

Cryptography

for IT 7th Sem Students

1

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

2

- Symmetric Key Cryptography
- Asymmetric Key Cryptography

Symmetric Key Cryptography

3

- 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

4

- 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= $2^{32}=2^{16} \times 2^{16}=65536 \times 65536$ ns
 - =near about 4.2 sec
 - 64 bit= $2^{64}=2^{32} \times 2^{32}$ ns
 - =584.46 years
 - =nearly 600 years

How to Exchange the Key Safely

Diffie- Hellman Key Exchange Algorithm

5

- 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:

$$A = g^x \text{ mod } n$$

- 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...

6

- Bob sends the number B to Alice.
- Now A computes the secret key k_1 as follows:
$$k_1 = B^x \text{ mod } n$$
- Now B computes the secret key k_2 as follows:
$$k_2 = A^y \text{ mod } n$$
- So if $k_1 = k_2 = k$ then we follow this algorithms

Example

7

- For example let $n=11, g=7$ and $x=3, y=6$ calculate A, B and k_1, k_2 .
- Here $n=11, g=7$
- $A = g^x \text{ mod } n$
 $= 7^3 \text{ mod } 11$
 $= 343 \text{ mod } 11$
 $= 2$
- Alice sends the 2 to Bob.

Cont...

8

- $B = g^y \pmod n$
 $= 7^6 \pmod{11}$
 $= 117649 \pmod{11}$
 $= 4$
- Bob sends 4 to Alice.
- $K1 = B^x \pmod n$
 $= 4^3 \pmod{11}$
 $= 9$

Cont..

9

- $K_2 = A^Y \text{ mod } n$
 $= 2^6 \text{ mod } 11$
 $= 64 \text{ mod } 11$
 $= 9$
- So $k_1 = k_2 = 9$

Problem of Diffie Algorithms

10

- 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

11

• Alice

$$n=11, g=7$$

$$x=3$$

$$\begin{aligned} A &= g^x \pmod n \\ &= 7^3 \pmod{11} \\ &= 343 \pmod{11} \end{aligned}$$

$$A = 2$$

Tom

$$n=11, g=7$$

$$x=8, y=6$$

$$\begin{aligned} A &= g^x \pmod n \\ &= 7^8 \pmod{11} \\ &= 5764801 \pmod{11} \end{aligned}$$

$$A = 9$$

$$\begin{aligned} B &= g^y \pmod n \\ &= 7^6 \pmod{11} \\ &= 117649 \pmod{11} \end{aligned}$$

$$B = 4$$

Bob

$$n=11, g=7$$

$$y=9$$

$$\begin{aligned} A &= g^x \pmod n \\ &= 7^9 \pmod{11} \\ &= 4035360 \pmod{11} \end{aligned}$$

$$A = 8$$

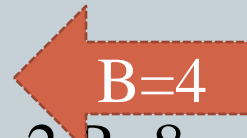
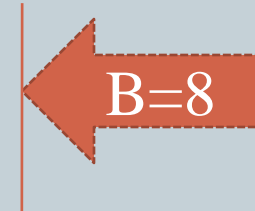
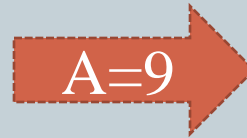
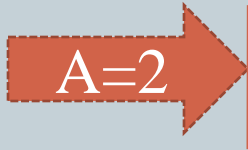
Cont...

12

• Alice

Tom

Bob



• $A=2, B^*=4$

$A=2, B=8$

$A^*=9, B=8$

• $K1 = B^x \text{ mod } n$
 $= 4^3 \text{ mod } 11$

$K1 = B^x \text{ mod } n$
 $= 8^8 \text{ mod } 11$

$K2 = A^y \text{ mod } n$
 $= 9^9 \text{ mod } 11$

Cont...

13

• Alice

$$=64 \text{ mod } 11$$

$$A = 9$$

Tom

$$=16777216 \text{ mod } 11$$

$$= 5$$

$$k_2 = A^6 \text{ mod } 11$$

$$= 2^6 \text{ mod } 11$$

$$= 64 \text{ mod } 11$$

$$= 9$$

Bob

$$=387420489 \text{ mod } 11$$

$$= 5$$

Reference

14

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