JAYOTI VIDYAPEETH WOMEN'S UNIVERSITY, JAIPUR
Government of Rajasthan established
Through ACT No. 17 of 2008 as per UGC ACT 1956
NAAC Accredited University

**Faculty of Education and methodology**

**Department of Science and Technology**

**Faculty Name**- Jv'n Narendra Kumar Chahar (Assistant Professor)

**Program**- B.Tech 8thSemester

**Course Name**– Cryptography and Network Security

**Session no.**: 23

**Session Name-** ElGamal

Academic Day starts with –

- Greeting with saying **'Namaste'** by joining Hands together following by 2-3 Minutes Happy session, Celebrating birthday of any student of respective class and **National Anthem**.

Lecture starts with- quotations' answer writing

Review of previous Session **– RSA and the Chinese Remainder Theorem**

Topic to be discussed today- Today We will discuss about **ElGamal**

Lesson deliverance (ICT, Diagrams & Live Example)-

- Diagrams

Introduction & Brief Discussion about the Topic**– ElGamal**

# ElGamal

A variant of the Diffie-Hellman key distribution scheme, allowing secure exchange of messages, it was originally published in 1985 by ElGamal and it is like Diffie-Hellman its security depends on the difficulty of factoring logarithms.

**Key Generation**

select a large prime p (~200 digit), and $\alpha$ a primitive element mod p

A has a secret number $X_A$

B has a secret number $X_B$

A and B compute $Y_A$ and $Y_B$ respectively, which are then made public

$$Y_A = ( \alpha ) ^{X_A} \bmod p$$

$$Y_B = ( \alpha ) ^{X_B} \bmod p$$

to encrypt a message M into ciphertext C, selects a random number k, 0 <= k <= p-1 and

computes the message key K

$$K = (Y_B)^K \bmod p$$

computes the ciphertext pair: $C = \{C_1, C_2\}$

$$C1 = ( \alpha )^K \bmod p$$

$$C2 = K.M \bmod p$$

to decrypt the message

extracts the message key K

$$K = (C1) ^{X_B} \bmod p$$

$= (\alpha)^{K}.X_B \bmod p$

extracts M by solving for M in the following equation:

$C2 = K.M \bmod p$

**Other Public-Key Schemes**

A number of other public-key schemes have been proposed, some of the better-known being:

- Knapsack based schemes
- McEleice's Error Correcting Code based schems

ALL of these schemes have been broken.

The only currently known secure public key schemes are those based on exponentiation (all of which are patented in North America). It has proved to be very difficult to develop secure public key schemes and this in part is why they have not been adopted faster, as their theoretical advantages might have suggested.

## Reference-

1. **Book:** William Stallings, “Cryptography & Network Security”, Pearson Education, 4th Edition 2006.

**QUESTIONS: -**

**Q1. Explain ElGamal key generation.**

**Q2. List other algorithms that are based on PKI.**

Next, we will discuss more about Authentication requirements.

.

- Academic Day ends with-
  National song ‘Vande Mataram’