A Review Paper On Concepts Of Cryptography And Cryptographic Hash Function

Dr. R.K Gupta

Professor, Department of Mathematics, Lovely Professional University, Phagwara
rajesh.gupta@lpu.co.in

Abstract: We start with basic concepts of cryptography and move towards its history. Main concentration is on various algorithms including DES, RSA. Here we also discussed cryptographic hash functions- MD family, SHA family and RIPEMD, BLAKE and WHILPOOL families also and finally we wind up the paper comparison

Keywords: DES, AES, RSA, Hash Function, MD5,SHA-3,BLAKE, RIPEMD, WHIRLPOOL

1. INTRODUCTION

1.1 Cryptography It is the process of transforming the secret data or information into a unreadable or scrambled form. In fact it is the art of writing the message secretly. The concept of cryptography depends on five factors. These are discussed below [1]

(a) Plain text: The message or information that we want to send secretly. The set of plain text is represented by ***P***.

(b) **Cipher text:** It is the scrambled or unreadable form of information or message. The set of cipher text is represented by ***C.***

(c) **Key:** It is the rule with the help of which data is scrambled. The set of keys is represented by ***K.***

(d) Encryption Function: It is the method using which the cipher text is generated. The set of encryption function is represented by ***E(x)***.

(e) Decryption Function: It is the inverse function of E(x). It is the effort to generate the original message. The set of decryption function is represented by ***D(x)***.

Thus cryptography is depends on {***P, C, K, E(x), D(x)***}

1.2 Cryptography Goal

Cryptographic goals are set before developing a new encryption model.

- Access Control
- Authentication
- Confidentiality
- Data Integrity
- Non-Repudiation

:

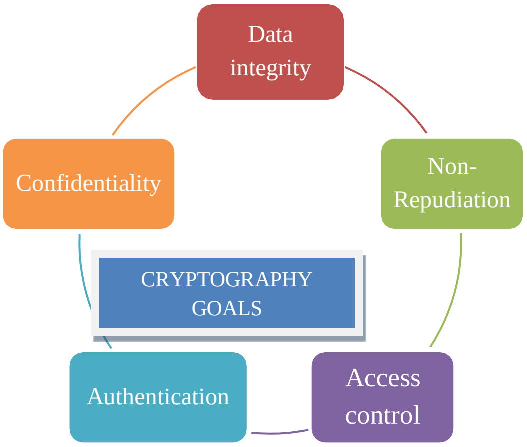


Figure1: Cryptography goals

1.3 Types of Keys

- Symmetric Key Cryptography
- Asymmetric Key Cryptography

It is a two key system also known as the public key system, one key encrypts the information and another, and mathematically related key decrypts it. RSA algorithm is one such example.

2. HISTORY OF CRYPTOGRAPHY

It is considered that as people become able to write the art of cryptography was born along with it. With the time, human beings got organized in kingdoms, tribes and groups. Then ideas such as politics, battles, power evoke the natural need of people to communicate secretly. Thus journey of cryptography begins.

2.1 Hieroglyph

Some 4000 years ago, the technique named ***Hieroglyph*** was used by the Egyptians to communicate secret messages within the scribes. It was known to be the oldest cryptographic technique. This secret code was only available with the person who used to deliver message on the behalf of the king.

2.2 Caesar Shift Cipher

Then came the Roman method of cryptography. Each alphabet of English language is associated to a specific number and performs accordingly. Substitution is shown below

A → 0	**B → 1**	**C → 2**	**D → 3**	**E → 4**
F → 5	**G → 6**	**H → 7**	**I → 8**	**J → 9**
K →10	**L → 11**	**M → 12**	**N →13**	**O →14**
P→15	**Q →16**	**R→17**	**S→ 18**	**T→ 19**
U → 20	**V → 21**	**W →22**	**X→23**	**Y →24**
Z →25				

Figure 2: Substitution matrix

Mathematically, we define a
E(x): L → Z_{26}
where L is the set of letters
i.e.,
Let the encryption function be

……….(1) Plain Text:

D A U G H T E R

Position:

3 0 20 6 7 19 4 17

(Substitution by numbers)

Key:

6 6 6 6 6 6 6 6

E(x):

9 6 26 12 13 25 10 23

(Result
)

E(x):

9 6 1 12 13 25 10 23

(Replace 26 by 1)

Cipher
Text:

J G B M N Z K X

(encoded message)

i.e., the word **DAUGHTER** is encrypted as **JGBMNZKX** under the function E. Now, we have to decode the message, for this we need to define another function i.e., decryption function which is the inverse function of (1)

The decryption function is given by

– ……………(2) Cipher Text:

J G B M N Z K X

(encoded message)

E(x):

9 6 1 12 13 25 10 23

Key:

6 6 6 6 6 6 6 6

(Subtracting the key)

D (y):

3 0 -5 6 7 19 4 17

E(x)

3 0 20 6 7 19 4 17 (Replace -5 by 20)

Original message:

D A U G H T E R

In this way the receiver gets the original message using decryption function depending upon same key.

Shortcomings:

(a) Search space is very small, each letter has only 25 shifts besides itself. Only a little patience of trying all the possibilities will reveal the message

(b) As every letter is shifted by a fixed number, if we able to determine the decryption of one then we are able to decode the entire message.

2.3 Substitution Cipher

Later, during 500 to 600 BC the scholars evolved simple mono-alphabetic substitution ciphers. It replaces one character of plaintext with other symbol or character by using some rule. This rule used to get back the message. A substitution cipher is harder to break. The way this one works is we map each alphabet to another alphabet in the letter.
Shortcomings: Search space is very small, spending reasonable time on searching for results the attacker gets the solution easily.

2.4 Affine Cipher

P = = {0, 1, 2, 3,.., 25}

. Length of key = 2

Mathematical Modeling :

.

For Example : Consider key k = (15,18) clearly gcd(15,26)=1

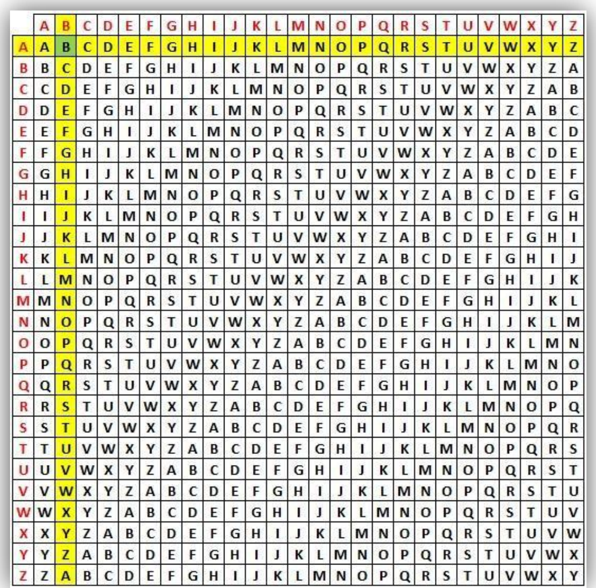
Vigenere Cipher

An improved cipher ***vigenere cipher*** came into existence in the 15th century and was first published in 1863
Plain text: M E E T I N G A T N I N EKey: L I G H T L I G H T L I G

Cipher text: X M K A B YOG A G T VK

Here, key is the word LIGHT. In figure 3 rows represents the plain text whereas columns represents the key and the cells represents the encrypted transformations.

Shortcomings: The repeating nature of the key is the major problem with this cipher .If the guess for key's length sets correct then the message is easily decrypted by the attacker.



	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

Figure 3: Vigenere Table

2.5 Hill Cipher

In 1929, Lester S. Hill gives new dimensions to cryptography by introducing the usage of linear algebra to scramble the plain text. He used familiar concepts like matrix multiplication and inverse of matrix for encryption and decryption. In this method the key is a n x n invertible matrix.

Shortcomings: As the Hill cipher is completely linear so an attacker can set up a linear system which can be easily solved. Calculating this solution by standard linear algebra algorithms then takes very little time.

3 FAMOUS ALGORITHMS

3.1 RSA

It is the system in which part of the Key made public by the receiver and part of key left secrect. Public key used for encryption and secret/Private key is used for decryption.

Public key cryptosystem	Key Space(Public ,Private)	Encryption	Decryption
RSA	{(| Public =(n,e) ,Private =(p,q,d)		

3.2 Block Cipher

- Suppose Alice and Bob want to use block cipher for encryption.
- They agreed on block cipher.
- Suppose Alice has long message of m bits .
- Suppose Alice and Bob have ‘ L’ bit block cipher (DES-64 bit, Triple DES-64 bit,AES-128 bit, SPN) with key .
- Long message ‘m ‘ will be broken ‘L’ bit blocks , in the last block some dummy bits will be appended to make it L bit [3].

3.3 Advanced Encryption Standard (AES)

- Earlier Ciphers (Classical) broken under the if we have the modern computer speed . Not secure.
- If we have the DES which is also broken by the generic attack, time trade off attack, Exhaustive search Attack
- On DES one can mount the Non -generic attack like differential cryptanalysis attack, linear cryptanalysis attack . DES is not secure .
- We need to have alternate standard , we have Triple DES , 3X16=48 rounds , so huge .
- AES is designed to resist the generic ,Differential and linear cryptanalysis attack and all other existing attacks [5,12].

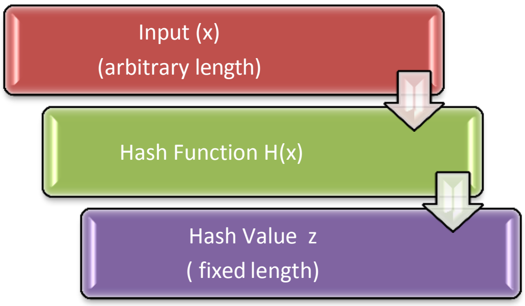
Table 2: Comparison between Standard Algorithms

Name of Algorithm	**Origin**	**Key type**	**Created by**	**Year**	**Key Size (in bits)**	**Block size (in bits)**	**Rounds**	**Shortcomings**
DES [3]	Lucifer	Symmetri c key	IBM	1975	56	64	18	Not deemed sufficient to encrypt sensitive data

3DES	DES	Symmetric key	IBM	1978	112 or 168	64	48	Slow
AES	Square	Symmetric key	Joan Daemen and Vincent Rijmen	1998	128, 192, 256	128	10,12,14	Power Analysis Attack
RSA	Mathematical, based on product of large primes	Asymmetric key	**R**ivest **S**hamir **A**delman	1977	1024 to 4096		1	Difficult to decide large p and q (slowest)

4. CRYPTOGRAPHIC HASH FUNCTION

It is the one of the Mathematical functions where hardness lies in finding the inverse. Output of the hash functions is of fixed length irrespective of length of input numerical message. Such output of fixed length is called message digest [4].



4.1 Properties of Hash Functions

It should be applied to any size input and produce fixed length output.

H(x) , the hash function has the following mathematical properties:

(a) Pre-Image Resistance (Hard to reverse the functional value)

Let x be the input and z be the hash value which is produced using the hash function, i.e., H(x) = z then $H^{-1}(z) = x$ is difficult to compute. It means computationally infeasible

It secure from an attacker having only output value of hash function .

(b) Second Pre-Image Resistance (Hardness in finding equal value of given hash value)

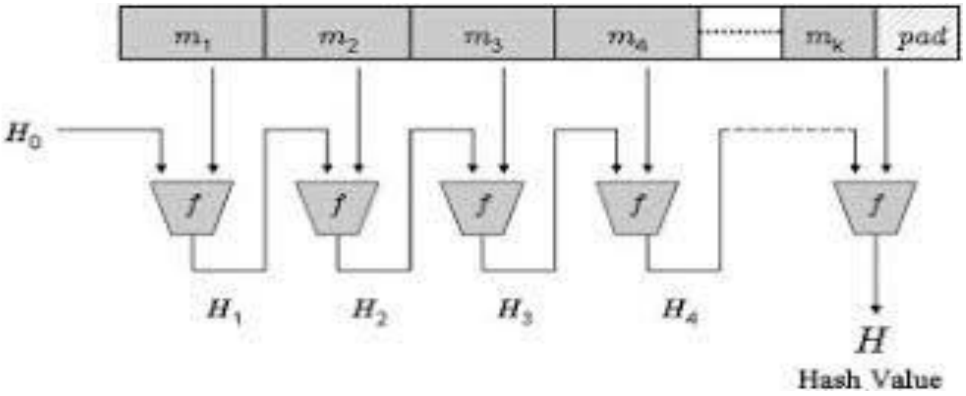
s.t. .

(c) Collision Resistance (Different inputs but same output)

Let be two different input values and exists but the condition is hard to develop [6].

<u>General Structure of Hash Function :</u>

, Big message M divided into blocks each.



5. SOME HASH FUNCTIONS

1) **Message Digest (MD) :** There are various hash functions developed in this category like MD2,MD4,MD5 and MD6 [7].

2) **RIPEMD (Race Integrity Primitive Evaluation Message Digest):** Open research community had developed these type of functions. It includes RIPEMD160

3) **Whirlpool :** It 512 bit function derived from advanced encryption standard [14].

4) **Secure Hash Function (SHA) :** Various secure hash functions are part of this family like SHA- 3,SHA-2,SHA-1 and SHA-0 [10].

5) BLAKE

Family of **BLAKE** comprises of BLAKE, BLAKE 2, BLAKE 256, BLAKE 224, BLAKE 384, BLAKE 512[13] .

- These are hash functions based on Dan Bernstein's ChaCha stream cipher, but a permuted copy of the input block, XORed with some round constants, is added before each ChaCha round.
- Like SHA-2, there are two variants differing in the word size. ChaCha operates on a 4×4 array of words. BLAKE repeatedly combines an 8-word hash value with 16 message words, truncating the ChaCha result to obtain the next hash value.
- **BLAKE-256** and **BLAKE-224** use 32-bit words and produce digest sizes of 256 bits and 224 bits, respectively, while **BLAKE-512** and **BLAKE-384** use 64-bit words and produce digest sizes of 512 bits and 384 bits, respectively. When run on 64-bit x64 and ARM architectures, BLAKE2 is faster than SHA-3, SHA-2, SHA-1, and MD5.

Table 2: Comparison between various Hash Functions

Hash Function	**Designer**	**Year**	**Structure**	**Attack**	**Attack year**	**Output size**	**Block size /Rounds**
MD5	Ronald Rivest	1992	Merkle-demgard construction	collisions found	2012	128	512
RIPEMD	Hans dobertin, Antoon Bosselears, Bart Preneel	1996	Based on Md4	Collision	2004	128 160 256 320	
WHIRLPOOL **[11]**	Vincent Rijmen, Paulo S.L.M. Barreto	2000	Miyaguchi preneel	Rebound attack	2009	512	Round 10
SHA 2	National security Agency	2001	Merkle- damgard construction with devies meyer compression function	Pre image resistance Collision resistance	2011	224,256, 384, 512	256 , (8 x 32), 512 (8 x 64)
SHA 3 (KECCAK)	Guido Bertoni, Joan daemen, Micheal	2012	Sponge Construction	Collisions found		224, 256,	1152 1088

[9]	Peeters, Gilles van Assche					384, 512	832 576
BLAKE	Jean-Philippe Aumasson, Luca Henzen, Willi Meier, Raphael C.-W. Phan	2012	HAIFA Construction	-----	------	224, 256, 384, 512	Rounds (14,16)

6. CONCLUSION AND FURTHER RESEARCH

This paper gives the comparisons between various cryptographic algorithms and different hash functions which help to understand the crux of cryptography. In various hash function attacks were found. More effective attacks can be develop i.e., the security level of newly and effectively develop hash functions can be checked.

7. REFERENCES

1. Atul Kahate “Cryptography and Network Security”, Tata McGraw-Hill Companies, 2008
2. D. Boneh and M. Franklin, “Identity-based encryption form the weil pairing”, in Advance in Cryptology (CRYPTO’01), LNCS 2139, Springer Verlag, 37, 213-229, 2011
3. Davis.R, “The Data Encryption Standard in Perspective”, Proceeding of Communication Society magazine, IEEE, Vol 16, Nov 1978
4. Mr. Gurjeevan Singh, Mr. Ashwani Singla and Mr. K S Sandha, "Cryptography Algorithm Comparison for Security Enhancement in Wireless Intrusion Detection System", International Journalof Multidisciplinary Research, Vol.1 Issue 4, pp. 143-151, August 2011.
5. Zilhaz Jalal Chowdhury, Davar Pishva and G. G. D. Nishantha, “AES and Confidentiality from the Inside Out”, the 12th International conference on Advanced Communication Technology (ICACT), pp. 1587-1591,2010.
6. https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm
7. Xiaoyun Wang; Dengguo Feng; Xuejia Lai; Hongbo Yu (2004-08-17). "Collisions Hash Functions MD4 MD5 RIPEMD HAVAL". Retrieved 2017-03-03.
8. Guido Bertoni, Joan Daemen, Michaël Peeters and Gilles Van Assche. "On the Indifferentiability of the Sponge Construction". EuroCrypt 2008.
9. Keccak implementation overview Version 3.2, section 3.1
10. Hernandez, Paul (5 August 2015). "NIST Releases SHA-3 Cryptographic Hash Standard".

11. Florian Mendel1, Christian Rechberger, Martin Schläffer, Søren S. Thomsen (2009-02-24). The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grøstl (PDF). Fast Software Encryption: 16th International Workshop.
12. Paulo S. L. M. Barreto (2008-11-25). "The WHIRLPOOL Hash Function". Retrieved 2017-03- 03.
13. Saarinen, M-J; Aumasson, J-P (November 2015). *The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC)*. IETF. doi:10.17487/RFC7693. RFC 7693. Retrieved 4 December 2015.
14. Joan Daemen and Vincent Rijmen, “The Rijndael Block Cipher,” AES submission available at: http://www.nist.gov/aes.