NIS LAB7

Prof. Mrudang T. Mehta
Associate Professor
Computer Engineering Department
Faculty of Technology,
Dharmsinh Desai University, Nadiad

- Write a program to implement Elgamal Cryptosystem.
  - Function to create Primitive root for the given Multiplicative Group
  - Key Generation
  - Encryption
  - Decryption

- Primitive Root
- Find the primitive roots for $\langle Z^*_7, x \rangle$
- $Z^*_7 = \{ 1,2,3,4,5,6\}$
- $\phi(7) = 6$

Mod 7

	i=1	i=2	i=3	i=4	i=5	i=6
a=1	1	1	1	1	1	1
2	2	4	1	2	4	1
3	**3**	**2**	**6**	**4**	**5**	**1**
4	4	2	1	4	2	1
5	**5**	**4**	**6**	**2**	**3**	**1**
6	6	1	6	1	6	1

- Ord(1)=1
- Ord(2)=3
- **Ord(3)=6**
- Ord(4)=3
- **Ord(5)=6**
- Ord(6)=2

- 3 and 5 are primitive roots. (Generator for the group)

Key Generation

1. Select P (Very large prime number)
2. Select e_1 (primitive root) of the group $<Z^*_p, x>$
3. Select d to be a member of the group $G= <Z^*_p, x>$ such that $1<=d<=p-2$
4. $e_2 = e_1^d \bmod p$
5. Public key: $(e_1, . e_2, p)$
6. Private key= d

Encryption

Elegamal_Encryption (M, $e_{1,}$. $e_{2,}$ p)

{

$c_1 = e_1^r \bmod p$ r is random number from group G= $<Z^*_p, x>$

$c_2 = (e_2^r \times M) \bmod p$

}

Decryption

Elegamal_decryption(c_1,c_2, d, p)

{

$M = [c_2 \times (c_1^d)^{-1}] \bmod p$

}