Proceedings of the 4th National Conference; INDIACom-2010
Computing For Nation Development, February 25 – 26, 2010
Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi

Cryptography and Mathematics

S. A. M Rizvi[1] and **Neeta Wadhwa**[2]
[1,2]Deptt. of Comp. Sc., Jamia Millia Islamia,New Delhi
E-Mail:[1]samsam_rizvi@yahoo.com,[2]neeta.088@gmail.com

ABSTRACT
Research says, By 2010, Business data worldwide are expected to swell to 988 billion gigabytes, up from 161 billion gigabytes in 2006. Credit card numbers, account numbers , personal identification numbers (PINs) and passwords have become like gold in the cybercrime. In USA, more than 162 million records have been reported lost or stolen in 2007, triple the 49.7 million that went missing in 2006.The need of secrecy of information had never been so much concerned, until the evolution of the Internet. Now every secret information is just some clicks away. The increasing need of security of data leads to the new inventions of cryptography. Although , Cryptography is as old as the time when human learned to communicate in written form. But in real sense, Cryptography flourished during the twentieth century only. And The basic foundation of this scientific art is Mathematics. How much field of cryptography is developed, At every step of its development, there lies some simple and complex mathematical concepts. In this paper, we describe the deep relationship between mathematics and cryptography.
This relationship should be introduced even from the high school level. It directs the aptitude of students towards computer, electronics and electrical engineering fields in a right way. Cryptographic algorithms can't be understood without mastering mathematical fundamentals as: functions, fields, modular arithmetic, Boolean algebra etc.Cryptographic fundamentals can be used as illustrative examples for explaining mathematic concepts. It means both are closely related. Thus this paper introduces a new subject called CRYPTOMATH. It will definitely motivates the engineering students of computer, electrical and electronic stream. It also gives the right direction to the student's interest and aptitude.

KEYWORDS
Cryptography, mathematics, classic ciphers , modern ciphers, substitution , permutation.

1. INTRODUCTION

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication [1].Thus Cryptography is an art and science of secret writing. Cryptographer encode the data by doing some simple and complex mathematical computations. The main tool used for encoding data is a cipher. A cipher is a well defined set of some mathematical computations performed on plain text to convert it in to cipher text and vice versa. The general structure of encryption and decryption is given below in fig 1.

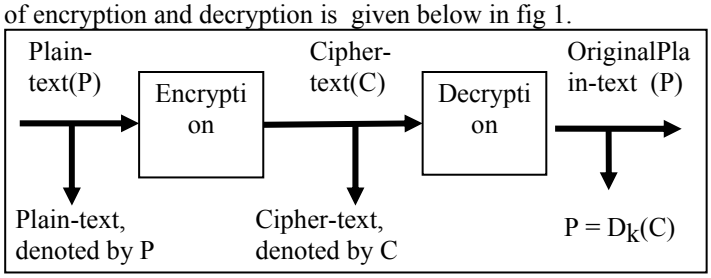

Figure 1: General structure of Encryption

P : a set of possible plaintext
C : a set of possible ciphertext
$C = E_k(P)$, where E is encryption algorithm,
K : the finite set of possible keys.
$P=D_k(C)$, where D is decryption algorithm,
which is reverse of encryption algorithm
Before computers ,encoding was done manually or with simple machines, thus called pen and paper cryptography. The introduction of computers has changed the face of encryption. A typical modern personal computer will be able to perform around 5 billion "operations" per second. This processing power not only proves a boon to encryption as it opens the doors to otherwise long and tedious mathematical calculation, but it is also a threat, providing a resource a hacker could utilise to attempt to break an encryption.

Thus Cryptography can be classified as classical and modern cryptography according to fig 2.

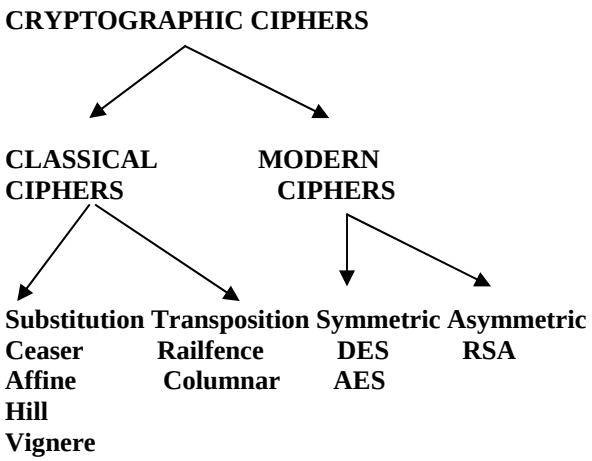

Figure 2: Broad classification of CRYPTOGRAPHY

2. CLASSICAL CIPHERS

The classical ciphers are the basic simplest forms of encryption, they have been around for thousands of years. There are basically two principles that drive all of the classical ciphers: substitution and transposition [2] . These principles are extremely basic at their cores and are simple to understand. And , these principles of substitution and transposition form the basis for many of today's encryption standards. By combining substitution and transposition in creative ways, it is possible to produce extremely secure cryptosystems, which are actually many of our modern encryption ciphers.

2.1 Substitution

Substitution ciphers are those that replace or substitutes symbols in plaintext with another symbols. To reverse the process, each ciphertext symbol is simply replaced with the corresponding original plaintext symbol . In this basic and simple cipher , the very basic mathematic concepts are used : Functions and Modular Arithmetic / Clock Arithmetic / Calender Arithmetic [3].

a. Caeser cipher / Shift cipher

It is named after Julius Caesar, who used it to communicate with his generals. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet

P**:** plain text , C :cipher text , K : key (from fig 1)

P=C=K=Z_{26}(as there are 26 letters in english alphabet).

Encryption : $C=E_K(P)=P+K \bmod 26$

Decryption : $P=D_K(C)=\tilde{C}K \bmod 26$

Where $E_K(P)$ is a one-to-one function, and that $D_K(E_K(P))=P$.

b. Affine cipher

It is a monoalphabetic substitution cipher and it can be the exact same as a standard Caesarian shift when "a" is 1. It is based on the concept of Affine functios [3].

Encryption: $C = E_k(P) = aP + b \pmod{26}$, K = a, b.

Decryption: $P = D_k(C) = (c - b)\, a^{-1} \pmod{26}$,

If and if gcd(a, 26) = 1.(gcd is greatest common divisor)

c. Vignere Cipher

The **Vigenere Cipher** is named after Blaise de Vigenere (1523-1596),a french diplomat and cryptographer. It is a polyalphabetic substitution cipher, in it the letters are replaced by some other letters of the alphabet [4]. The difference to Caesar Cipher is that not all letters are replaced using the same shift in the alphabet. It is a polyalphabetic cipher which maps one letter to many other letters. The Vegenere Cipher is a collection of 26 permutations, represented in a 26 * 26 matrix. All 26 letters are shown in each row and each column.

If K = alphabetic string of length m alphabets as (k1,k2,k3,…,km).

P= m characters at a time as (x1, x2, x3,…….,xm) then

Encryption : $C= E_k(x1,x2,\ldots\ldots, xm) = x_i + k_i \pmod{26}$

Decryption : $P=D_k(c1,c2,\ldots\ldots,cm) = c_i - k_i \pmod{26}$

d. Hill Cipher / Matrix cipher

It was invented in 1929 by Lester S. Hill. It utilises linear algebra [5] over $\mathbf{Z}_{26}$ .The key K is an invertible m×m matrix with entries in $\mathbf{Z}_{26}$, Each string of m characters from the Plaintext is first converted to a sequence x of m numbers in $\mathbf{Z}_{26}$, so x $\in \mathbf{Z}_{26}^{m}$.

Then x is encrypted by multiplying by the matrix K:

Encryption: $C= E_k(P)= PK$

Decryption: $P=D_k(C) = CK^{-1}$

2.2 Transposition

Transposition Ciphers form the second basic building block of ciphers. The core idea is to rearrange the order of basic units (letters/bytes/bits) without altering their actual values. A transposition cipher simply rearranges the symbols in plaintext to produce ciphertext..

Let P=C=K= $(Z_{26})^m$

If K = alphabetic string of length m alphabets as (k1,k2,k3,…,km).

P= m characters at a time as (x1, x2, x3,…….,xm) then

A permutation is defined as follows:

k1(x1)=x3, k2(x2)=x5, k3(x3)=x7,……km(xm)=x1.

Thus we can say (x3,x5,x7,…….x1) is a key

Apermutation can be described in various ways. It can be displayed as above or as an array:

x	1	2	3	4	5	6
k	3	5	1	2	6	4

where the top row in the array is the domain and the bottom row is the image under the mapping. Since permutations are bijections, they have inverses. If a permutation is written as an array, its inverse is easily found by interchanging the rows in the array means decryption can be done easily.

Thus transposition or permutation ciphers are based on **bijective functions** [6].

a. Rail Fence cipher

It encodes a message by reordering the plaintext in some definite way. It write message with letters on alternate rows in which the plain-text is written down as a sequence of diagonals and then read off as a sequence of rows. For eg.:

Plain: G D S N
O I O E

Cipher: GDSNOIOE

b. Columnar Transposition Cipher

It is the scheme to write the message in a rectangle, row by row and read the message off, column by column, but permute

the order of the column. The order of the columns become the key [7].
Example:
plaintext: attack postponed until two am

Key	4	3	1	2	5	6	7
Plain-text:	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ
A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. A single columnar transposition could be attacked by guessing possible column lengths, and then looking for possible anagrams. This cipher can be made significantly more secure by performing more than one stage of transposition. The same key can be used for all transpositions, or different keys can be used.

3. MODERN CIPHERS

The era of modern ciphers starts actually when the IBM's design named LUCIFER [8] evolved as a first encryption standard and NIST approved it as a DES (Data Encryption Standard) in 1977 [9]. Where Classic ciphers were based on the principles of substitution and permutation, Modern ciphers are product ciphers means they are the complex and creative combinations of substitution and permutations. To explain these ciphers, the concept of Composition functions is used .Compositions are a convenient way of constructing more complicated functions from simple functions.

3.1 Symmetric ciphers

In these ciphers same key is used for encryption and decryption as

$C = E_k(P)$

$P = D_k(C)$

k is same in both processes.

a. DES (Data Encryption Standard)

DES was developed at IBM, based on LUCIFER.DES was first published in the Federal Register of March 17, 1975. After a considerable amount of public discussion, DES was adopted as a standard in 1977. It is a block cipher ,encrypts 64 bits at a time with key length of 56 bits .

$$\text{DES}: \{0,1\}^{56} \times \{0,1\}^{64} \rightarrow \{0,1\}^{64}$$
$$\text{DES}^{-1}: \{0,1\}^{56} \times \{0,1\}^{64} \rightarrow \{0,1\}^{64}$$

4 step Encryption process of DES is as follows:
1. It is a Transposition cipher.
2. Step 2 accepts as input a 64-bit string L,R (where each of L, R is a 32-bit string) and outputs R, L.
3. Step 3 is a `standard round ' having 16 rounds that accepts as input $L_{i-1}$, $R_{i-1}$ and outputs $L_i$, $R_i$ (where each of $L_{i-1}$, $R_{i-1}$, $L_i$, $R_i$ is a 32-bit string ,where i lies ,$2 < i < 17$). Stage i is rather like Step 2 with a `twist' using a function f that does not depend on i, but on a 48-bit key K_i that depends on i: $L_i = R_{i-1}$, but R_i is the sum of L_{i-1} (+) $f(R_{i-1}, K_i)$.
4. It is the inverse of Step 1.
The function f used is basically a product cipher of substitution (using s-boxes) and permutation (p-boxes) ciphers.

b. AES (Advanced Encryption Standard)

AES is a block cipher, designed by Joan Daemen and Vincent Rijmen. It has a variable block length (128-256 bits)and key length (128-256 bits) [10].
There are basically Four stages in its each round :
Substitute (confusion) "S-box"
Shift (diffusion)
Mix (diffusion)
Add key
Finite fields and Polynomial Modular Airthmetic [11] over Galois field (GF) are the main concept used in them. A Galois field is defined as any finite set satisfying the axioms of a field, and is denoted by GF(q), where $q \in N$. The finite Field $GF(2^8)$ consists of the $2^8 = 256$ different numbers (0…255) represented by one byte (8 bits) and it actually doing arithmetic with polynomials of order 8.
Mathematic background of each step is :

- The *SubBytes* is a transformation which actually is the composition of the following two functions:
  a. Inversion $GF(2^8) \rightarrow GF(2^8)$: $x \rightarrow (0,$ if $x=0$ and x^{-1} otherwise)
  b. Affine-linear transformation $x \rightarrow Mx + b$
  where M is an element of $GL(8,GF(2))$ and b is a byte, represented as 8 bit vector. The specific values of M and b can be found in the Rijndael specification
- The ShiftRows is very easy operation . It shifts every row of the current state cyclically by 0, 1, 2 and 3 positions to the left to attain good dffusion / permutaion.
- In The *MixColumns* operation single byte-byte multiplication is performed by the rules of finite field multiplication in $GF(2^8)$.
- The *Addkey* operation simply adds the key to the text with the simple XOR operation.

3.2 Asymmetric Ciphers

In these ciphers , a pair of keys (public key and private key) is used , one is for encryption and other is for decryption.

$C = E_{k1}(P)$

$P = D_{k2}(C)$

a. RSA

RSA Encryption is a asymmetric encryption scheme ,where "RSA" are the initials of the three creators: "Rivest, Shamir, and Adleman". It is based on the following idea that , It is very simply to multiply numbers together, especially with computers. But it can be very difficult to factor numbers [12].
If e = public key, n = product of any two large primes r and s , d = private key

Encryption: $C = E(P) = P^e \bmod n$

Decryption: $P = D(C) = C^d \bmod n$

4. CONCLUSION AND FUTURESCOPE

Cryptography is an ancient subject that has changed a lot throughout the years. At one time the subject was mainly a linguistic one, the key concern was the ability to recognize words and make words unrecognizable with a simple cipher. But Today, scenario has changed and in this computerized era, the subject is very much mathematical. All the ciphers whether classic or modern based on mathematic concepts. So In modern times, cryptography is considered to be a branch of both mathematics and computer science. As we see many of the basic mathematic concepts relying behind ciphers, are of high school level , Cryptography should be introduced at high school level mathematics in its Application domain.. Because interest in math can be a key to develop cryptographic aptitude. Cryptographic systems can prove to be the illustrative and real examples of mathematics concepts as , modular arithmetic, number theory, set theory and their many theorems. In this way students can develop their interest and direct their aptitude in right direction of engineering fields right from the basic level. Thus MATH is a basic tool to learn CRYPTOLOGY and CRYPTOLOGY can be used as a teaching tool to explain MATH. Math lies in understanding domain of Cryptography and Cryptography lies in application domain of Math.

5. REFERENCES

[1]. A. Menezes, P. van Oorschot and S. Vanstone, "*Handbook of Applied Cryptography",* CRC Press, 1996.

[2]. W.Stallings; "Cryptography and Network Security" 2nd Edition, Prentice Hall,1999

[3]. R.G. Ayoub, " An Introduction to the Theory of Numbers*"*, Providence, RI: American Mathematical Society, 1963

[4]. Mao, W., "Modern Cryptography: Theory & Practice*",* Upper Saddle River, NJ: Prentice Hall PTR, 2004.

[5]. I. C. Smith, "Cryptography in the Algebra Class," NCTM Western Regional Conference, Phoenix. AZ. December 3.

[6]. M.W.Baldoni, C. Clliberto, G.M.Piacentini Cattaneo, " Elementary Number Theory, Cryptography and Codes", 2009 Springer-Verlag Berlin Heidelberg.

[7]. Alan G. Konheim, "Computer security and cryptography", Wiley & Sons, Inc. 2007.

[8]. B. Schneier, "Applied Cryptography", second edition. John Wiley & Sons, Inc. New York, 1996.

[9]. National Bureau of Standards, " Data Encryption Standard", U. S. Department of Commerce, FIPS pub.46, January 1997.

[10]. FIPS 197, "Advanced Encryption Standard," Federal Information Processing Standard (FIPS). Publication 197, Nationil Bureau of Standards, ' US**.** Department of Commerce, Washington D.C., November 26 2001.

[11]. Hans Delfs ,Helmut Knebl , "Introduction to Cryptography**,**Principles and Applications" ,Second Edition, springers.

[12]. D. R. Stinson. "Cryptography, Theory and Practice". Second edition. Chapman & WalllCRC Press, 2002.

Continued from Page No. 184

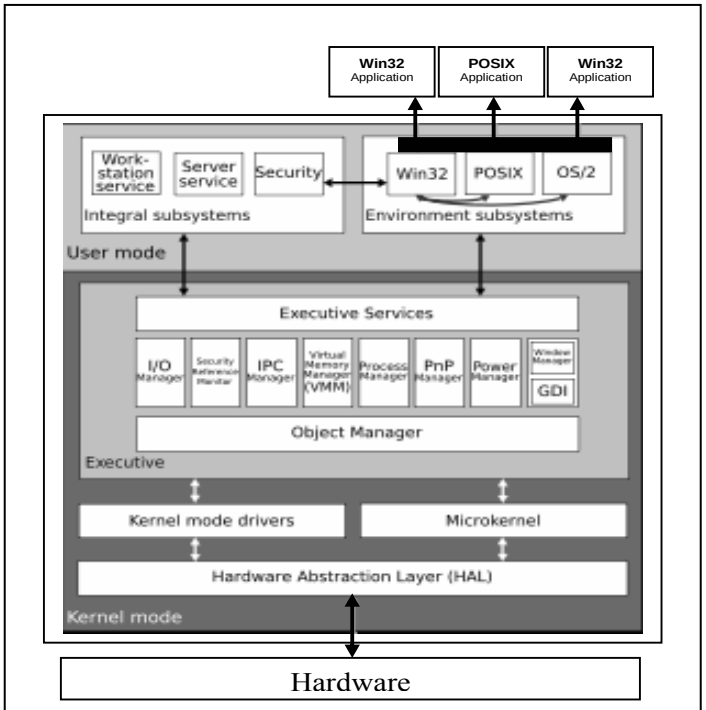

Figure 3: Microsoft Windows XP

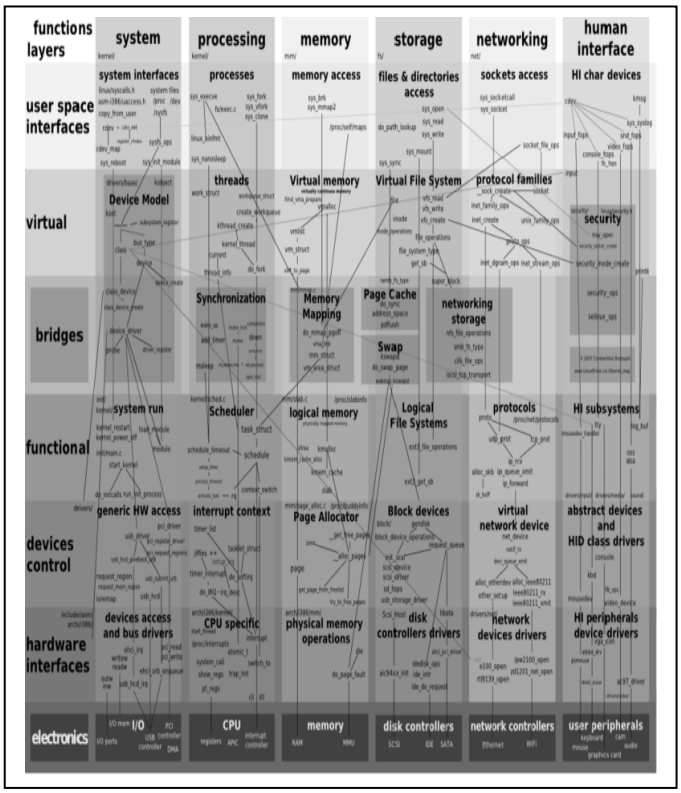

Figure 4: Linux Kernel Architecture