Cryptography
for IT 7th Sem Students

Developed and Presented By:

Dileep Kumar Yadav

Assistant professor

Dept. of CSE

V.B.S PU,Jaunpur

Mb. No.8726943272

Email-dileep1482@gmail.com

Types of Cryptography

- Symmetric Key Cryptography
- Asymmetric Key Cryptography

Symmetric Key Cryptography

- If the same key is used for encryption and decryption process then it is called symmetric key cryptography.
- There are some techniques by which we can encrypt or decrypt the message like:
- DES,IDEA,RC5,BLOWFISH AND AES and so on.

Minimum Size of Key

- Minimum size of key=1 bit=0 or 1

2 bit= 2^2=4=00,01,11,10

4 bit= 2^4=16

16 bit=2^16=64 k= 65536 NS

=65536/10^9

=near about 1 sec(less than)

32 bit= 2^32=2^16×2^16=65536×65536 ns

=near about 4.2 sec

64 bit=2^64=2^32 × 2^32 ns

=584.46 years

=nearly 600 years

How to Exchange the Key Safely
Diffie- Hellman Key Exchange Algorithm

- Firstly Alice and Bob agree on two large prime no. **n** and **g**. These two integers need not be kept secret. Alice and Bob can use an insecure channel to agree on them.
- Alice choose another large number x and calculate A such that:

$$A=g^x \bmod n$$

- Alice sends the number A to Bob.
- Bob independently choose another large random integer y and calculate B such that:

$$B=g^y \text{ mode } n$$

Cont…

- Bob sends the number B to Alice.
- Now A computes the secret key k1 as follows:

$$k1= B^x \bmod n$$

- Now B computes the secret key k2 as follows:

$$k2=A^y \bmod n$$

- So if k1=k2=k then we follow this algorithms

Example

- For example let n=11,g=7 and x=3,y=6 calculate A,B and k1,k2.
- Here n=11,g=7
- A=g^x mod n

  =7^3 mod 11

  =343 mod 11

  =2
- Alice sends the 2 to Bob.

Cont…

- B=g^y mod n

  =7^6 mod 11

  =117649 mod 11

  =4
- Bob sends 4 to Alice.
- K1=B^x mod n

  =4^3 mod 11

  =9

Cont..

- K2=A^Y mod n

  =2^6 mod 11

  =64 mod 11

  =9

- So k1=k2=9

Problem of Diffie Algorithms

- Number of keys as well as key exchange.
- Expensive in complexity like time and space complexity.
- Man in the middle attack.

Man in the Middle Attack

Alice	Tom	Bob
n=11,g=7	n=11,g=7	n=11,g=7
x=3	x=8,y=6	y=9
A=g^x mod n	A=g^x mod n	A=g^x mod n
=7^3 mod 11	=7^8 mod 11	=7^9 mod 11
=343 mod 11	=5764801 mod 11	=4035360 mod11
A = 2	A = 9	A = 8
	B=g^ mod n	
	=7^6 mod 11	
	=117649 mod 11	
	B = 4	

Cont…

- Alice Tom Bob

A=2

A=9

B=8

B=4

- A=2,B*=4 A=2,B=8 A*=9,B=8
- K1=B^x mod n K1=B^x mod n K2=A^y mod n

  =4^3 mod 11 =8^8 mod 11 =9^9 mod 11

Cont…

- Alice Tom Bob

=64 mod 11 =16777216 mod 11 =387420489 mod11

A= 9 = 5 = 5

k2=A^ mod 11

=2^6 mod 11

= 64 mod 11

= 9

Reference

- Cryptography and network security “Atul Kahate” 3e,Mc Graw hill education.