. The attackers are not just monitoring on the traffic, but they also attempt to breach or shut down the service [4,15].

Authentication is the process of determining whether someone is the same person who really is, such as login and password in login pages while authorization is the process of ensuring that this person has the ability to do something [4, 9, 15].

Brute force is the attacker who is trying all of the possible keys that may be used in either decrypt or encrypt information [15].

1.3 A Brief History of Cryptography

The encryption process is as old as writing itself, Through this short historical combo, the most important stations in the progress of data encryption will be reviewed. It is believed that the first texts used or contained any encryption techniques were known 4000 years ago at the Veterans Egyptian where the hieroglyphic inscriptions on the tomb of the nobleman Khnumhotep II, They were written with a number of unusual symbols to confuse or obscure the meaning of the inscriptions [6].

2000 years ago, the Greek knew cylinder device called Scytale, which was the sender's part very similar to the recipient part, where a narrow strip of parchment or leather, was wounded around the Scytale and the message was written across it, so if anyone tries to read the text he will find meaningless letters, The only one that can read this text is the one who has the Scytale, This technique is similar to the transposition technique which will be later discussed in symmetric encryption section [5].
The Arab role in the data encryption, was since ancient times, Through the analysis of the text of the holy Qur'an text, Muslim scholars were able to invent frequency analysis technique for breaking monoalphabetic substitution ciphers about 1200 years ago, by Sheikh AL-Kindi in his famous book "Risalah fi Istikhraj al-Mu'amma (Manuscript for the Deciphering Cryptographic Messages)", which it was

the most advanced in cryptography since that time, until the World ware two, Figure 1 shows the first page of AL-Kindi's book, After AL-Kindi's invention, all cipher text became vulnerable to this cryptanalytic technique, until the development of the polyalphabetic cipher by Leone Battista Alberti, who is known as "The Father of Western Cryptology" in 1465 [6].

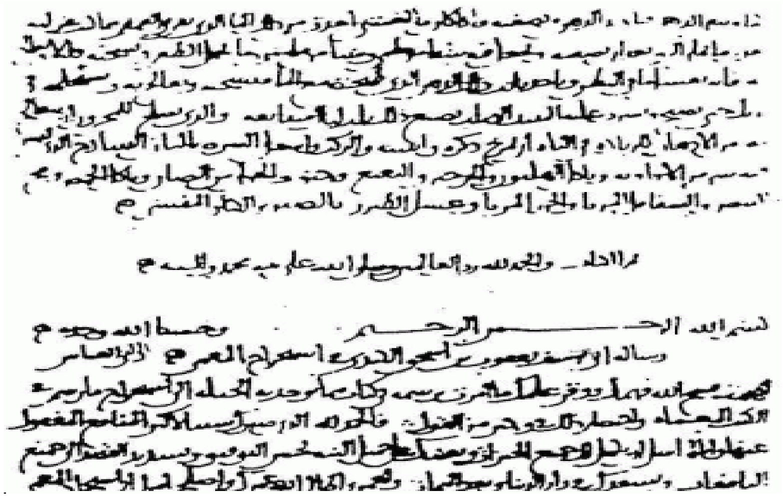


FIGURE.1: The first page of al-Kindi's manuscript On Deciphering Cryptographic Messages

The next step was in 1518 by Trithemius, a German monk, who wrote a table of Twenty-six column and Twenty-six row. Each row duplicate the above row but shifted by one letter.

In 1585, Blaise de Vigenere developed a Trithemius table by changing the way that the keywords system works. One of his used techniques is the plaintext as its own key.

Forty-three years later, a Frenchman named Antoine Rossignol helped his army to defeat the Huguenots, by deciphering a captured message. After that victory, Antoine was deciphering messages for the benefit of the French government many times. He used two lists to solve his ciphers: "one in which the plain elements were in alphabetical order and the code elements randomized, and one to facilitate decoding in which the code elements stood in alphabetical or numerical order while their plain equivalents were disarranged" [7].

The wheel cipher is a cylinder composed of Twenty six cylindrical piece of wood, The alphabetical letters inscribed randomly on each piece the [8].
The development in data encryption has begun to accelerate after the discovery of the telegraph, simply sending messages by the telegraph is not secure; therefore they had to provide means of data encryption before transmission.

In 1854, Charles Wheatstone and Lyon Playfair invented the Playfair system, which was consisted from 5X5 rectangle key, while the plaintext message divided into adjacent pairs, This system will be discussed later.

Before 1883, the encrypt ion process often depended on hiding of algorithm to protect data, Of course, This is not practical, but the first major advances in cryptography were made in the year 1883 by Kerkhoff by developing a set of principles which is now known as Kerkhoff principle, The major principle is, hidding the key of algorithm instead of hiding the algorithm itself [5].

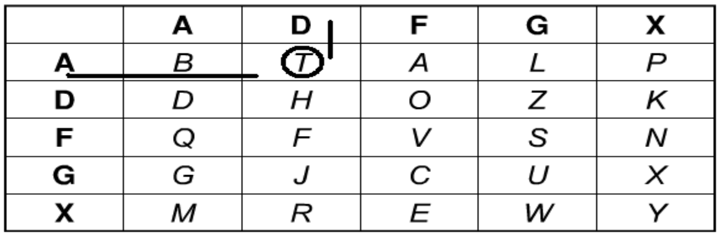
Kerkhoff Principles [9]

1. Ciphertext should be unbreakable.
2. The cryptosystem should be convenient for the correspondent.
3. The key should be easily remembered and changeable.

4. The Ciphertext should be transmitted by the telegraph.
5. The cipher apparatus should be easily portable,
6. The cipher machine should be relatively easy to use.

In 1915, two Dutch navy officers invented the rotor machine; which is a combination of electrical and mechanical systems. The simple view of rotor machine is an electrical system with twenty-six switches pressed by the plaintext, These switches attached by a wire to a random contact letter on the output, for example if the plaintext letter is pressed, the wiring is placed inside a rotor, and then rotated with a gear every time a letter was pressed. So while pressing ***A*** the first time might generate character ***D***, the next time it might generate character ***S*** [10].

In 1918, the german army during the world war one, used ADFGVX cipher system, which consisted from a table, the first row and first column was the key while the data entry was randomly replaced by the plaintext with pair of characters of text at the top of the corresponding row and corresponding column, The following figure shows the replaced character T with pair AD Figure 2 explain ADFGVC cipher system [11].



	A	D	F	G	X
A	*B*	*T*	*A*	*L*	*P*
D	*D*	*H*	*O*	*Z*	*K*
F	*Q*	*F*	*V*	*S*	*N*
G	*G*	*J*	*C*	*U*	*X*
X	*M*	*R*	*E*	*W*	*Y*

FIGURE 2 : Example of Using ADFGVX cipher system.

Lester Hill is one of the few scientists who had concluded that mathematics inevitably necessary for the success of encryption, and the encryption remained the same until 1941 when Adrian Albert Benefited from Hill theorem and built an encryption system based on mathematics [12].

In 1948, Shannon published "A Communications Theory of Secrecy Systems", In this paper Shannon's analysis demonstrates several important features of the statistical nature of language that make nearly the solution of all previous ciphers very straight forward, One of the most important result in this paper is that Shannon developed a measure for cryptographic strength called the "unicity distance" [14].

During a collaboration between Whitfield Diffie and Martin Hellman in 1976 , the Diffie-Hellman key agreement was invented, The method was based on the selected three variables at the sender ***(x, a, P)*** and generating of ***s***, then sending ***(s, a, P)*** to the recipient, the recipient chooses ***y*** and uses ***y*** with ***(a, P)*** to generate ***r*** and sends ***r*** to the sender, the sender use ***r*** with ***(x, P)*** to generate the public key, The recipient also uses ***s*** with ***(y, P)*** to generate the same public key, Figure 3 explains this idea [15].

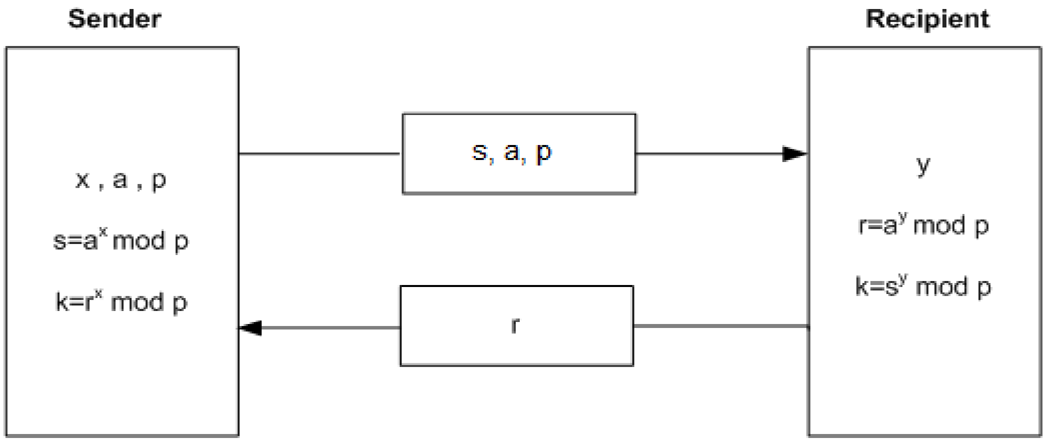


FIGURE .3 : Diffie-Hellman key generation

After Diffie-Hellman approach, the cryptography was divided into symmetric and asymmetric cryptography, and then many techniques and methods were developed. The next section is about the symmetric and asymmetric encryption [16].

2. SYMMETRIC AND ASYMMETRIC ENCRYPTION

Encryption is the strongest and the safest way in securing data. Certainly, it is the most common one. Encryption systems are divided into two major types or forms, symmetric and asymmetric.
Symmetric encryption is known as secret key or single key, The receiver uses the same key which the sender uses to encrypt the data to decrypt the message,. This system was the only system used before discovering and developing the public key., A safe way of data transfer must be used to moving the secret key between the sender and the receiver in symmetric encryption. Figure 4 shows how the system works. Symmetric encryption occurs either by substitution transposition technique, or by a mixture of both. Substitution maps each plaintext element into cipher text element, but transposition transposes the positions of plaintext elements.

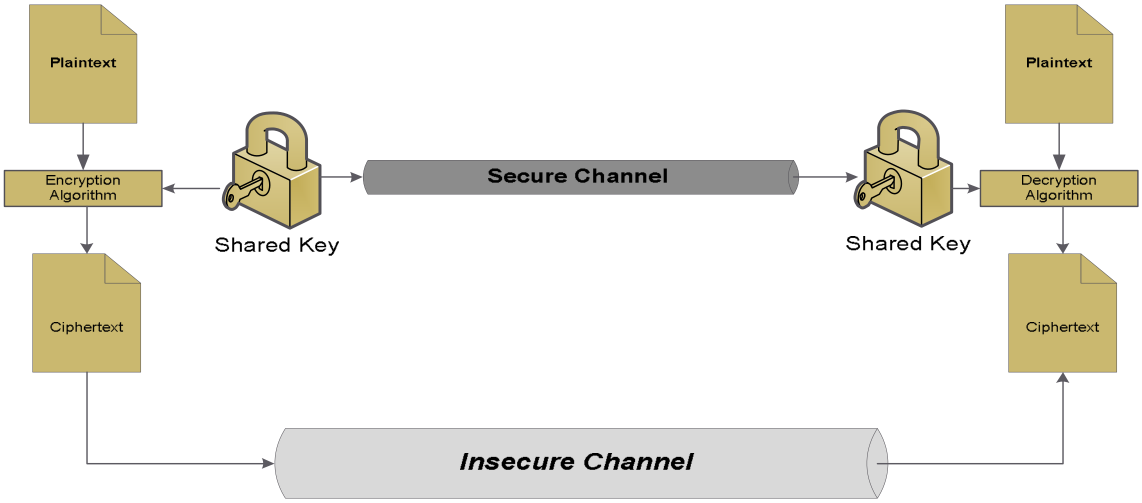


FIGURE .4 : Simplified model of conventional encryption

Plaintext	Encryption Process	Cipher text
p➔15	(15+12) mod 26	1➔ b
a➔ 0	(0+12) mod 26	12➔m
l ➔11	(11+12) mod 26	23➔x
e➔ 4	(4+12) mod 26	16➔q
s➔18	(18+12) mod 26	4➔ e
t➔19	(19+12) mod 26	5➔ f
i➔ 8	(8+12) mod 26	20➔u
n➔13	(13+12) mod 26	25➔z
e➔ 4	(4+12) mod 26	16➔q

The common simplified cipher algorithm which assigns each character of plaintext into numerical value is called Caesar cipher, , its sums the key value to the numerical value of plaintext character, and then assigns the rest of the division by modular value into cipher text character, where the modular value is the max numerical value plus one [17], The mathematical model of Caesar cipher is:

At encryption side: $$E_n(x) = (x + n)\ mod\ p \qquad (3)$$

At decryption side: $$E_n(x) = (x - n)\ mod\ p \qquad (4)$$

Where $\boldsymbol{x}$ is the plaintext character and $\boldsymbol{x}$ is shift value, the following example illustrates Caesar cipher model:

Example 1:
Let the plaintext message is "Palestine" and the key value=12 , and use the simplest symmetric encryption algorithm ,which called "Caesar cipher", the Caesar table will be:

Table .1: Caesar Table

a	b	C	d	e	f	g	h	i	j	k	L	m	n	o	p	q	r	s	T	u	v	W	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

The cipher text which arrive to the receiver is “bmxqefuzq“, and the cipher text is entered into decryption process in the receiver to decrypt the text as follow:

Cipher text	Decryption Process	Plaintext
b➔ 1	(1 - 12) mod 26	15➔ p
m➔12	(12 - 12) mod 26	0➔ a
x➔ 23	(23 - 12) mod 26	11➔ l
q➔ 16	(16 - 12) mod 26	4➔ e
e➔ 4	(4 - 12) mod 26	18➔ s
f➔ 5	(5 - 12) mod 26	19➔ t
u➔ 20	(20 - 12) mod 26	8➔ i
z➔ 25	(25 - 12) mod 26	13➔ n
q➔ 16	(16 - 12) mod 26	4➔ e

an advanced rail fence technique which is more sophisticated technique on symmetric encryption , uses the original plaintext to write it in row-by-row, and read the cipher text column-by-column, but at decryption side write the cipher text column-by-column and retrieve the plaintext by reading the message row-by-row, the mathematical model of advanced rail fence when $(\boldsymbol{key} = d_1 d_2 d_3 \cdots d_n)$, where $(d_3 > d_1 > d_n > d_2)$:

$$\begin{array}{cccccc} \boldsymbol{key} & d_1 & d_2 & d_3 & \cdots & d_n \\ & p_1 & p_2 & p_3 & \cdots & p_n \\ \hline \end{array} \qquad (5)$$

$$\begin{array}{llllll} \boldsymbol{key} & d_1 & d_2 & d_3 & \cdots & d_n \\ & C_{2\times l/n+1} & C_1 & C_{3\times l/n+1} & \cdots & C_{l/n+1} \\ & C_{2\times l/n+2} & C_2 & C_{3\times l/n+2} & \cdots & C_{l/n+2} \\ & \vdots & \vdots & \vdots & \vdots & \vdots \\ & C_{3\times l/n} & C_{l/n} & C_{4\times l/n} & \cdots & C_{2\times l/n} \end{array} \tag{6}$$

Where $d_1$is the smallest digit among digits of $\boldsymbol{key}$ that consist from n digits, l represent number of characters in plaintext message, p_i is the i^{th} character of plaintext message and C_i is the i^{th} character of cipher text output.

Example 2:

To understand and accommodate advance rail fence technique, let us consider $(\boldsymbol{key} = 5236417)$, plaintext (p)"AES is a block cipher intended to replace DES for commercial application":

Using equation (5), the encryption message:

Key	5	2	3	6	4	1	7
Plaintext:	A	e	s	i	s	a	b
	L	o	c	k	c	i	p
	H	e	r	i	n	t	e
	N	d	e	d	t	o	r
	E	p	l	a	c	e	d
	E	s	f	o	r	c	O
	M	m	e	r	c	i	A
	L	a	p	p	l	i	C
	A	t	i	o	n	x	X

Output: Aitoeciixeoedpsmatscrelfepiscntcrclnalhneemlaikidaorpobperdoacx

Using equation (6), the decryption message (plaintext):

Key	5	2	3	6	4	1	7
Plaintext:	A	e	s	i	s	a	B
	i	o	c	k	c	i	P
	h	e	r	i	n	t	E
	n	d	e	d	t	o	R
	e	p	l	a	c	e	D
	e	s	f	o	r	c	O
	m	m	e	r	c	i	A
	l	a	p	p	l	i	C
	a	t	i	o	n	x	X

Output: Aesisablockcipherintendedtoreplacedesforcommercialapplication

From previous examples, the plaintext is translated into different cipher text and then transferred throw unsecured channel to the receiver, while the secrete key which is been used in encryption process will be transferred throw secured channel, At the receiver side the inverse of the secret key or/and the inverse of encryption process are used to decrypt the cipher text and to retrieve the original plaintext, Caesar mechanism is the core for all encryption model, from easy to very complicated one, in other word, the encryption process needs key to convert the plaintext into cipher text, but at the receiver the inverse of processes will retrieve the original plaintext.

Symmetric encryption has many advantages over asymmetric. Firstly, it is faster since it doesn't consume much time in data encryption and decryption. Secondly, it is easier than asymmetric encryption in secret key generation. However, it has some disadvantages, for example key distribution and sharing of the secret key between the sender and the receiver, also symmetric key encryption incompleteness, since some application like authentication can't be fully implemented by only using symmetric encryption [18].

In 1976 Diffie and Helman invented new encryption technique called public key encryption or asymmetric encryption; Asymmetric encryption is the opposite of symmetric encryption in safety, since it doesn't require sharing the secret key between the sender and the receiver. And this is the main difference between symmetric and asymmetric encryption, the sender has the public key of the receiver. Because the receiver has his own secret key which is extremely difficult or impossible to know through the public key, no shared key is needed; the receiver is responsible for establishing his private and public key, and the receiver sends the public key to all senders by any channel he needs, even unsecured channels to send his public key, asymmetric key can use either the public or secret key to encrypt the data. Also it can use any of the keys in decryption, asymmetric encryption can be used to implement the authentication and non-repudiation security services, and also it can be used for digital signature and other application that never be implemented using symmetric encryption. Figure.5 shows how the system works.

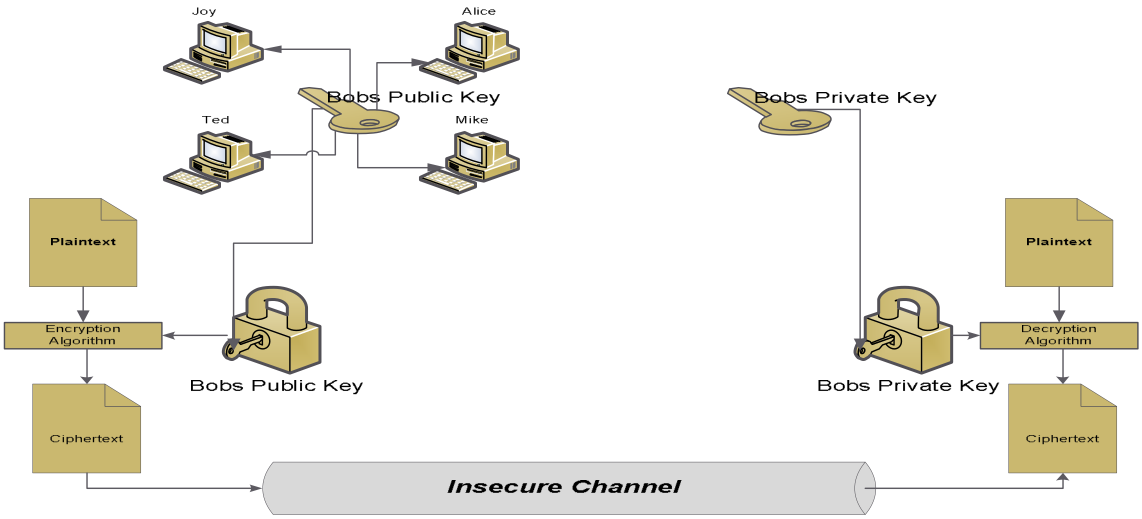


FIGURE 5 : Simplified model of asymmetric encryption

Asymmetric encryption is slower and very complicated in calculations than symmetric encryption . Therefore, asymmetric encryption deals with plaintext as a group of numbers which are manipulated in mathematics, while the plaintext in symmetric encryption deal as group of symbols and characters, the encryption process may permute these symbols, or may substitute one symbol by another.

So the nature of the data determines the system of encryption type. And every system has its own uses. For example, asymmetric encryption may be used in authentication or in sending secret key for decryption.

To understand asymmetric encryption, lets us take RSA model which is an example on asymmetric encryption, RSA model main steps:

RSA Model Steps:

- Each user generates a public/private key pair by selecting two large primes at random p, q.
- Computing modular value $n = p \times q$
- Calculating the Euler's function $\phi(n) = (p-1) \times (q-1)$
- Selecting at randomly the public encryption key e, where$1 < e < \phi(n)$, and e is prime relative to the$\phi(n)$.

- Solving the following equation to find private decryption key d, $e \times d = 1 \, mod \; \phi(n)$, and $0 \leq d \leq n$.
- Publishing their public encryption key: $P_K = (e, n)$.
- Keeping secret private decryption key: $P_R = (d, n)$.
- At the encryption side the sender uses encryption mathematical equation $C = P^e \; mod \; n$.
- At the decryption side the receiver uses decryption mathematical equation $P = C^d \; mod \; n$.

Example 3:

Let a part of the plaintext message be "Palestine", then the RSA key generation process is:

- Select two prime numbers: p=23 & q=17
- Computing $n = p \times q = 23 \; x \; 17 = 391$
- Computing $\phi(n) = (p-1) \times (q-1) = 22 \; x \; 16 = 352$
- Selecting $e: gcd(e, 352) = 1; \; choose \; e = 7$
- Determining $d: d \times e = 1 \; mod \; 352 \; and \; d < 352$ Value is $d = 151$ since $151 x7 = 1057 = 352 \times 3 + 1$
- Publishing public key$P_K = (7{,}391)$.
- Keeping private key secrete$P_R = (151{,}391)$.

The encryption process and decryption process then is applied to previously calculated parameters as follow:

Plaintext			Encryption Process
p	➔	15	$15^7 \; mod \; 391 = 195$
a	➔	00	$00^7 \; mod \; 391 = 000$
l	➔	11	$11^7 \; mod \; 391 = 122$
e	➔	04	$04^7 \; mod \; 391 = 353$
s	➔	18	$18^7 \; mod \; 391 = 052$
t	➔	19	$19^7 \; mod \; 391 = 383$
i	➔	08	$08^7 \; mod \; 391 = 219$
n	➔	03	$13^7 \; mod \; 391 = 055$
e	➔	04	$04^7 \; mod \; 391 = 353$

The cipher text will arrive the receiver, and at the receiver the cipher text will be entered into decryption process to decrypt the text as follow:

Decryption Process	Plaintext		
$195^{151} \; mod \; 391 = 015$	015	➔	p
$000^{151} \; mod \; 391 = 000$	000	➔	a
$122^{151} \; mod \; 391 = 011$	011	➔	l
$353^{151} \; mod \; 391 = 004$	004	➔	e
$052^{151} \; mod \; 391 = 018$	018	➔	s
$383^{151} \; mod \; 391 = 019$	019	➔	t
$219^{151} \; mod \; 391 = 008$	008	➔	i
$055^{151} \; mod \; 391 = 003$	003	➔	n
$353^{151} \; mod \; 391 = 004$	004	➔	e

The mathematical model for symmetric and asymmetric encryption consists of key, encryption and decryption algorithm and powerful secured channel for transmitting the secrete key or any channel for transmitting the public key from the sender to the receiver, the mathematical model similar to equations (1 - 2):

At encryption side: $\boldsymbol{C = E_K(P)}$

At decryption side: $\boldsymbol{P = D_K(C)}$

Where C is the cipher text to be sent, E is the encryption algorithm, P is the plaintext, D is the decryption algorithm, and K is the key used inside the encryption and/or decryption process.

3. RESULTS AND COMPARISON

When it comes to encryption, the latest isn't necessarily the best. You should always use the encryption algorithm that is right for the job and has been extensively publicly analyzed and tested, something the cryptographic community won't have had the chance to do with a brand new algorithm. Let's have a look at some of the most widely-used algorithms. For most people, encryption means taking plaintext and converting it to cipher text using the same key, or secret, to encrypt and decrypt the text. This is symmetric encryption and it is comparatively fast compared to other types of encryption such as asymmetric encryption. The most widely-used algorithm used in symmetric key cryptography is AES (Advanced Encryption Standard). It comprises three block ciphers, AES-128, AES-192 and AES-256, each of which is deemed sufficient to protect government classified information up to the SECRET level with TOP SECRET information requiring either 192 or 256 key lengths.

The main disadvantage of symmetric key cryptography is that all parties involved have to exchange the key used to encrypt the data before they can decrypt it. This requirement to securely distribute and manage large numbers of keys means most cryptographic services also make use of other types of encryption algorithms. Secure MIME (S/MIME) for example uses an asymmetric algorithm - public/private key algorithm - for non-repudiation and a symmetric algorithm for efficient privacy and data protection.

Asymmetric algorithms use two interdependent keys, one to encrypt the data, and the other to decrypt it. This interdependency provides a number of different features, the most important probably being digital signatures which are used amongst other things to guarantee that a message was created by a particular entity or authenticate remote systems or users. The RSA (Rivest, Shamir and Adleman) asymmetric algorithm is widely used in electronic commerce protocols such as SSL, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations. As RSA is much slower than symmetric encryption, what typically happens is that data is encrypted with a symmetric algorithm and then the comparatively short symmetric key is encrypted using RSA. This allows the key necessary to decrypt the data to be securely sent to other parties along with the symmetrically-encrypted data.

4. SUMMARY

Cryptography is used to ensure that the contents of a message are confidentiality transmitted and would not be altered. Confidentiality means nobody can understand the received message except the one that has the decipher key, and "data cannot be changed" means the original information would not be changed or modified; this is done when the sender includes a cryptographic operation called a hash function in the original message. A hash function is a mathematical representation of the information, when information arrives at its receiver; the receiver calculates the value of this hash function. If the receiver's hash function value is equivalent to the sender's, the integrity of the message is assured [15].in this survey paper we describe and compare between symmetric and asymmetric encryption technique ,provide many example to show the differences .

5. REFERENCES

[1] J. Badeau.,: " The Genius of Arab Civilization ", Second Edition. MIT Press,(1983), USA.

[2] M .Chapple., M Solomon,: " Information Security Illuminated " First Edition. Jones and Bartlett Publishers, (2005), USA.

[3] J.R Childs: " General Solution of the ADFGVX Cipher System ". Aegean Park Press, ,(2000), USA.

[4] D.Delfs., and K. Helmut.,: " Introduction To Cryptography: Principles and applications ", Second Edition. Springer Science & Business Media, (2007), Germany.

[5] G .Dieter: " Computer Security ", Second Edition. John Wiley & Sons, , (2005), UK.

[6] A. Forouzan.,: " Cryptography and Network Security ", First Edition. McGraw-Hill, (2007), USA.

[7] R Hamamreh., M Farajallah., " Design of a Robust Cryptosystem Algorithm for Non-Invertible Matrices Based on Hill Cipher ". International Journal of Computer Science and Network Security, (2009): Vol (9), pp: 12-21.

[8] J Hoffstein., et al, " An Introduction to Mathematical Cryptography ", First Edition. Springer Science & Business Media, (2008):, Germany.

[9] H.Kenneth, " Elementary Number Theory and Its Applications " Third Edition. Addison-Wesley, (1992): Germany.

[10] M.Lucas, " Thomas Jefferson wheel cipher ", Monticello Research Department, Thomas Jefferson Foundation, Charlottesville, (1995):, VA.

[11] S .Maret," Cryptography Basics PKI ", First Edition. Dimension Data SA, ., (1999):, Switzerland.

[12] E.Ralph., F Weierud" Naval Enigma: M4 and Its Rotors ". Crypologia, ,. (1987):, Vol(11),pp:235-244.

[13] W .Reinhard., " Cryptology Unlocked ", Translation Edition By Angelika Shafir. John Wiley & Sons, (2007):, UK.

[14] H. Rodríguez, et al,: " Cryptographic Algorithms on Reconfigurable Hardware ", First Edition. Springer, (2006), USA.

[15] D.Salomon" Data Privacy and Security " First Edition. Springer-Verlag New York, ., (2003):, Inc. USA.

[16] C .Shannon,. " Communication Theory of Secrecy Systems ". Bell Syst, (1949):, Tech. J., Vol (28), pp: 656-715.

[17] W .Stallings, " Cryptography and network security, Principles and practices ", Fourth Edition. Pearson Prentice Hall, (2006):, USA.

[16] K .Thomas, : " The Myth Of The Skytale ". Taylor & Francis, (1998), Vol (33), pp: 244-260.