THE ROLE OF MATHEMATICS IN EMERGENCE OF CRYPTOGRAPHY: A REVIEW

Savkirat Kaur

Department of Mathematics, Dev Samaj College for Women, Ferozepur (India)

ABSTRACT

Cryptography is an art of developing techniques of writing messages in a secret way and ensuring the security in communication. Earlier, the use of cryptography was restricted to the safety of information in diplomatic and military areas. With the growth in e-commerce, ATM machines, e-mail and video conferencing through computers, the threat of unauthorized accessibility to the data became a serious concern. So, in order to secure the stored data and to communicate safely the need was to develop economical, efficient and safe cryptography systems. The intent of this paper is to discuss how mathematics plays a significant role in developing various techniques of cryptography.

***Keywords**: Ciphertext, Cryptography, Decryption, Encryption, Plaintext*

I. INTRODUCTION

The term Cryptography, coined from the Greek language, is collaboration of two words 'kryptos'- ‘hidden’ and 'graphein'- ‘to write’. Cryptography came into picture when the use of physical locks was abandoned in communication. The first recorded use of cryptography comes from Julius Caesar, a Roman army commander, around 50 B.C [1]. Some of the important terms related to cryptography are following:

Encryption**:** Encryption is part of cryptography used to hide information by converting it into an illegible code. It uses a particular parameter or key to perform the information conversion. Decryption is the reverse of encryption.

Plaintext: It is the information to be encrypted.

Ciphertext: It is the output of the encryption.

Cipher: Cipher is an algorithm used for encrypting and decrypting messages. It is the set of transformations to convert plaintext into ciphertext. Cipher can be thought of as the virtual lock.

Cryptanalysis: The art of interpreting secret messages and discovering the method used for cryptography is called cryptanalysis. It exposes the drawbacks in existing cryptography systems. Cryptographers invent hidden codes and cryptanalysts try to break these codes [2].

II. ANCIENT CRYPTOGRAPHY TECHNIQUES

2.1 Caesar Cipher

Julius Caesar solved the problem of secure communication with his army. He shifted each letter of his military commands to make the message meaningless [3]. Caesar used three ‘3’ as the key to his cipher system. All the alphabets represent one-to-one correspondence with numbers 0 to 25 as below:

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Hence, the mathematical formula used to encrypt plaintext was:

E(n) = (n+ 3) (modulo26) where n is the number corresponding to a plaintext letter.

As 23 is the additive inverse of 3 modulo 26, the formula used to decrypt ciphertext was:

D(c) = (c + 23) (modulo26) where c is the number corresponding to a ciphertext letter.

The reason behind cipher key ‘3’, used by Julius Caesar, is unknown. He could have used any number from 0 to 25. While working in residue class modulo 26, there are 26 different possibilities to the keys where the key 0 does not provide any secrecy. Though Caesar Cipher was one of the easiest cryptography techniques, it provided minimum security to the information because extensive cryptanalysis with 25 non trivial keys could be simply performed [1]. 800 years later, the Arab mathematician, Al-Kindi, broke the Caesar Cipher using the hint of frequency analysis of the letters in any language [4].

2.2 Polyalphabetic Cipher

In the mid of 15th century, Cryptography progressed towards Polyalphabetic Cipher to obtain more security than Caesar Cipher [2]. The objective was to flatten the distribution of letter frequencies which acted as a major breakthrough for Caesar Cipher [5]. Unlike Caesar Cipher, here multiple shifts were used (In Caeser Cipher a single shift key was used). A sequence of n letters was used as a key. This key was repeated several times for encrypting the message. The mathematical formulation was as follows:

The plaintext message can be considered in the form of blocks each of length n. Then the encryption formula becomes:

E_p(c) = (c + k) (modulo 26) where c is the number corresponding to the plaintext letter, p is the position of the plaintext letter in the block of n letters and k is the number corresponding to the p^{th} keyword letter. Clearly 1 ≤ p ≤ n. This method is repeated across the plaintext message. Using this logic one can also build a program in computer to make the encryption easier [1].

Polyalphabetic Cipher provided more secrecy than Caesar Cipher because a particular plaintext letter was always represented by a different ciphertext letter whereas in Caesar Cipher a plaintext letter was represented by the same ciphertext letter each time. The polyalphabetic cipher had $(26)^n$ possible keys for key length n.

2.3 One-time Pad

Polyalphabetic Cipher continued for almost 400 years. In 1882, Frank Miller invented cipher called as One-time Pad [6]. In One-time Pad, a key was selected whose length was same as that of the plaintext message [7], [8]. The shifts in the plaintext never followed a repetitive pattern and the encrypted message had uniform frequency distribution, thereby providing no leakage of the information. The number of possible keys was $(26)^n$ so this cipher was theoretically unbreakable for large values of n.

This technique of cryptography provided a high level of security but the disadvantage was that to communicate, both the sender and the receiver of a message must share the same keyword. How is it possible if they do not know each other? This question posed a new problem for the cryptographers.

III. MODERN CRYPTOGRAPHY TECHNIQUES

3.1 Public Key Cryptosystems

With the advancement of internet in 20^{th} century, the need of cryptography became public. So, the aim was to develop a technique which would not need the two parties to share the secret key.

3.1.1 Diffie-Hellman Key Exchange: In 1976, Whitfield Diffie and Martin Hellman proposed a new technique called as Public key cryptosystem [2]. They devised an amazing trick to produce a one-way function that was easy on the one side and difficult on the other side. The mathematical method that served their purpose was modular arithmetic. Given a generator ‘g’, an exponent ‘e’ and prime modulus ‘p’ it is easy to calculate x (an integer between 0 to p-1):

$$g^{e} \text{ modulo } p \equiv x$$

But it is very difficult to calculate exponent ‘e’ when g, p and x are given:

$$g^{?} \text{ modulo } p \equiv x$$

This problem is called Discrete Logarithm problem. The potency of this one way function depends upon the time needed to reverse the discrete algorithm problem. For 100 digits long prime modulus it is practically impossible to evaluate the exponent ‘e’. First the two parties share the prime modulus ‘p’, generator ‘g’ publically and keep their individual exponents e and e' as their secret keys. The first party evaluates:

$$g^{e} \text{ mod } p \equiv x \text{ (say)}$$

and sends x publically to the second party. The second party uses his secret key e' to evaluate:

$$g^{e'} \text{ mod } p \equiv x' \text{ (say)}$$

and sends x' publically to the first party. Now, both the parties do following calculations:

First party: $(x')^{e}$ mod p

Second party: $(x)^{e'}$ mod p

which are the same numbers modulo p. This way they shared the same public key without knowing each other [9]. While maintaining the same level of security, the public key cryptosystem solved the problem of huge key management in One-time pad system.

3.1.2 RSA Encryption: In 1977, Ronald L. Rivest, Adi Shamir and Leonard Adelman implemented the Diffie-Hellman system, using the elementary concepts of number theory. The mathematical formulation was:

If m is the plaintext message and e is the public exponent, it is easy to calculate the ciphertext message c using:

$$m^{e} \text{ mod } n \equiv c \text{ where n is any random number.}$$

Given c, e and n it is difficult to calculate m. So, this is the required one way function that is easy to perform and difficult to reverse. Some piece of information ‘d’, called as trapdoor, is required to reverse the encryption as:

$$c^{d} \text{ mod } n \equiv m$$

So, $$m^{e*d} \text{ mod } n \equiv m \qquad (1)$$

Now, the task is to find d.

It is easy to multiply two prime numbers and quite hard to factorize a given number into prime factors. To make this encryption possible the work done by Swiss mathematician, Leonard Euler, was used. The trick was to use a function that depends upon the prime factorisation of n. Euler's totient function Φ served the purpose. If n = p × q, then Φ being multiplicative function, Φ(n) = (p-1)(q-1). Euler's theorem was used to connect Φ function to modular exponentiation (1) as follows:

$$m^{\Phi(n)} \equiv 1 \text{ mod } n; \text{ where m and n are co-prime.}$$

$$m^{k^{*}\Phi(n)} \equiv 1 \text{ mod } n; \text{ where k is any number.}$$

$$m^{1+k^{*}\Phi(n)} \equiv m \text{ mod } n \qquad (2)$$

From (1) and (2), the derived equation was:

$$e * d = 1+k^{*}\Phi(n)$$

$$d= \frac{1+k^{*}\Phi(n)}{e}$$

Now the person who knew the prime factorisation of n could solve $\Phi(n)$ easily and further calculate d. Without knowing the prime factorisation of n it was very difficult and time consuming to find the trapdoor information d. To ensure the security of RSA encryption system p and q must be 100 digit long primes or even more than that [10], [11].

3.2 Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is a move towards the encryption that uses the nature of elliptic curves in finite fields. ECC utilizes the methods of Diffie-Hellman Key Exchange and RSA Encryption. The only difference is that in ECC, the prime numbers are selected with the help of elliptic curve in a finite field. The advantage of this usage is that key sizes may become smaller while maintaining the same level of security. This provides more efficient cryptography method [2].

IV. CONCLUSION

The current research reveals that cryptology and coding theory are related. The symmetric block cipher standard AES and some hash functions are linked with MDS codes and special codes of coding theory. The major fields of mathematics like number theory, field theory and coding theory play an important role in cryptology. A thorough understanding of cryptography is required to develop better ways to protect valuable information as technology becomes faster and more efficient.

REFERENCES

1. Dennis Luciano, and Gordon Prichett, Cryptology: From Caesar Ciphers to Public-Key Cryptosystems, *The College Mathematics Journal, 18(1)*, 1987, 2-17.

2. Nicholas G. McDonald, *A research review: Past, Present and Future Methods of Cryptography and Data Encryption* (University of Utah).

3. A. Sinkov, Elementary Cryptanalysis-A Mathematical Approach, *New Mathematical Library, 22,* Mathematical Association of America, 1966.

4. Simon Singh, *The Code Book* (2000, 14-20).

5. W. Francis, *A Standard Sample of Present-Day Edited American English for Use with Digital Computers* (Linguistics Department, Brown University, 1964).

6. John Markoff, *Codebook Shows an Encryption Form Dates Back to Telegraphs* (New York Times).

7. C. H. Meyer and S. M. Matyas, *Cryptography: A New Dimension in Computer Data Security* (Wiley-Interscience, New York, 1982).

8. C. E. Shannon, Communications Theory of Secrecy Systems, *Bell Sys. Tech. Journal, 28,* 1949, 656-715.

9. Diffie W, Hellman M, *New Directions in Cryptography*, Stanford University, 1976, 40.

10. R.L.Rivest, A. Shamir, and L.Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* (Laboratory for Computer Science, M.I.T., LCS/TM-82, 1977).

11. R.L.Rivest, A.Shamir, and L.Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Communications of the ACM, 21(2),* 1978, 120-126.