SURVEY ON CRYPTOGRAPHY ALGORITHMS: A COMPARATIVE APPROACH

P. B. Zirra[1], G. M. Wajiga[2], S. Boukari[3]
[1]Department of Mathematical Sciences, Adamawa State University, Mubi, Nigeria
Email: zirrapeter@yahoo.com
[2]Department of Mathematics and Computer Science, Modibbo Adama University of Technology, Yola, Nigeria
Email: gwajiga@gmail.com
[3]Mathematical Sciences Programme, Abubakar Tafawa Balewa University Bauchi, Nigeria
Email: bsouley2001@yahoo.com

Abstract
Cryptography has been used in the military, diplomatic services and in protecting the national secret. However, the use was limited in many ways. Nowadays, the range of cryptography applications is much wider in scope and its acceptance. Cryptography helps protect data and helps provide a secure means of communication over otherwise insecure channels. Also, cryptography is a powerful means in securing e-applications. In this survey various ways of encryption algorithms are reviewed and compared. Also a lot of examples have been provided.
The examples show that symmetric encryption algorithm has faster performance compared to asymmetric encryption algorithm.

Keyword: Asymmetric Encryption, Symmetric Encryption, Cryptosystem, Cryptography, Cryptanalysis.

INTRODUCTION

The growth of the Internet has made cryptography more important and critical in electronic application systems. Unless the system is able to provide some mechanisms to ensure security services, the system will have problems to be accepted. More reliable cryptosystems have to be proposed and, cryptography is being an essential part of today's information systems. Cryptography is the science of using mathematics to encrypt and decrypt data. It enables us to store or transmit sensitive information across insecure networks like the Internet. So that it cannot be read by anyone except the intended recipient (Agnew *et al.*, 1995). Cryptography is one of the technological means to provide security to data being transmitted on information and communications systems. A cryptography system which provides two complementing functions, encryption and decryption is called cryptosystem. Cryptosystems are used to achieve several goals such as (Schneier, 1996):

a) **Confidentiality** is the most important goal, that ensures that nobody can understand the message except the one who has the decipher key.
b) **Authentication** is the process of providing proof of identity of the sender to the recipient; so that the recipient can be assured that the person sending the information is who and what he or she claims 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).
c) **Data integrity** is a service which addresses the unauthorized alteration of data. To assure data

integrity, one must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution. This can be achieved by using hashing at both sides by the sender and the recipient in order to create a unique message digest and compare it with the one that is received.

d) **Non-repudiation** is a 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 (Chapple and Solomon, 2005). This is achieved by using a digital signature mechanism.

e) **Access control** is the process of preventing an unauthorized use of resources. This goal controls access to the resources. If one can access, under which restrictions and conditions the access can occur, and what is the permission level of a given access.

CRYPTOGRAPHY BASICS

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 needed to make sure that 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 originated from two Greek words "Kryptos", which means secrete, and "graphos" which means writing (Childs, 2000), hence it literally means *secret writing*.

In cryptographic terminology, the message is called plaintext or cleartext, 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 owner of a plaintext emanating from sender is called a receiver/recipient. The originator of a plaintext emanating to a receiver is called a sender.

Data can be encrypted using an encryption algorithm and transmitted in an encrypted state. Encoding the contents of the message in such a way that hides its contents from outsiders is called encryption.

The encrypted message is called ciphertext, it's a term refers to the string of *"meaningless"* data, or unclear text that nobody must understand, except the recipients.

Data can later be decrypted by the intended party using a decryption algorithm. The process of retrieving the plaintext from the ciphertext is called decryption.

Encryption and decryption usually make use of a key, and the coding method is such that decryption can be performed only by knowing the proper key (Seth and Mishra, 2011). 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.

There are two classes of key-based encryption algorithms namely symmetric (or secret-key) and asymmetric (or public-key) algorithms. The difference is that

symmetric algorithms use the same key for encryption and decryption (or the decryption key is easily derived from the encryption key), whereas asymmetric algorithms use a different key for encryption and decryption, and the decryption key cannot be derived from the encryption key (Salomon, 2003).

A cryptography system which provides two complementing functions, encryption and decryption is called cryptosystem.

Symmetric algorithms can be divided into stream ciphers and block ciphers. Stream ciphers encrypt a single bit of plaintext at a time, whereas block ciphers take a number of bits (typically 64 bits in modern ciphers), and encrypt them as a single unit.

Asymmetric ciphers (also called public-key algorithms) permit the encryption key to be public (it can even be published to a web site), allowing anyone to encrypt with the key, whereas only the proper recipient (who knows the decryption key) can decrypt the message. The encryption key is also called the public key and the decryption key the private key. The security provided by these ciphers is based on keeping the private key secret.

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, mathematical tools and pattern-finding. The field of both cryptography and cryptanalysis is called cryptology (Salomon, 2003; Delfs and Helmut, 2007).

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 Salomon, 2003; Delfs and Helmut, 2007).

Brute force is the attacker who is trying all of the possible keys that may be used in either decrypt or encrypt information (Salomon, 2003).

A Brief History of Cryptography

Cryptography has a long and fascinating history (Kahn, 1996). 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 (Forouzan, 2007).

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 (Dieter, 2005).

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 war II, Fig.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 (Forouzan, 2007).

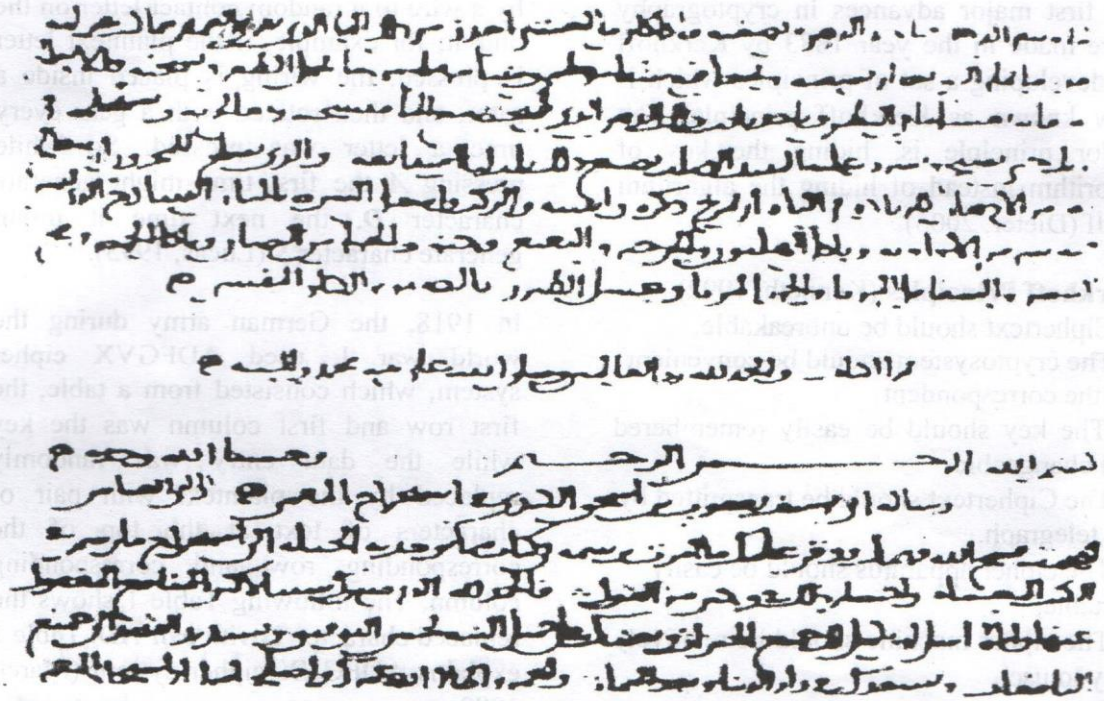

Fig. 1: The first page of al-Kindi's manuscript On Deciphering Cryptographic Messages

The next step was in 1518 by Trithemius, a German monk, who wrote a table of Twenty-six column and twenty-six rows. Each row duplicates 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" (Hamamreh and Farajallah, 2009).

The wheel cipher is a cylinder composed of twenty six cylindrical piece of wood. The alphabetical letters inscribed randomly on each piece of wood (Hoffstein, 2008).

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, hiding the key of algorithm instead of hiding the algorithm itself (Dieter, 2005).

Kerkhoff Principles (Kenneth, 1992)
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 26 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*** (Lucas, 1995).

In 1918, the German army during the world war I, 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 Table 1 shows the replaced character **T** with pair **AD**. Table 1 explains ADFGVX cipher system (Maret, 1999).

Table 1: Example of Using ADFGX cipher system

	A	D	F	G	X
A	B		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

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 (Ralph and Weierud, 1987).

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" (Rodríguez *et al.*, 2006).

During collaboration between Whitfield Diffie and Martin Hellman in 1976, the Diffie-Hellman key agreement was invented (Diffie and Hellman, 1976). 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, Fig. 2 explains this idea (Salomon, 2003).

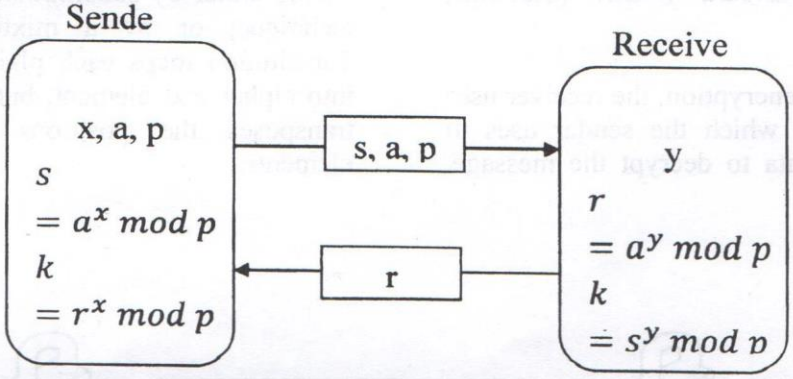

Fig. .2 : Diffie-Hellman key generation scenarios

Although the authors had no practical realization of a public-key encryption scheme at the time, the idea was clear and it generated extensive interest and activity in the cryptographic community.

In 1978 (Rivest *et al.* 1978) discovered the first practical public-key encryption and signature scheme, now referred to as RSA. The RSA scheme is based on another hard mathematical problem, the intractability of factoring large integers. This application of a hard mathematical problem to cryptography revitalized efforts to find more efficient methods to factor.

The 1980s saw major advances in this area but none which rendered the RSA system insecure. Another class of powerful and practical public-key schemes was found by El Gamal (1985) in 1985. These are also based on the discrete logarithm problem. One of the most significant contributions provided by public-key cryptography is the digital signature. In 1991 the first international standard for digital signatures (ISO/IEC 9796) was adopted. It is based on the RSA public-key scheme. In 1994 the U.S. Government adopted the Digital Signature Standard (National Institute of Standards and Technology, 1994), a mechanism based on the El Gamal public key scheme.

After Diffie-Hellman approach, the search for new public-key schemes, improvements to existing cryptographic mechanisms, and proofs of security continues at a rapid pace. Various standards and infrastructures involving cryptography are being put in place. Security products are being developed to address the security needs of an information intensive society.

CRYPTOGRAPHY ALGORITHMS

Encryption is the strongest and the safest way in securing data. Certainly, it is the most common one. Encryption algorithms are divided into two major types or forms, symmetric and asymmetric (Agnew *et al.*, 1995; Stinson, 2006).

SYMMETRIC KEY ALGORITHMS

(Thomas, 1998)

Symmetric encryption (also called secret-key or single-key) is divided into stream ciphers and block ciphers. Stream ciphers

encrypt a single bit of plaintext at a time, whereas block ciphers take a number of bits (typically 64 bits in modern ciphers), and encrypt them as a single unit. The most popular secret key encryption algorithms are Data Encryption Standard (DES), Triple DES, and Advance Encryption Standard (AES) (Stallings, 2006).

In Symmetric encryption, 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. Fig. 3 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.

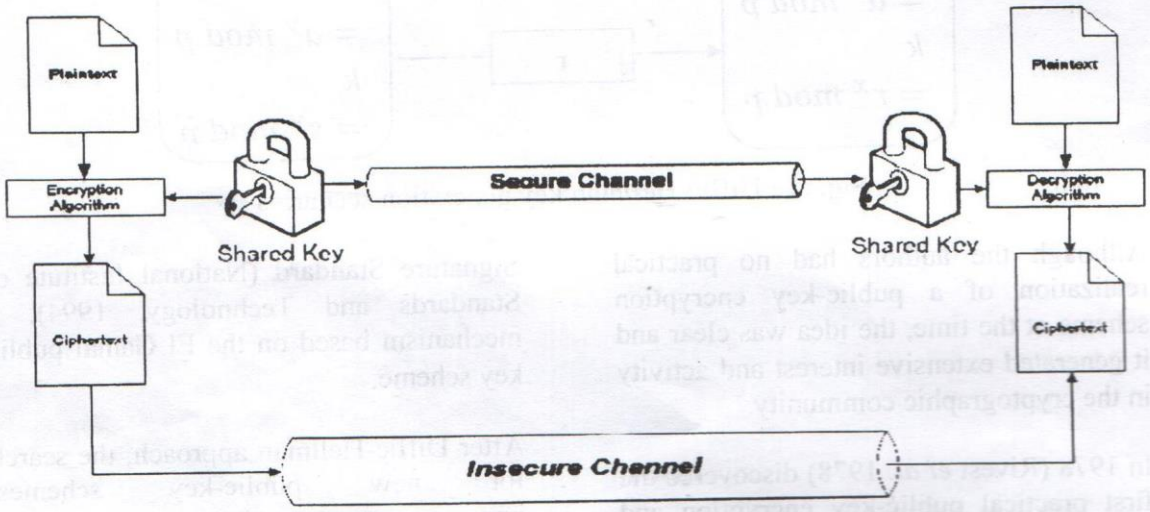

Fig. 3 : Simplified model of conventional encryption

Plaintext	Encryption process	Ciphertext
a = 00	(00 + 7) mod 26	07 = H
d = 03	(03 + 7) mod 26	10 = K
a = 00	(00 + 7) mod 26	07 = H
m = 12	(12 + 7) mod 26	19 = T
a = 00	(00 + 7) mod 26	07 = H
w = 22	(22 + 7) mod 26	03 = D
a = 00	(00 + 7) mod 26	07 =H

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 (Stallings, 2006), The mathematical model of Caesar cipher is:

At encryption side: $$E_n(x) = (x + n) mod\ p \quad (1)$$

At decryption side: $$D_n(x) = (x - n) mod\ p \quad (2)$$

Where x is the plaintext character and n is shift value, the following example illustrates Caesar cipher model:

Illustrative Example 1

Let the plaintext message is "adamawa" and the key value = 7, and use the simplest symmetric encryption algorithm, which called "Caesar cipher", the Caesar table will be:

Table 2: Caesar Cipher

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
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

The cipher text which arrives to the receiver is "HKHTHDH", and the cipher text is entered into decryption process in the receiver to decrypt the text as follow:

Ciphertext	Encryption process	Plaintext
H = 07	(07 - 7) mod 26	00 = a
K = 10	(10 - 7) mod 26	03 = d
H = 07	(07 - 7) mod 26	00 = a
T = 19	(19 - 7) mod 26	12 = m
H = 07	(07 - 7) mod 26	00 = a
D = 03	(03 - 7) mod 26	22 = w
H = 07	(07 - 7) mod 26	00 = a

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 $key = (d_1, d_2, d_3, \dots, d_n)$, where $(d_3 > d_1 > d_n > d_2)$

$$key = \begin{cases} d_1 & d_2 & d_3 & \dots & d_n \\ p_1 & p_2 & p_3 & \dots & p_n \end{cases} \quad (3)$$

$$\text{Key} = \begin{cases} d_1 & d_2 & d_3 & \dots & d_n \\ C_{2xl/n+1} & C_1 & C_{3xl/n+1} & \dots & C_{l/n+1} \\ C_{2xl/n+2} & C_2 & C_{3xl/n+2} & \dots & C_{l/n+2} \\ \vdots & \vdots & \vdots & & \vdots \\ C_{3xl/n} & C_{l/n} & C_{4xl/n} & \dots & C_{2xl/n} \end{cases} \quad (4)$$

Where d_1 is the smallest digit among digits of *Key* that consist from n digits l, represent number of characters in plaintext message p_l, is the character of plaintext

message and C_l is the l^{th}character of cipher text output.

Illustrative Example 2:
To understand and accommodate advance rail fence technique, let us consider ($key = 5236417$), plaintext (P) "AES is a block cipher intended to replace DES for commercial application"

Using equation (3), 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	l	i	o	n	x	x

Output: Aitoeciixeoedpsmatscrclfepiscntcrclnalhneemlaikidaorpobperdoacx

Using equation (4), the decryption 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	l	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 (Thomas, 1998).

PUBLIC KEY ALGORITHMS (Thomas, 1998)

In 1976 Diffie and Helman invented new encryption technique called public-key algorithms or asymmetric encryption. Asymmetric algorithm 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 algorithm, 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 applications that can never be implemented using symmetric encryption. Fig. 4 shows how the system works.

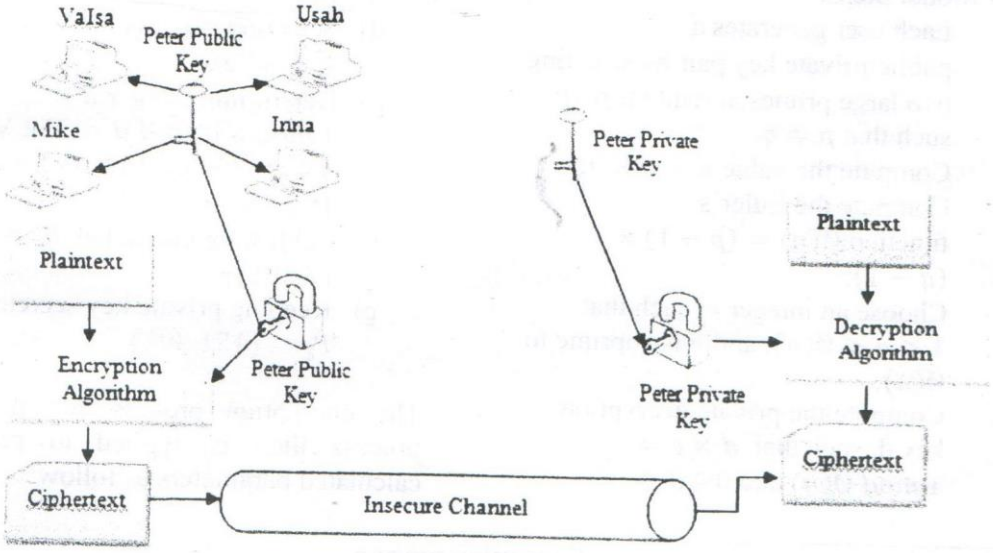

Fig. 4 : Simplified model of asymmetric encryption

The most popular public key encryption algorithms are RSA (Rivest, Shamir, and Adleman) and ELGamal cryptosystem (Schneier, 1996). 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 of asymmetric encryption and the most popular public key encryption algorithm that is still the most used one. RSA involves two keys: public key and private key (a key is a constant number later used in the encryption formula.) The public key can be known to everyone and is used to encrypt messages. These messages can only be decrypted by use of the private key. In other words, anybody can encrypt a message, but only the holder of a private key can actually decrypt the message and read it.

RSA Model Steps:

i. Each user generates a public/private key pair by selecting two large primes at random p, q; such that $p \neq q$;
ii. Compute the value $n = p \times q$;
iii. Compute the Euler's function $\emptyset(n) = (p-1) \times (q-1)$;
iv. Choose an integer e, such that $1 < e < \emptyset(n)$, and e is coprime to $\emptyset(n)$;
v. Compute the private decryption key d, such that $d \times e = 1 \ mod \ \emptyset(n)$ and $0 \leq d \leq n$;
vi. Users publish their public encryption key: $P_k = (e, n)$;
vii. Users Keep their secret private decryption key: $P_k = (d, n)$;
viii. The sender uses encryption mathematical equation $C = P^e \ mod \ n$ to encrypt the message;
ix. The receiver uses decryption mathematical equation $P = C^d \ mod \ n$ to decrypt the message;

Illustrative Example 3:

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

a) Select two prime numbers: $p = 23, q = 17$;
b) Computing $n = p \times q = 23 \times 17 = 39$;
c) Computing $\emptyset(n) = (p-1) \times (q-1) = 22 \times 16 = 352$;
d) Selecting e, $\gcd(e, 352) = 1$: choose $e = 7$;
e) Determining d: $e \ x \ d = 1 \ mod \ 352 \ and \ d < 352$ Value is $d = 151$ since $151 \times 7 = 1057 = 352 \times 3 + 1$;
f) Publishing public key $P_k = (7,391)$;
g) Keeping private key secrete $P_k = (151,391)$.

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

Plaintext	Encryption process
a = 00	$00^7 \ mod \ 391 = 00$
d = 03	$03^7 \ mod \ 391 = 232$
a = 00	$00^7 \ mod \ 391 = 00$
m = 12	$12^7 \ mod \ 391 = 177$
a = 00	$00^7 \ mod \ 391 = 00$
w = 22	$22^7 \ mod \ 391 = 367$
a = 00	$00^7 \ mod \ 391 = 00$

On receiving the ciphertext, the recipient entered it into the decryption process to decrypt the text as follow:

Decryption process	Plaintext
$00^{151}\ mod\ 391 = 00$	00 = a
$232^{151}\ mod\ 391 = 232$	03 = d
$00^{151}\ mod\ 391 = 00$	00 = a
$177^{151}\ mod\ 391 = 177$	12 = m
$00^{151}\ mod\ 391 = 00$	00 = a
$367^{151}\ mod\ 391 = 367$	22 = w
$00^{151}\ mod\ 391 = 00$	00 = a

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) and (2).

At encryption side $C = E_k(P)$, and at decryption side $P = D_k(C)$, 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.

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 Advanced Encryption Standard (AES). 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 (CNSS Policy No. 15, Fact Sheet No. 1., 2003).

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 or decryption key is derive from the encryption key. 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 Rivest, Shamir and Adleman (RSA) 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. RSA is much slower than other symmetric cryptosystems, in that data is encrypted

with a symmetric key algorithm and then the comparatively short symmetric key is encrypted with RSA. This allows the key necessary to decrypt the data to be securely sent to other parties along with the symmetrically-encrypted data.

SUMMARY

In this survey paper we describe and compare between symmetric and asymmetric encryption technique, and provide many examples to show their differences. We conclude from the examples that asymmetric encryption algorithm still has low performance compared to symmetric encryption algorithm.

REFERENCES

Agnew, G. B., Mullin, R. C., Onyszchuk, I. M. and Vqanstone, S. A. (1995). An implementation for a fast public-key cryptosystems. *Journal of Cryptology*, 3(2), 63- 79.

Chapple, M. and Solomon, M. (2005). *Information security illuminated (1st ed.)*, USA: Jones and Bartlett Publishers.

Childs, J.R. (2000). *General solution of the ADFGVX cipher system*, USA: Aegean Park Press.

CNSS Policy No. 15, Fact Sheet No. 1. (2003). National policy on the use of the advanced encryption standard (AES) to protect national security systems and national security information

Delfs, D. and Helmut, K. (2007). *Introduction to cryptography: principles and applications (2nd ed.)*, Germany: Springer Science & Business Media.

Salomon, D. (2003). *Data privacy and security (1st ed.)*, New York: Springer-Verlag.

Dieter, G. (2005). *Computer Security (2nd ed.)*, UK: John Wiley & Sons.

Diffie, W. and Hellman, M. E. (1976), "New directions in cryptography", *IEEE transaction information theory IT*, 22(6), 644–654.

El Gamal, T. (1985). "A public key cryptosystem and signature scheme based on discrete logarithms", *IEEE Transaction information theory IT*, 31, 469—472.

Forouzan, A. (2007). *Cryptography and network security (1st ed.)*, USA: McGraw-Hill.

Hamamreh, R. and Farajallah, M. (2009) " Design of a Robust Cryptosystem Algorithm for Non-Invertible Matrices Based on Hill Cipher ", *International journal of computer science and network security*, **9**, 12-21.

Hoffstein, J. (2008). *An introduction to mathematical cryptography (1st ed.)*. Germany: Springer Science & Business Media.

Kahn, D. (1996). *The Codebreakers; The Comprehensive History of Secret Communication from Ancient Times to the Internet*. NY:Charles Scribner's Sons,

Schneier, B. (1996). *Applied cryptography: protocols, algorithms, and source code in C.*, New York: John Wiley & Sons,.

Kenneth, H. (1992). *Elementary number theory and its applications (3rd ed.)*, Germany: Addison-Wesley.

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

Maret, S. (1999). *Cryptography Basics PKI (1st ed.)*. Switzerland: Dimension Data SA.

National Institute of Standards and Technology, (1994). NST FIPS PUB 186, *Digital Signature Standard*, U.S. Department of Commerce.

Ralph, E. and Weierud, F. (1987). " Naval Enigma: M4 and Its Rotors ". *Crypologia*, **11**, 235-244.

Rivest, R., Shamir, A. and Adleman, L. (1978). "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, **21**(2), 120-126.

Rodríguez, H., Saqib, N.A. Arturo, D. P. and Cetin, K. K. (2006). *Cryptographic algorithms on reconfigurable hardware (1st ed.)*, USA: Springer.

Seth, S. M. and Mishra, R.(2011). "Comparative analysis of encryption algorithms for data communication", *International journal of computer science and technology*, **2**(2), 292-294.

Stallings, W. (2006). *Cryptography and network security. Principles and practices (4th ed.)*, USA: Pearson Prentice Hall.

Stinson, D.R. (2006). *Cryptography, theory and practice (3rd ed.)*. Boca Raton: Chapman and Hall/CRC.

Thomas, K. (1998). "The myth of the skytale". *Taylor & Francis*, 33, 244-260.