IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Analysis Of Tools And Techniques In Cryptography

T. Sangeetha Msc.,M.Ed

Assistant Professor, Department of Computer Science

Christ college of Arts and Science, Kilachery-631402

ABSTRACT

In the epoch of advanced electronic and communication systems, it is being observed most of the times that the information is being assaulted with worms and viruses.

To shield the data, a secure and advanced cryptosystem is required to devoid any type of dilemma. There are several tools and techniques that are being used, to meet the challenging needs for a highly secure transmission and reception system.

In the spirit of algebraic abstraction, this paper advocates the definition and use of higher levels of abstraction in cryptography (and beyond).

If contrasted with the standard bottom-up approach to defining models of computation, algorithms, complexity, efficiency, and then security of cryptographic schemes, our approach is top-down and axiomatic, where lower abstraction levels inherit the definitions and theorems (e.g. a composition theorem) from the higher level, but the definition or concretization of low levels is not required for proving theorems at the higher levels.

The goal is to strive for simpler definitions, higher generality of results, simpler proofs, improved elegance, possibly better didactic suitability, and to derive new insights from the abstract viewpoint.

Previously security was mainly concerned with the exchange of messages that took place in communication. After that some techniques came into existence that provided more reliable and superior results.

But the prerequisite for a more secret system is increase in amount day by day. As the communication system is being more complex, according to the demand more advanced and protected cryptograms are important. In the following paper diverse cryptographic techniques have been analyzed that serve the purpose of security from 1900 B.C up to the present day visual.

General Terms:

Security Algorithms, Pseudo codes, Hierarchy of Cryptography, Language of encryption, definition of cryptography ,Techniques of cryptography, important of cryptography et. al.

Keywords

Hieroglyphics Enigma Machine, DES, AES, RSA Quantum Cryptography.

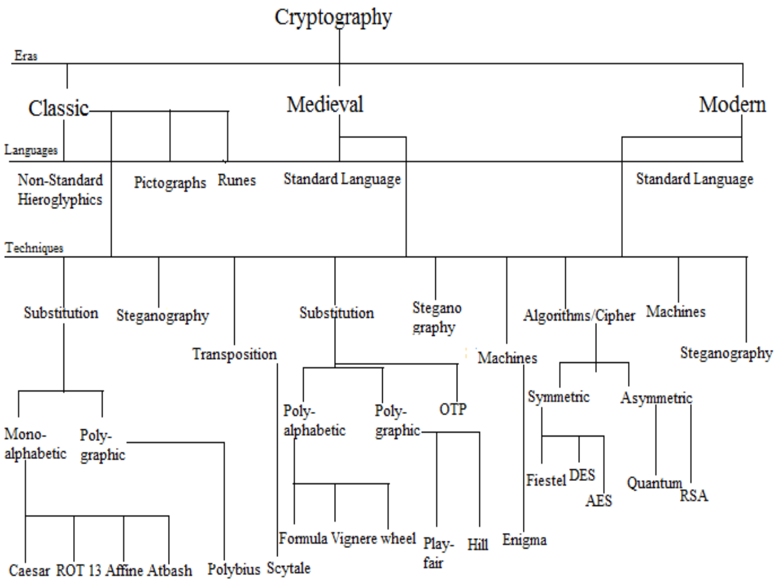
INTRODUCTION

It is propensity of humans to veil their information from others. Even children apply different methods to tervert messages from their parents, friends, well wisher and from siblings. There are several of examples where distinct heaped tricks and techniques are applied to cosset the communication from enemy. [1] There are many techniques paves way to perform security tasks. In past only pen paper based methods were used to exchange the message from a person to person. In World War II various equipments were procured that helped to awkwardly up a steep slope the message. Hence there are more arts and equipments that are pepped to provide safety to the information. Beside, many methods are available that can be an effective use an efficiently for breaking the not morally correct.

In contrast, in cryptography (and in other areas of computer science), definitions, theorems, and evidence are highly technical and have genuine an issue due to the technical an object made by a human being of the specific model (e.g. defining the computational model via Turing machines and communication via tapes, using asymptotic definitions of systems and protocols, defining efficiency as polynomial-time, using a particular adversarial model, etc.).

There are also difference ways to break the cipher not morally correct.) All the techniques and tricks for both cipher making and cipher breaking come venerate the category of cryptography. Therefore cryptography is the area of computer science that deals with different procedures and activities to steep ground and viewable state the data. The action of content of data has begun 4000 years ago in 1900 B.C by one of the Egyptian scribes. They made use of non standard mark known as hieroglyphics, but this was not a worrying because of techniques came into existence that somehow provided the safety measure. The key used for the two can be a symmetric key or an asymmetric key.

2.CRYPTOGRAPHY



In cryptography, encryption is the process of not clear enough to read disappearing information to make it without knowledge. This is usually done keep privacy, and for underhanded communications. Encryption can also be used for certification, digital signatures, and digital cash etc. This channel could be a telephone line or a computer network.

We give a first high-level example of how the concepts of the previous section could be interpreted in a case cryptographic context. We also refer to [12] for a discussion of concrete examples of resources and converters in a cryptographic context.

Mathematical_ Notation_ of_ Cryptosystem

From the above cryptosystem there are basically five tuples (*O*, *C*, *K*,*E*,*D*), where the following conditions are satisfied:

1. O is the finite set of possible originate message;
2. C is the finite set of possible cipher texts;
3. K is the finite set of possible keys;

Rule: - For each task there is an encryption rule e K ∈ E and corresponding rule d K∈ D where, e K: O → C and d K ∈ C → O are functions such that d K (e K (m))= m for every original message m∈ O. [3]

Figure 1 Mathematical Notation of Cryptosystem.

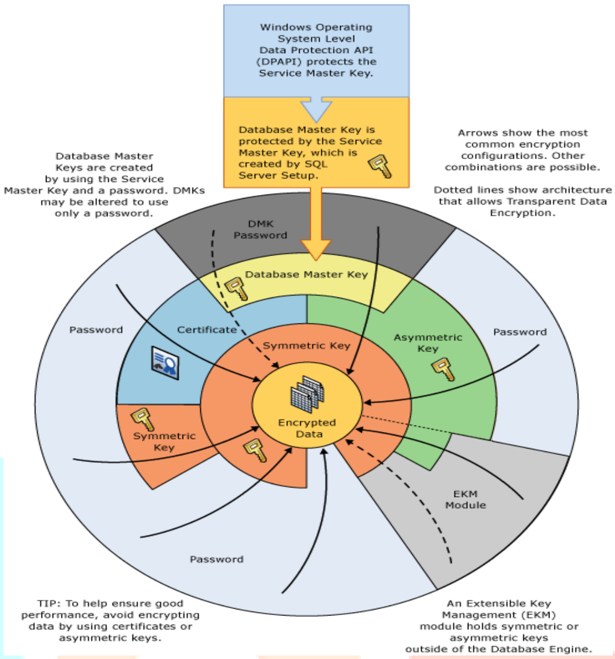
1. CRYPTOGRAPHIC TECHNIQUES

Cryptography, the art of enciphering and deciphering the message in a secret code has played and still playing vital roles in every nation. It is becoming a important step in this world where there is fight among the code makers and code breakers [4]. From 1900 B.C the process of cryptology was begin by the Egyptian scribe while an effort to achieving to uphold the records in their own language. They made use of the non-standard hieroglyphics for communication purpose.

Cryptography is not abjection to separate or to a group of separates; it serves the whole world for keeping their information secure from others. The use of cryptography is growing day by day; it is being employed in wars and used in many educational institutions.

The cryptography plays vials roll in to three main domain that is classic cryptography where enciphering is done only with the help of pen and paper, then medieval domain of cryptography where different substitution and transposition came into existence and at last the modern era of cryptography where revolutionary encryption techniques are introduced such as DES, AES, RSA etc.

The above hierarchy is showing some of the important cryptographic tools and techniques.



Windows Operating System Level Data Protection API (DPAPI) protects the Service Master Key.

Database Master Key is protected by the Service Master Key, which is created by SQL Server Setup.

Database Master Keys are created by using the Service Master Key and a password. DMKs may be altered to use only a password.

Arrows show the most common encryption configurations. Other combinations are possible.

Dotted lines show architecture that allows Transparent Data Encryption.

TIP: To help ensure good performance, avoid encrypting data by using certificates or asymmetric keys.

An Extensible Key Management (EKM) module holds symmetric or asymmetric keys outside of the Database Engine.

Figure 2.Hierarchy of Cryptography

Classic Era

In Classic era non-standard hieroglyphics, pictographs runes etc were used to encrypt the messages at that time and were attractive strong according to that time because less number of people was there who knew about these languages or symbols so the techniques worked effectively at that time but when people got educated and the language became a part of everyone's daily life, new and even more complex techniques came into existence [6].

Substitution Techniques

In cryptography substitution ciphers plays a crucial role to awkwardly up a steep slope the message. In substitution, every single bit of message is being replaced with other and a particular sequence is followed for the whole procedure. Substitution can be or substituting one bit at a time or many bits at a single moment and called as mono alphabetically or poly alphabetically respectively.

Definition: Sequential replacement of an original message with cipher text in order to scramble every single bit of the plain text so that no other not having office permission party can take advantage of it.

```
Substitution_ Cipher
Assume O=C= X 26, whereas K includes set of all
    Possible permutations starting from 0 to 25.
There should be a random permutation say, Ω and
belongs to K.
                 Encryption can be done as
E Ω (α ) = Ω (α ), And,
Decryption is defined as
D Ω ( β )= Ω -1( β )
Where,
Ω -1 is the inverse permutation to Ω .
```

Figure3 Pseudo code of Substitution Cipher

The above substitution basics followed in both mono and polyalphabetic substitution. In mono alphabetic substitution only single letter is substituted with other letter or symbol.

Shift Cipher

If you have a message you want to transmit securely, you can encrypt it (translate it into a secret code). One of the simplest ways to do this is with a shift cipher. Famously, Julius Caesar used this type of cipher when sending messages to his military commanders.

To make all of this more mathematical, consider the following conversion table for the English alphabet: 0 1 2 3 4 5 6 7 8 9 10 11 12 A B C D E F G H I J K L M

```
Pseudo code_ Ceaser_ Cipher_ Decryption

  Assume O=C= K= C 26,

For 0 £ K ³ 25
Perform,

DK ( b )= ( b -K) mod

26
Where,
                (K=3)
```

For the number of years shifting technique worked very well and it would be a tedious to crack the code at that time. In 50-60 B.C Julius Cease introduce one more way to scramble the message that is based on the shift technique.

In his way of encrypting message current letter was substituted to the third letter that is he shifts the positions of the letter to make the text irrelevant.

That is a will become d and d will become g [8]. There is an instance that will help to understand the working of the cease cipher.

Same technique work as the base for number of techniques for instance ROT 13 in which shifting is done for thirteen place.

All of them will follow the same sequence. This is all about the historical ciphers where all the attempts were made on the paper with pen.

PT

a

b
CT

D

E

c

d

e
F

G

H

Medieval Cryptography

Most of the noteworthy work on Cryptography in the early Medieval period happened in the Arab world. *The Manuscript for the Deciphering of Cryptographic Messages* of *Al-Kindi* is one of the most important scriptures on Cryptography. Cryptography enters the Dark Age; there is another civilization rising in the east. In 900 A.D Arabs society was one of the most literate cultures in the world and the study of code flourished.

Polyalphabetic Substitution (1466)

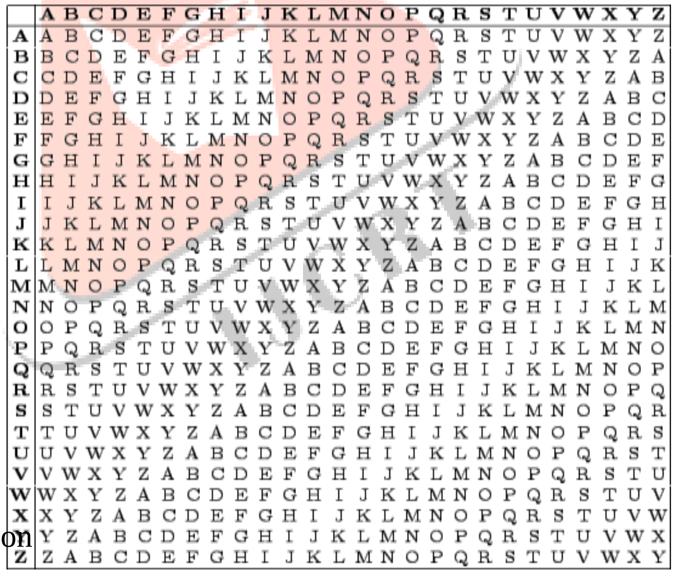
In 1466 an Italian architect Leon Battista Alberti develops a greatest crypto logic invention in 1000 years at the urging Vatican. He often called as the “father of western cryptology” and invented a polyalphabetic cipher to encode the message. It was a system of rotating cipher disk with two rings of letter and several numbers by scrambling so many letters randomly. It was the first to challenge Arab code breaking method of frequency analysis.

Previous systems just replace A D only at a time but according to the Alberti cipher disk used as disk in which these letters combination could be change from time to time. And as a coupling letter “A” would be representing not only by one letter but by many letters. This was called as polyalphabetic substitution and it was the basis for many modern cipher systems [2].

Vigenere Cipher

The successor of Alberti continued his work in the field of security. In 1585 Blaise de Vigenere publishes his work on the principle of polyalphabetic substitution.

Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the *Vigenère square or Vigenère table*. He proposed a table of 26*26 in which 26 alphabets arranged row wise and 26 alphabets are arranged column wise and the table is named as Vigenere table [10]. For generating covert message same length of key is used.



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

igure 6 Vigenere Square

```
Pseudo code_ Vigenere_ Cipher_ Decryption
Let n be a positive
integer Assume
O=C= K=( X 26)$^n$
For K= (K1- - - K n)
Execute,
Decryption;
DK ( β 1, β 2, β 3,- - - - β n )= ( β 1-K1, β 2-
K2,        β n-Kn)
Where,
All operations are performed in X 26
```

Figure 7(b). Pseudo Code of Vigenere Cipher Decryption

Wheel Cipher

In 1790 one more poly alphabetic substitution technique introduced by Thomas Jefferson in which 26 letters of alphabets are arranged. Using the cipher wheel to encrypt a message (make it secret) involves transforming each letter of the message into another letter or a number by following a series of steps: an algorithm. In this case, the algorithm involves simply shifting each letter of the message by a certain number of places through the alphabet.

Play fair Cipher

In 1854 one more substitution technique came into existence known as play fair cipher. In this cipher a 5*5 matrix is used in which the message is written. Then it is enciphered both row wise and column wise.

The **Playfair cipher** was the first practical digraph substitution cipher. The scheme was invented in **1854** by **Charles Wheatstone** but was named after Lord Playfair who promoted the use of the cipher. In playfair cipher unlike traditional cipher we encrypt a pair of alphabets(digraphs) instead of a single alphabet.

Hill Cipher

The idea of encrypting the information using matrix method is employed in one more encryption technique. In 1929 Lester S. Hill proposed a new way to encrypt the message and named his technique after his name that is hill cipher.

Hill cipher is a polygraphic substitution cipher based on linear algebra. Each letter is represented by a number modulo 26. Often the simple scheme A = 0, B = 1, …, Z = 25 is used, but this is not an essential feature of the cipher. To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

```
Pseudo code_ Hill_ Cipher
Let n be a positive integer Assume
Let n be a integer Let $O=C=( X 26)^n$
K= (n*n) invertible matrices over X 26
```

Vernam Cipher

Vernam Cipher is a method of encrypting alphabetic text. It is one of the Substitution techniques for converting plain text into cipher text. In this mechanism we assign a number to each character of the Plain-Text, like (a = 0, b = 1, c = 2, … z = 25).

Method to take key: In the Vernam cipher algorithm, we take a key to encrypt the plain text whose length should be equal to the length of the plaintext.

Encryption Algorithm:

1.Assign a number to each character of the plain-text and the key according to alphabetical order.
2.Bitwise XOR both the number (Corresponding plain-text character number and Key character number).
3.Subtract the number from 26 if the resulting number is greater than or equal to 26, if it isn't then leave it.

```
Pseudo code_ Vernam_ Cipher
Let n be a positive integer and $n \geq 1$
Let $O=C=( X\ 2)^{n}$ ;

$K= (X2)^{n}$ ;
Execute,
EK ( α ) = ( α K1 + α K2- - - α K n) mod
2                                        n
2 // EK exclusive or (XOR) of two terms.

and
for decryption;
Perform
DK ( β )= ( β K 1+ β K 1- - - β K n) mod
1                              1          n
2
```

Figure 9 Pseudo Code of Vernam Cipher

Enigma Machine

When the Enigma was in use, with each subsequent key press, the rotors would change in alignment from their set positions in such a way that a different letter was produced each time.

With a message in hand, the operator would enter each character into the machine by pressing a typewriter-like key. The rotors would align and a letter would then illuminate, telling the operator what the letter *really* was. Likewise, when enciphering, the operator would press the key and the illuminated letter would be the cipher text.

At the end both the sides are swapped to each other say, left become right and right become left [15]

Advanced Encryption Standard

Drawbacks that lead DES down is cover up in Advanced Encryption Standard. The main disadvantage of DES is the size.

But in AES the key size is large enough to encode the message into the cipher code. Here in AES three key sizes are available that is 128 bits that is used normally and 192 and 256 bits that is use where high security is required [16].

Asymmetric Key Encryption

In Asymmetric key encryption pair of key is used for encryption and decryption purpose. In this one key is used for encryption by the sender and another key used by the receiver for decryption purpose.

RSA

The approach of using public key cryptography was first introduced by Diffie and Hellman in their paper and that will lead to RSA [17]. RSA is well known public key encryption algorithm. Here, in RSA the cipher code is generated from the equation: -

$$C=Me \bmod n$$

And the inverse would be calculated from the following equation: -

$$M=C\ d \bmod n$$

$$= (Me)\ d \bmod n$$

$$=Med \bmod n$$

Quantum Cryptography

The use of quantum cryptography initiated in 2003. In it two protocols are used for quantum key distribution these are BB84 and E91. The message initiated from the sender side is in either horizontal or in vertical basis or in diagonal or anti diagonal basis.

CONCLUSION

From the ancient times it is seen that the security is one of the important aspects in the ways of communication. Lots of tricks and concepts have been exercised to maintain the high security.

Since the classic era various methods are used to hide the information. Vernam cipher, play fair ciphers are some of the examples.But as the time moved, more complex security systems were required to secure the communication over the network. In medieval era more techniques came into existence that promised to veil the information from the third party.

Moving forward various machines was designed at the time of World War II which played an enormous role in securing the information over the wide area the network e.g. the enigma machine. As clock is moving continuously more and more techniques came and serve the purpose of securing the information.

In the modern era some of the remarkable techniques were developed and it was difficult to break them. For instance in the category of symmetric key encryption, the DES and AES were developed and in the category of asymmetric key encryption RSA like algorithms were generated.

DES makes use of 56 bit keys to encrypt the message whereas AES make use of 128, 192 and 256 keys to encrypt the message. As from the key size it is easy to judge the breakability of the technique. It is clear from the previous knowledge in the cryptography that number of keys are directly proportional to the security provided by the algorithm.

From the above analysis,

security has become an paramount concern in our daily lives. In the competitive world everybody wants to move ahead of others through their introspection and innovations. But side by side the ethical issues are coming into existence that hampers the confidentiality and integrity of somebody’s personal information.

REFERENCES

[1] Wade Trappe and Lawrence C. Washington,” Introduction to cryptography with coding theory”2nd Edition, ISBN 0-13-198199-4, 2006.

[2] David Khan “The Code Breakers-The Story of Secret Writing”, February, 1973.
[3] Douglas Stinson, “Cryptography: Theory and Practice”, CRC Press, 1995.
[4] Gardner, M. “Codes, Ciphers, and Secret Writing”, ISBN 0-486- 24761-9, pp 7-96, December 1972.
[5] [A Short History of Cryptography Available at “https://www.youtube.com/watch?v=H9Cu36Qj3dQ “Access on 12/28/2014. Richard W. Selby.”Enabling Reuse-Based Software Development of Large-Scale Systems “, 2005, IEEE.
[6] Ancient Civilization available on “http://www.dl.ket.org/humanities/connections/class/ancient/index.htm” Accessed on 31/1/2015

[7] A Brief History of Cryptography." Cryptozine. 16 May 2008.
[8] Dennis Luciano and Gordon Prichett,”From Ceaser to public Key Cryptosystem”, published in Mathematical Association of America, vol. 18(1), pp 2-17, January 1987.
[9]Atul Kahate “Cryptography and Network Security” Tata McGraw- Hill Edition 2008 ISBN-10:0-07-064823-9.
[10]Richard A. Mollin “An Introduction to Cryptography
[11]Bedini, Silivio A. “Thomas Jefferson: Statesman of Science”,
ISBN 0028970411, Newyork: Macmillan c1990
[12]Mauborgne, “An Advanced Problem in Cryptography and its Solution” The Army Service Schools, Port Leavenworth, Kansas, 1914.
[13]C.E. Shannon “Communication Theory of Secrecy System”, Bell System Technical Journal, vol. 28(4), pp. 656-715, ISSN 0005- 8580, October 1949.
[14] Louis Kruth and Ciphere Deavours “The Commercial Enigma: Beginnings of a Machine Cryptography”, Cryptologia, Vol. XXVI (1), pp. 1-14, January 2002.
[15] Miles E. Smid and Dennis K. Brantad “The Data Encryption Standard: Past and Future”, Proceedings of IEEE, vol. 76(5), pp. 550-559, May 1998.
[16] Federal Information Processing Standards Publication 197“Specification for the Advanced Encryption Standard”, pp 1-47, 26 November 2001.
[17] Whitfield Diffie and Martin E. Hellman” New Directions in Cryptography” IEEE Transactions on Information Theory, Vol. IT 22 No. 6, pp. 644-654, November 1976.
[18] N. Gisin, G. Ribordy, W.Tittel, and H. Zbinden, “Quantum Cryptography”, Rev. Mod. Phys. 74, pp-145-195, 2002
[19]

Damien Stucki. Et. al.”Continuous High Speed Coherent One- way Quantum Key Distribution” OPTICS EXPRESS, Vol. 17(16), pp-13327-13334, 3 August 2009.
[20] Artur Scherer, Barry C. Sanders, and Wolfgang Tittel” Long- distance practical key distribution.