CS & IT ENGINEERING

Computer Networks

Network Security

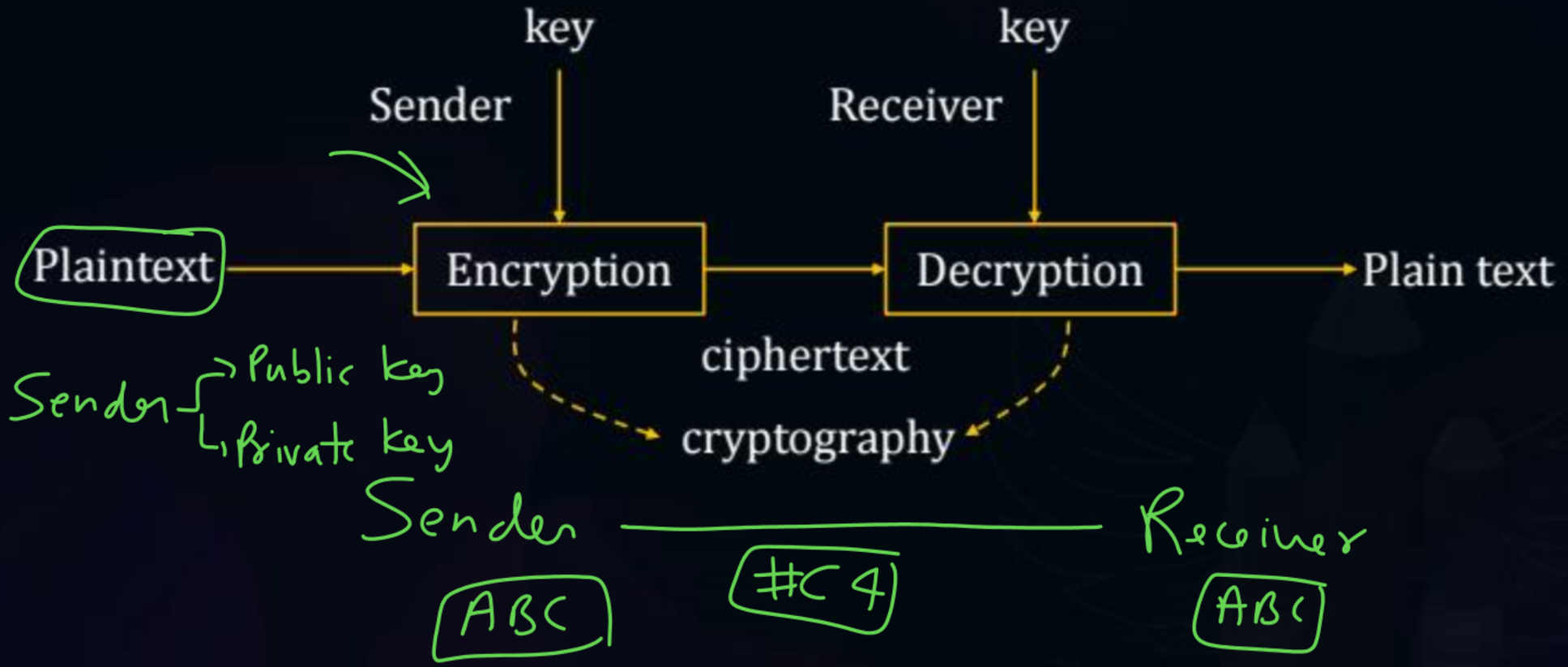
Lecture No.- 01

By- Devvrat Tyagi Sir

Topics to be Covered

- **Topic** Cryptography/Steganography
- **Topic** RSA Algorithm
- **Topic** Diffie-Hellman Algorithm

Topic : Security

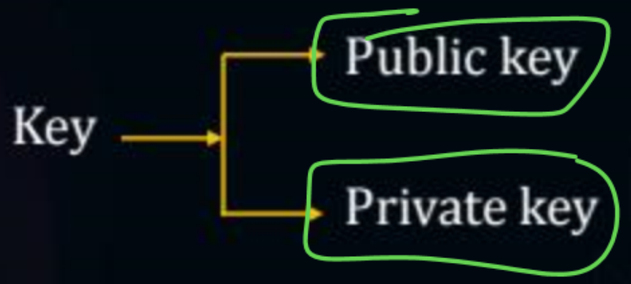


Topic : Network Security

e → public key
d → private key

Cryptography: cryptography is a science or art of converting of one form of data into other form for providing security to the data.

Steganography: is to hide the data behind an image or a video.



Sender & Receiver will have their own Private and public key.

- If the key in transmitted on the channel and letter used for encryption or decryption it is known as public key.
- If the key is kept as secret and letter used for encryption or decryption it is known as private key.

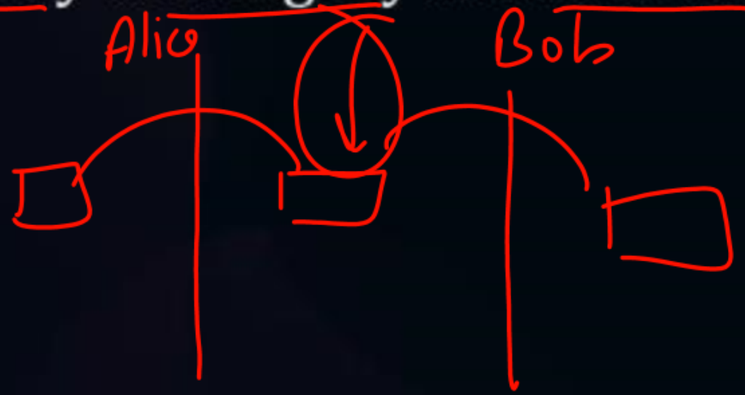
Topic : Network Security

Challenges of Cryptography

(i) Authentication

(ii) Confidentiality

- Providing security to a data or a system is known as confidentiality
- Providing users identity or integrity of the user is known as authentication.



Topic : Network Security

- An symmetric key cryptography both encryption and decryption are done with same key $\left(\frac{n(n-1)}{2}\right)$
- An Asymmetric key cryptography both encryption and decryption are done with different keys (2n).

Topic : Network Security

Key feature of cryptography

(i) Prime numbers

- Prime number will play the major role in cryptography because the number can not be gassed easily.

(ii) Random numbers

- Random number will also will play the major role

Ex. OTP, ATM Pin number.

(iii) Key

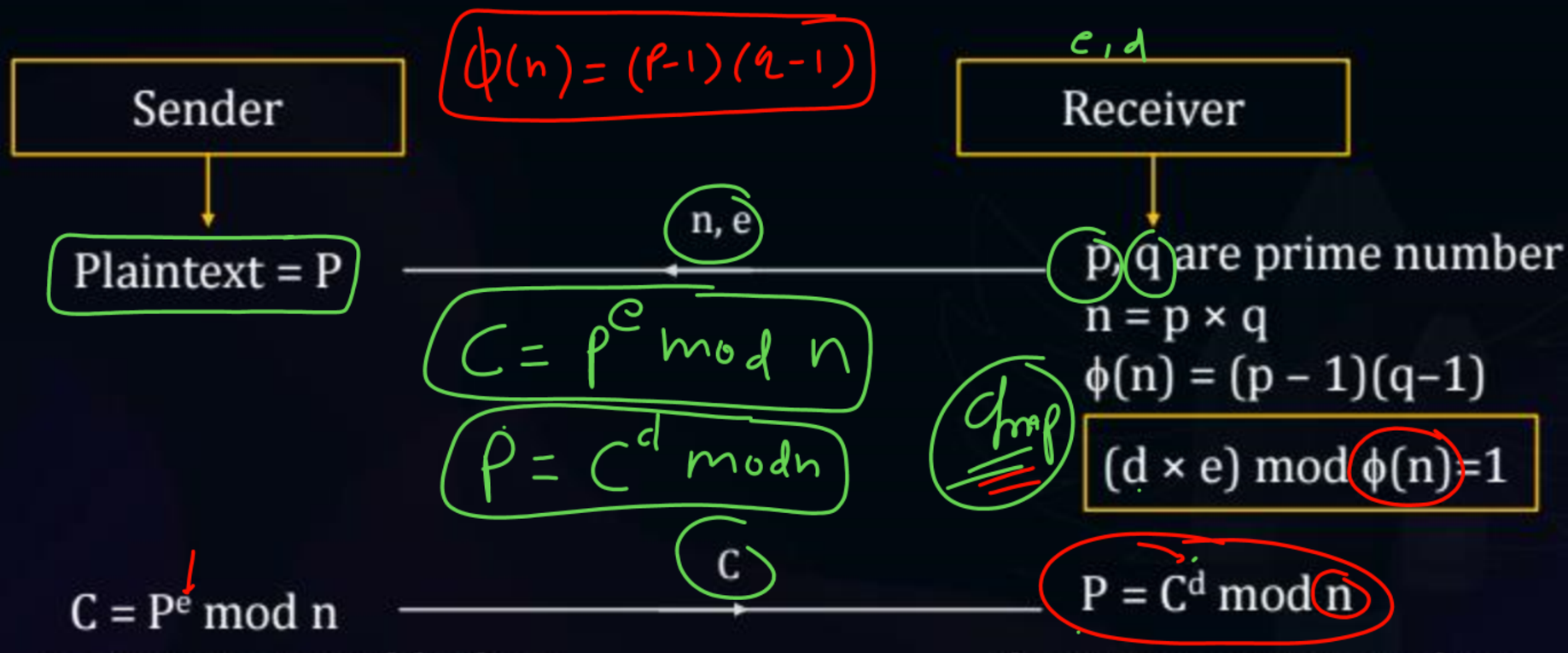
- Public key
- Private key

Topic : Network Security

Key feature of cryptography

(iv) Timestamp

: RSA Algorithms:



Topic : Network Security

e ⇒ public key
d ⇒ private key

- The design of RSA algorithm is to take two prime numbers p & q and generate two key values d & e.
- RSA algorithm also known as asymmetric key cryptography because different keys are used for encryption and decryption.

Note:

If sender is encrypted with Receiver public key and receiver is decrypted with its own private key it is used to provide confidentiality.

Topic : Network Security

- If receiver is encrypted with Sender public key and sender is decrypted with its own private key it is used to provide confidentiality.

- In the RSA algorithm of key generation only one system is involved.

Topic : Network Security

Q. In a RSA cryptosystem, a participant A uses two prime numbers p=13 and q=11 to generate his public and private keys. If the public key of A is 37, then the private key of A is ____ ?

A. 13 Prime no.
B. 35
C. 17 P.N.
D. 11 P.N.

$p = 13$
$q = 11$
$e = 37$

$n = p \times q$

$\phi(n) = (p-1)(q-1) = 12 \times 10 = 120$

formula: $(d \times e) \bmod \phi(n) = 1$

$(d \times 37) \bmod 120 = 1$

$\Rightarrow (13 \times 37) \bmod 120$

$\Rightarrow 481 \bmod 120$

$\Rightarrow 1$

$=$

Topic : Network Security

Q. In a system an RSA algorithm with p=5 and q=ll, is implemented for data security. What is the value of the decryption key if the value of the encryption key is 27?

d

e

d=??

Given: p=5, q=11, e=27

$\phi(n) = (p-1)(q-1)$

$= 4 \times 10 = 40$

A. 3 ✓
B. 7
C. 27
D. 40

formula: $(d \times e) \bmod \phi(n) = 1$

L.H.S: $(d \times e) \bmod \phi(n)$

$= (d \times 27) \bmod 40$

$= (3 \times 27) \bmod 40$

$81 \bmod 40$

$= 1$

Topic : Network Security

Q. Using p = 3, q = 13, d = 7 and e = 3 in the RSA algorithm, what is the value of ciphertext for a plain text 5 ?

A. 8
B. 16
C. 26
D. 33

Given: $p = 3$, $q = 13$, $d = 7$, $e = 3$

$P = 5$

$C = ??$

$n = p \times q$

$= 3 \times 13 = 39$

$$C = P^e \bmod n$$

$= (5)^3 \bmod 39$

$= 125 \bmod 39$

$C = 8$

$39 \overline{)125} (3$
117
8

Topic : Network Security

Q. In the RSA public key cryptosystem, the private and public keys are (d, n) and (e, n) respectively, where n = p*q and p and q are large primes. Besides, n is public and p and q are private. Let M be an integer such that 0 < M < n and f(n) = (p- l)(q-l). Now consider the following equations.

I. $M' = M^e \bmod n$
$M = (M')^d \bmod n$

II. $ed = 1 \bmod n$

III. $ed = 1 \bmod f(n)$

IV. $M' = Me \bmod f(n)$
$M = (M^e)^d \bmod f(n)$

Which of the above equations correctly represent RSA cryptosystem?

A. I and II
B. I and III
C. II and IV
D. III and IV

Topic : Network Security

Q. Suppose that everyone in a group of N people wants to communicate secretly with the N-l others using symmetric key cryptographic system. The communication between any two persons should not be decodable by the others in the group. The number of keys required in the system as a whole to satisfy the confidentiality requirement is _____ .

A. 2N
B. N(N-l)
C. N(N-l)/2
D. (N-l)2

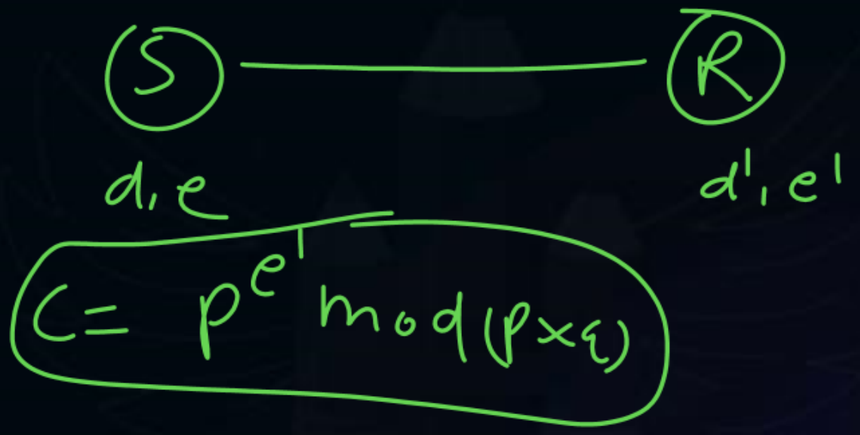
Gate
NIC
ISRO
VGC

Deffie Hellman

Topic : Network Security

Q. A sender is employing public key cryptography to send a secret message to a receiver. Which one of the following statements is TRUE?

A. Sender encrypts using receiver's public key
B. Sender encrypts using his own public key
C. Receiver decrypts using sender's public key
D. Receiver decrypts using his own public key



Topic : Network Security

Q. Anarkali digitally signs a message and sends it to Salim. Verification of the signature by Salim requires

GATE PYQ

A. Anarkali's public key.
B. Salim's public key.
C. Salim's private key.
D. Anarkali's private key.

Topic : Network Security

Q. The minimum positive integer p such that 3^p modulo 17 = 1 is

A. 5
B. 8
C. 12
D. 16

$3^p \bmod 17 = 1$

P:??

$= 3^5 \bmod 17$

$= 3\times3\times3\times3\times3 \bmod 17$

$= 243 \bmod 17$

$= 5$

$3^{16} \bmod 17$

$= 9^8 \bmod 17$

$= 81\times81\times81\times81 \bmod 17$

$\Rightarrow 13\times13\times13\times13 \bmod 17$

$169\times169 \bmod 17$

$16\times16 \bmod 17$

$16\times16 \bmod 17$

$256 \bmod 17$

$= 1$

17)256(15
255
1

$38 \bmod 17$

$\Rightarrow 9^4 \bmod 17$

$\Rightarrow 81\times81 \bmod 17$

$\Rightarrow 13\times13 \bmod 17$

$\Rightarrow 169 \bmod 17$

$\Rightarrow 16\times$

$3^{12} \bmod 17$

$9^6 \bmod 17$

$81\times81\times81 \bmod 17$

$13\times13\times13 \bmod 17$

$169\times13 \bmod 17$

$16\times13 \bmod 17$

$= 4$

Topic : Network Security

#Q. Which one of the following algorithm is not used in asymmetric key cryptography?

A. RSA Algorithm
B. Diffie-Hellman Algorithm
C. Electronic Code Book Algorithm
D. None of the above

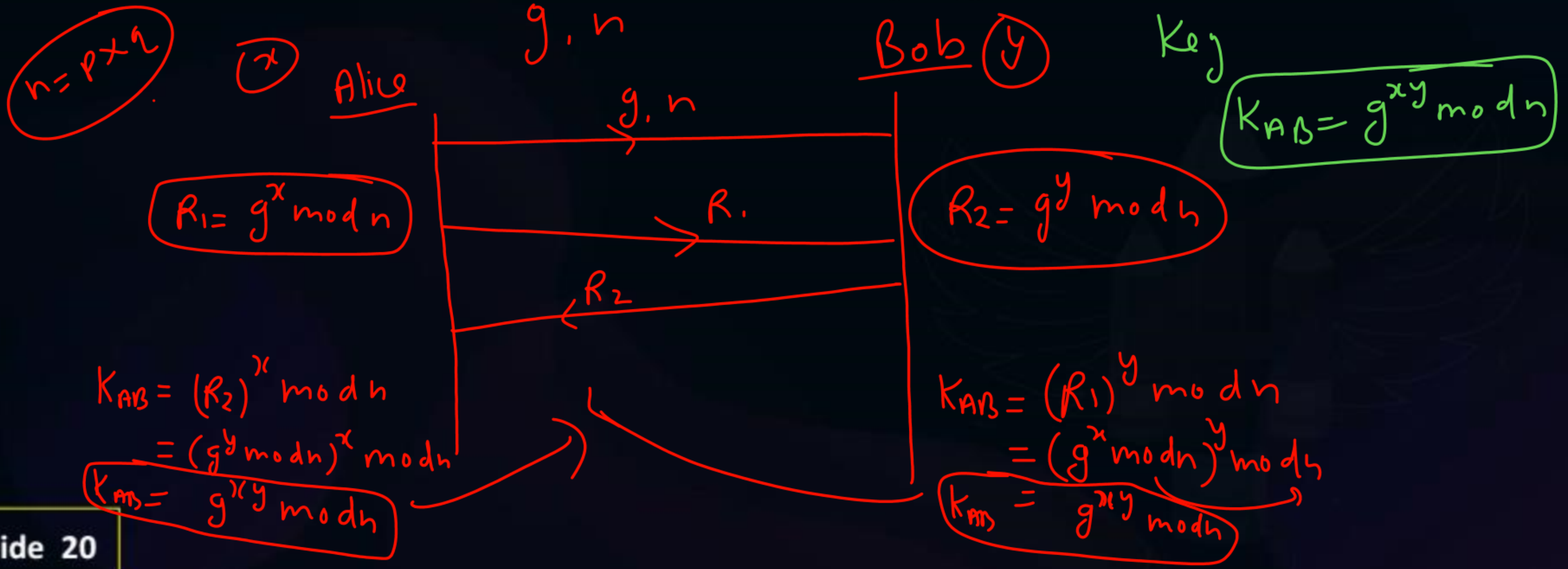
RSA ⇒ Asymmetric

Diffie Hellman

Topic : Network Security

Diffie Hellman key Exchange:

- Diffie Hellman key exchange is also known as symmetric key cryptography because sender side and receiver side same key is generated



Topic : Network Security

Q. The total number of keys required for a set of n individuals to be able to communicate with each other using secret key and public key crypto systems, respectively are:

DH
$\frac{n(n-1)}{2}$

RSA
2n

A. n(n-1)and2n
B. 2n and ((n(n -1))/2)
C. ((n(n -1))/2) and 2n
D. ((n(n -1))/2) and n

THANK - YOU

CS & IT ENGINEERING

Computer Networks

Network Security

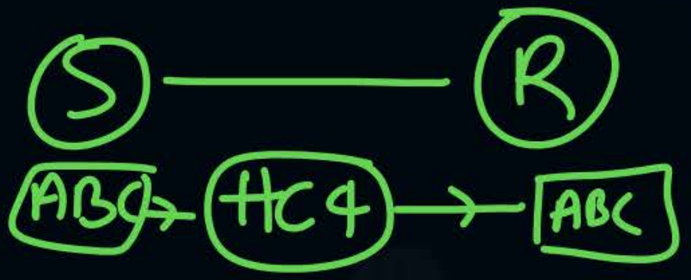
Lecture No.- 02

By- Devvrat Tyagi Sir

Recap of Previous Lecture

Topic Cryptography

Topic RSA algorithm



Topics to be Covered

Topic Public Key Cryptography

Topic Diffie Hellman Key Exchange Algorithm

Topic Questions

Security Services

Secures communications requires the following four basic services:

- **Privacy:** A person (say Rani) should be able to send a message to another person (say Raju) privately. It implies that for all other the message should be unintelligible.
- **Authentication:** After the message is received by Raju, he should be sure that the message has been sent by nobody else but by Rani.
- **Integrity:** Raju should be sure that message has not tampered on transit.
- **Nonrepudiation:** Raju should be able to prove at a later stage that the message was indeed received from Rani.

Public key Cryptography

Asymmetric key cryptography is also called as Public Key cryptography. In public key cryptography, ~~three~~ there are two keys: a private key and a public key. The public key is announced to the public; where as the private key is kept by the receiver.

The sender uses the public key of the receiver for encryption and the receiver uses his private key for decryption.

RSA Algorithm

Alice

Bob

die

d'ie'

$C = P^{e} \bmod n$

$P = C^{d'} \bmod n$

Public key Cryptography

P, C, n

Advantage

- The pair of keys can be used with any other entity
- The number of keys required is small.

Disadvantage

- It is not efficient for long message
- Association between an entity and its public key must be verified.

NOTE: Above theorem is known as asymmetric key cryptography because different keys are used for encryption and decryption.

10x2=20

RSA:

No. of keys gen. = 2n

Diffie Hellman:

No. of keys gen = $\frac{n(n-1)}{2}$

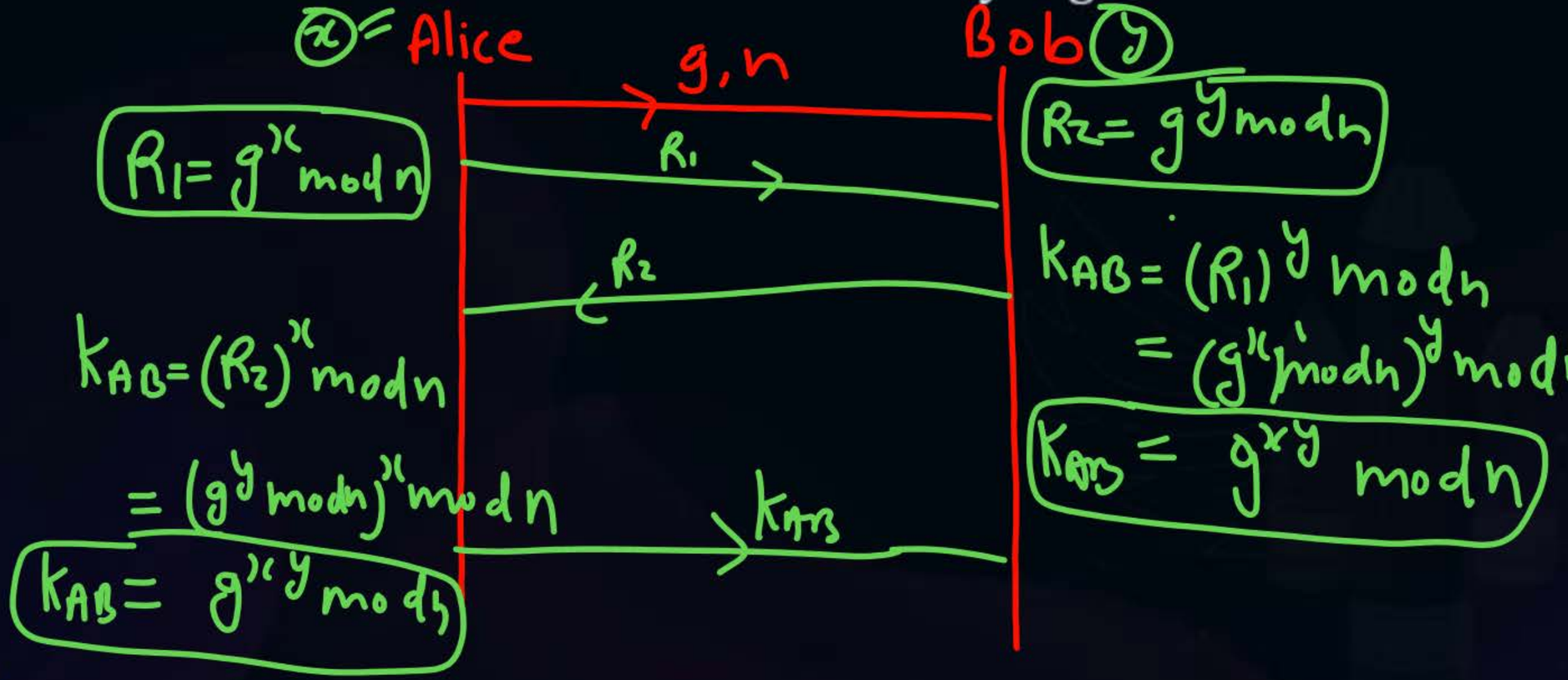
$\frac{5 \times (10-1)}{2} = 45$

Topic : Diffie Hellman

$n = p \times q$ $\quad \phi(n) = (p-1)(q-1)$

Diffie Hellman key Exchange:

- Diffie Hellman key exchange is also known as symmetric key cryptography because sender side and receiver side same key is generated



Cryptography

RSA Algorithm ⇒ Public key Cryptography
Diffie Hellman ⇒ Private " "

Symmetric key Cryptography

Diffie Hellman

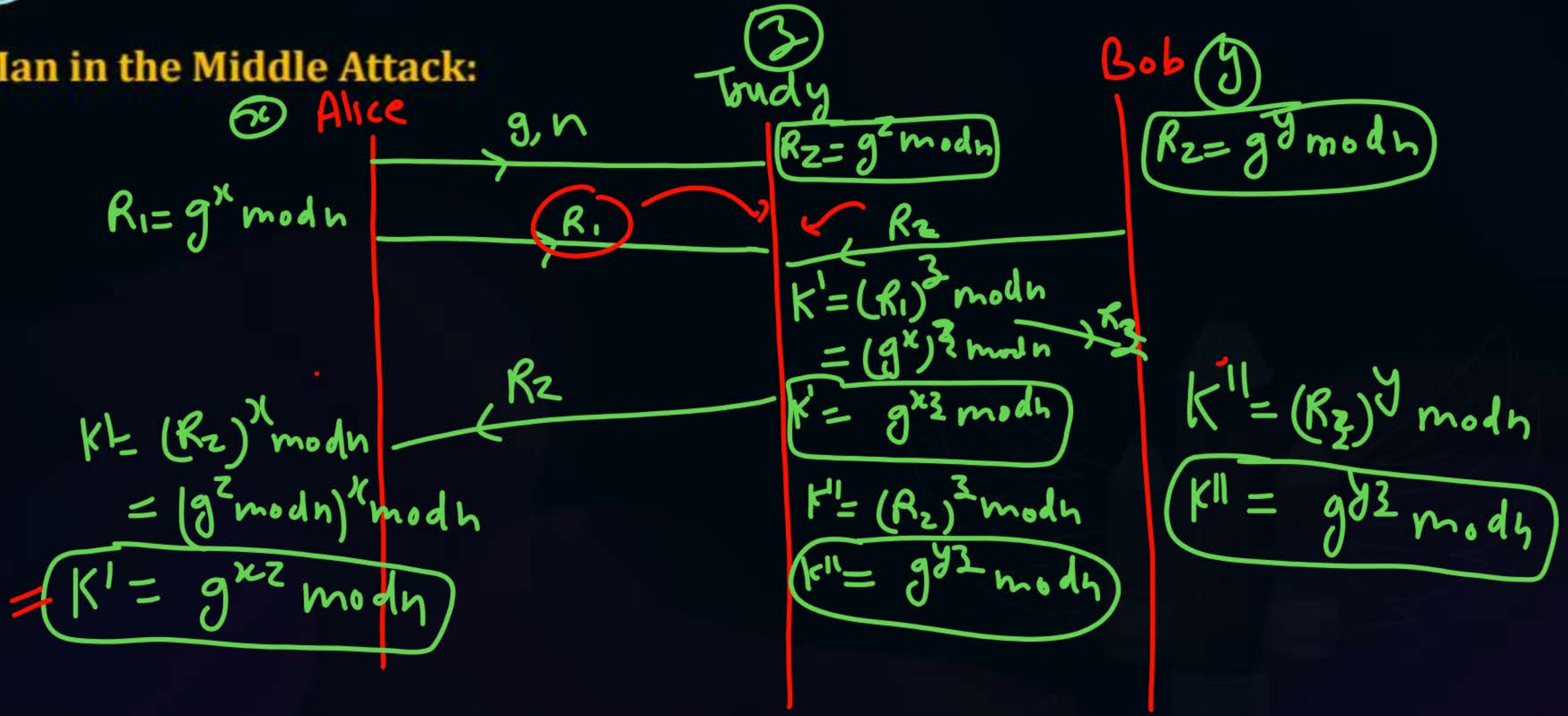
Symmetric key cryptography is also called as Private key cryptography.

We use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys.

$$K_{AB} = g^{xy} \bmod n$$

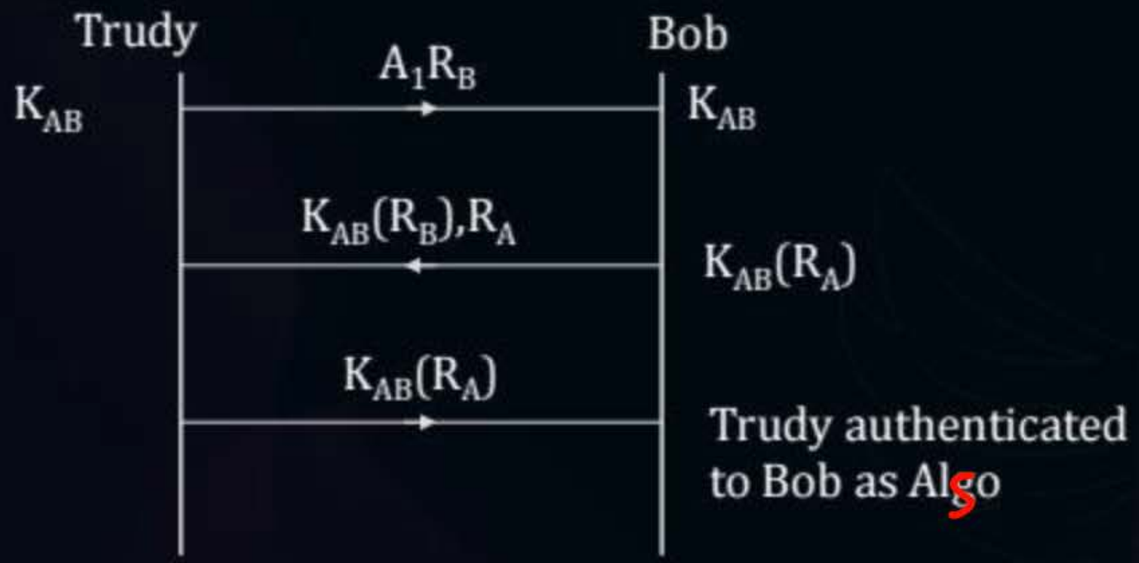
Topic : Network Security

Man in the Middle Attack:



Topic : Network Security

Reflection Attack:



Topic : Network Security

- Drawback of the Diffie Hellman key is if a person × wants to communicate with **n** people than **n** keys are generated. So remembering all the key values is difficult or maintaining a database of all the key values is difficult. So the Burdon of the key values is taken one by the third party agencies or public authority or certification authority.

$K_{AB} = 18$

$K_{AB} = g^{xy} \bmod n$

Q) $n = 23$

$g = 7$

$x = 3$

$y = 6$

Alice (x)

$R_1 = g^x \bmod n$

$= 7^3 \bmod n$

$= 343 \bmod 23$

$R_1 = 21$

Bob (y)

$K_{AB} = (7)^{3 \times 6} \bmod 23$

$= 7^{18} \bmod 23$

$= 7^6 \times 7^6 \times 7^6 \bmod 23$

$R_2 = g^y \bmod n$

$= 7^6 \bmod n$

$= 7^3 \times 7^3 \bmod n$

$= 21 \times 21 \bmod 23$

$= 441 \bmod 23$

$= 4 \times 4 \times 4 \bmod 23$

$= 64 \bmod 23 = 18$

$R_2 = 4$

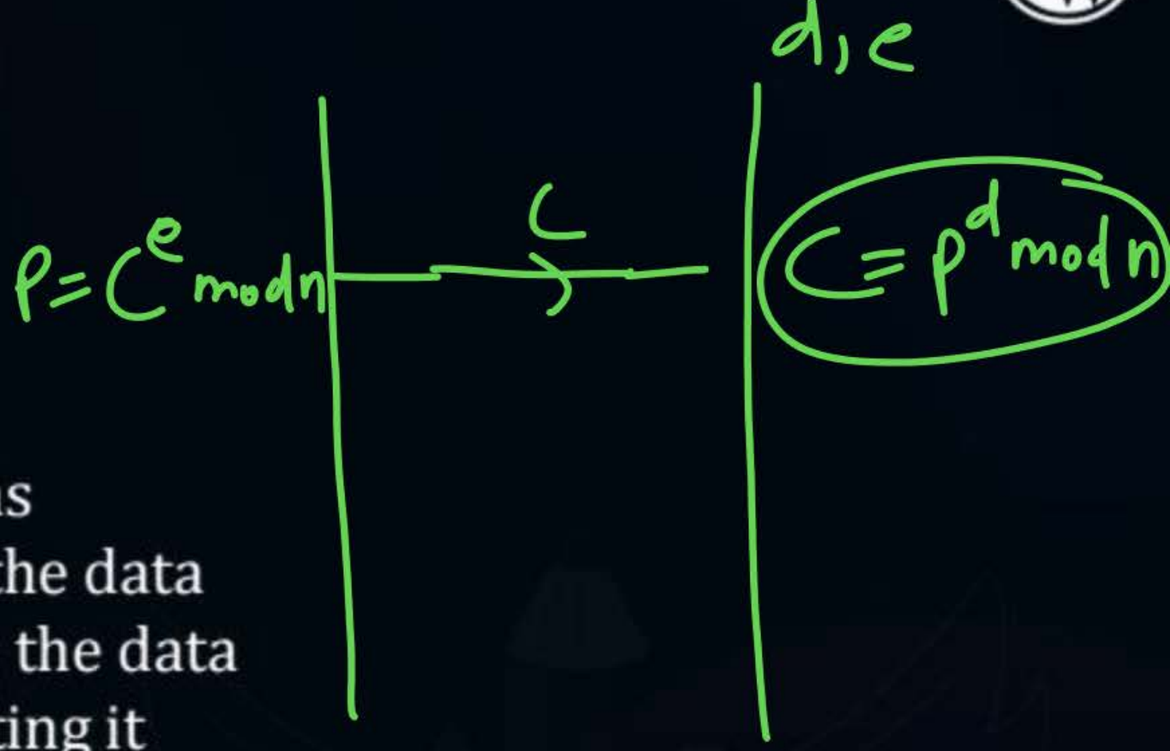
Topic : Network Security

- Mutual authentication using RSA algorithm is better than mutual authentication using Diffie Hellmann key ~~is better than mutual authentication using RSA in term of speed.~~
- RSA algorithm is used to provide both authentication as well as confidentiality
- In Diffie Hellmann key generation both the system are in valued.

Topic : Network Security

#Q. A public key encryption system

A. allows anyone to decode the transmissions
B. allows only the correct sender to decode the data
C. allows only the correct receiver to decode the data
D. does not encode the data before transmitting it



Topic : Network Security

RSA Algorithm

#Q. Which one of the following is true for asymmetric-key cryptography?

Ans Digital Signature

A. Private key is kept by the receiver and public key is announced to the public.
B. Public key is kept by the receiver and private key is announced to the public.
C. Both private key and public key are kept by the receiver.
D. Both private key and public key are announced to the public.

THANK - YOU

CS & IT ENGINEERING

Computer Networks

Network Security

Lecture No.- 03

By- Devvrat Tyagi Sir

Recap of Previous Lecture

Topic Public Key Cryptography

Topic Diffie Hellman Key Exchange Algorithm

RSA Algorithm $\Rightarrow 2n$

DH $\Rightarrow \frac{n(n-1)}{2}$

Topics to be Covered

Topic Certificate Authority

Topic Digital Signature

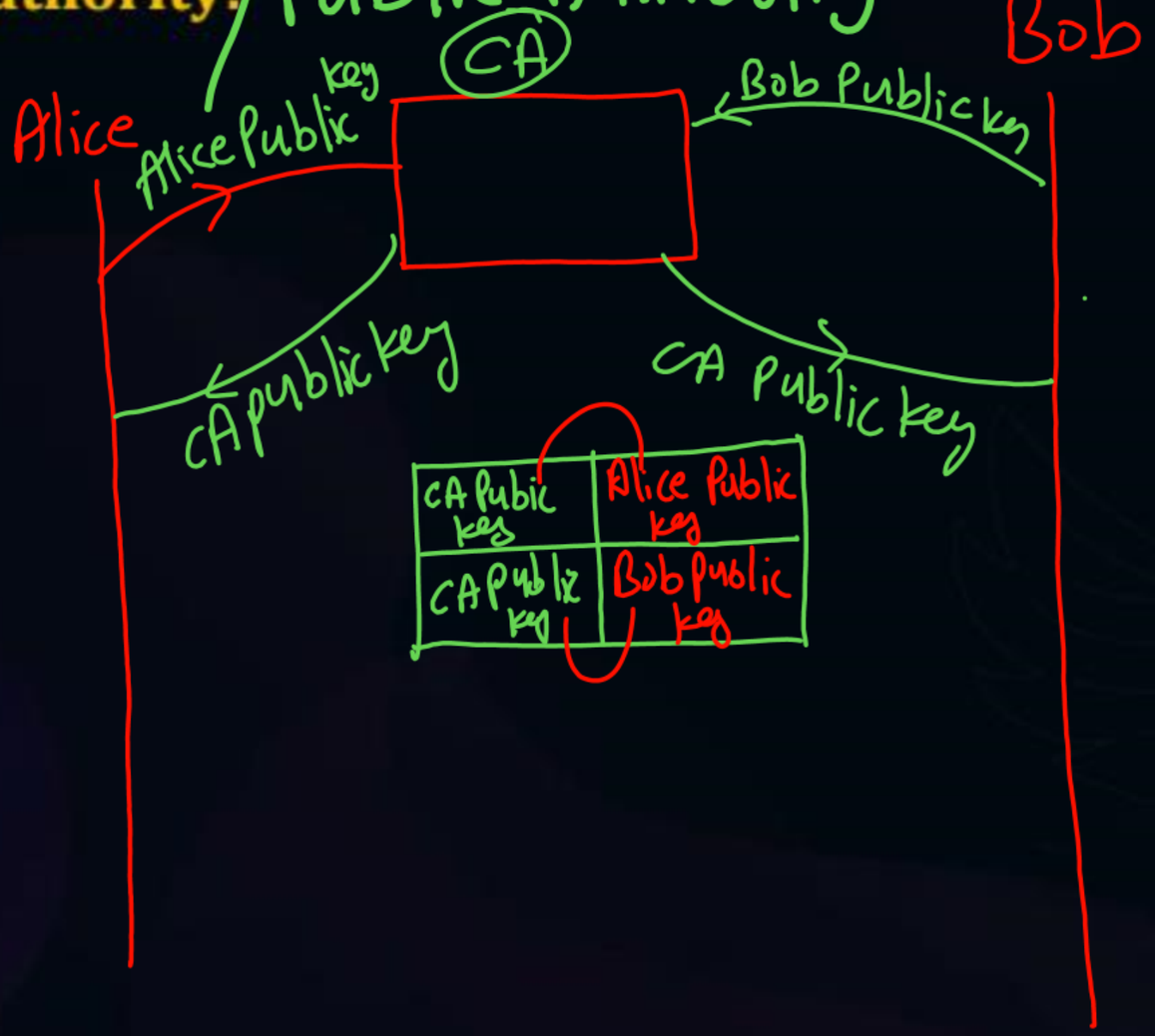
Topic Questions

Topic : Network Security

- Drawback of the Diffie Hellman key is if a person × wants to communicate with **n** people than **n** keys are generated. So remembering all the key values is difficult or maintaining a database of all the key values is difficult. So the Burdon of the key values is taken one by the third party agencies or public authority or certification authority.

Topic : Network Security

Certification Authority: / Public Authority



Topic : Network Security

- If sender is encrypted wd. Receivers public key & receiver is decrypted wd its own private key it is used to provide confidential.
- If sender is encrypted with its own private key and receiver is decrypted with sender's public key it is used to provide authentication.
- Sender is encrypted with its own public key than sender only can decrypt with its own private key it is used during testing time.
- ~~Sender is encrypting wd receiver private key~~

Topic : Network Security

A4 sheet

Digital Signature:

- In case of handwritten signature both data or signature can not be separated, whereas in the case of digital signature both data and signature can be separated

Devtaji

- In case of handwritten signature for all types of data. Same signature is maintain whereas in digital signature for every individual data separate signature is created.

Topic : Network Security

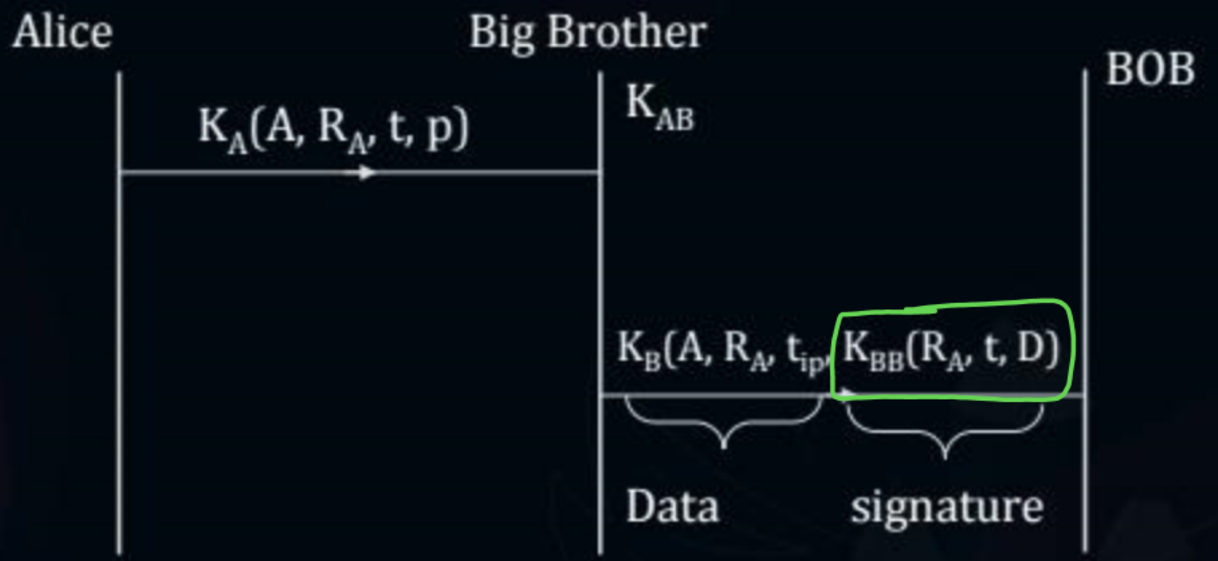
Symmetric key Signature:

A = Alice

R_A = challenge

t = timestamp

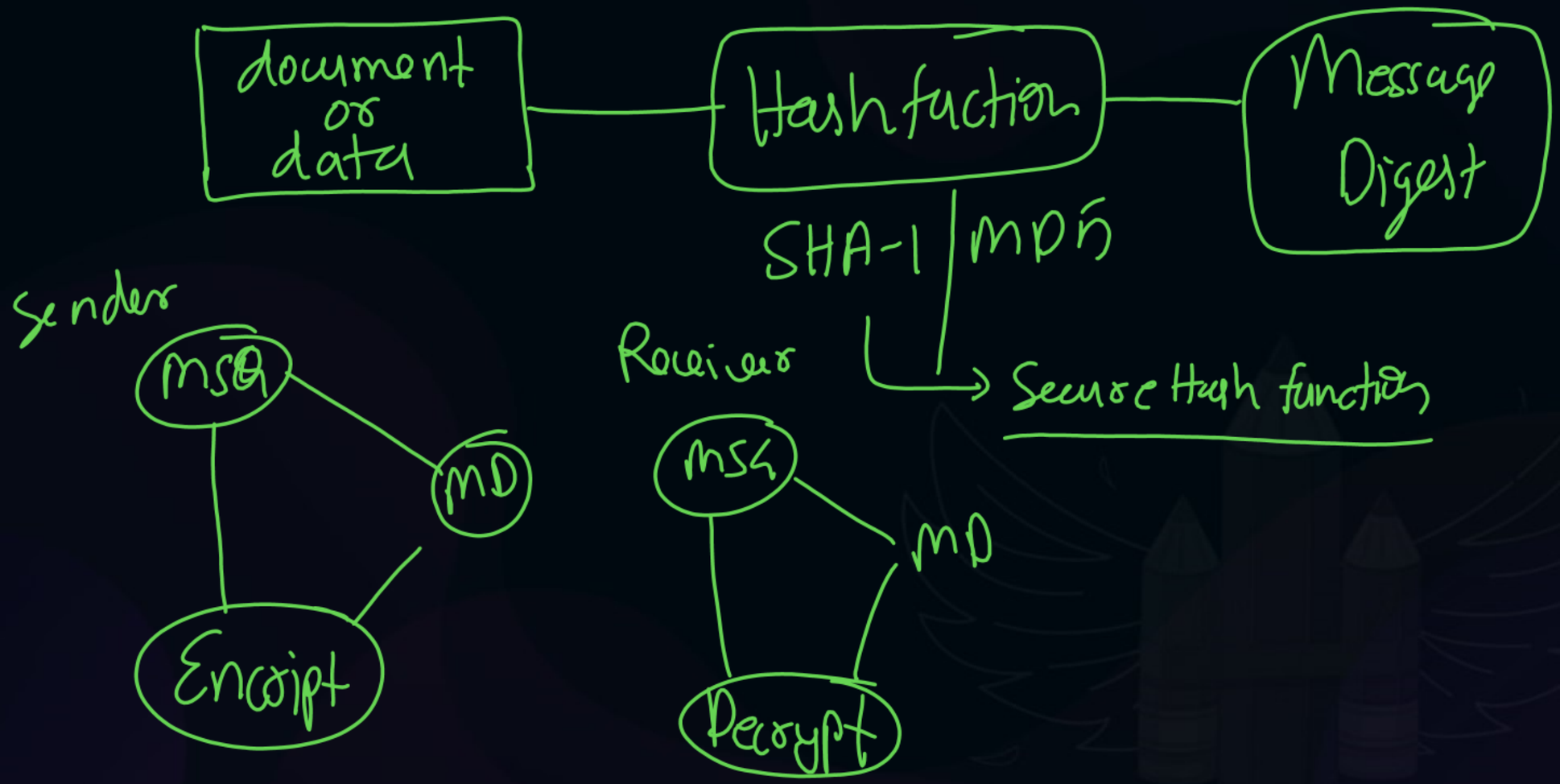
p = plaintext



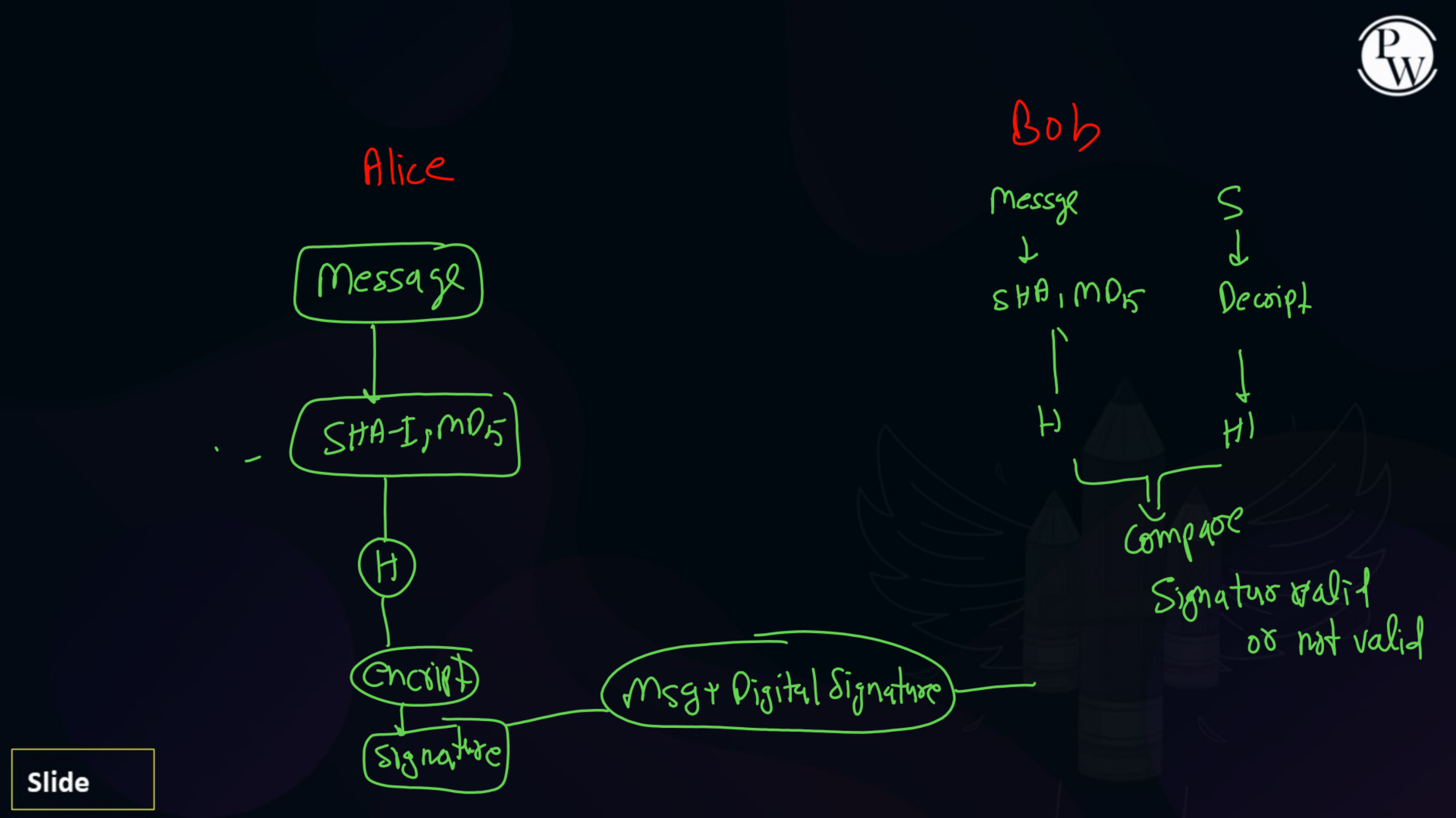
Topic : Network Security

Asymmetric key signature:

- In symmetric key signature the entire algorithm is based on big brother or third party, so it is not so reliable.
- In symmetric key signature the also is boned on Diffie Hellmann.
- Asymmetric key signature is boned on RSA algo
- Symmetric key signature is better than Asymmetric signature in ~~time~~ terms of speed.
- Asymmetric key signature is better than symmetric key signature in terms of security.


document or data
Hash fuction
Message Digest
SHA-1 | MD5
Secure Hash function
Sender
msg
MD
Encript
Receiver
msg
MD
Decrypt

Slide


Alice
Message
SHA-1, MD5
H
Encript
Signature
Msg + Digital Signature
Bob
Message
SHA, MD5
H1
S
Decript
H1
Compare
Signature valid
or not valid
Slide

Topic : Network Security

#Q. Using public key cryptography, X adds a digital signature σ to message M, encrypts $< M, \sigma >$, and sends it to Y, where it is decrypted. Which one of the following sequences of keys is used for the operations?

A. Encryption: X's private key followed by Y's private key; Decryption: X's public key followed by Y's public key

B. Encryption: X's private key followed by Y's public key; Decryption: X's public key followed by Y's private key

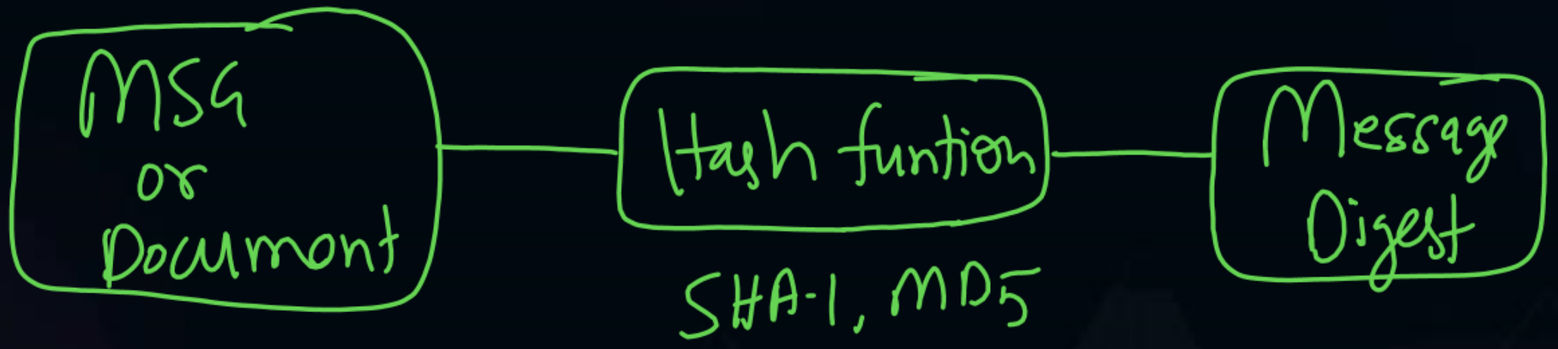
C. Encryption: X's public key followed by Y's private key; Decryption: Y's public key followed by X's private key

D. Encryption: X's private key followed by Y's public key; Decryption: Y's private key followed by X's public key

Topic : Network Security

#Q. Which of the following are used to generate a message digest by the network security protocols?

(P) RSA
(Q) SHA-1
(R) DES
(S) MD5



A. P and R only
B. Q and R only
C. Q and S only
D. R and S only

Topic : Network Security

K_A^-, K_B^- Public key

K_A^+, K_B^+ Poivate keys

#Q. Consider that B wants to send a message m that is digitally signed to A. Let the pair of private and public keys for A and B be denoted K_x^- and K_x^+ for x = A,B, respectively. Let $K_x(m)$ represent the operation of encrypting m with a key Kx and H(m) represent the message digest. Which one of the following indicates the CORRECT way of sending the message m along with the digital signature to A?

(A) $\{m, K_B^+(H(m))\}$

(B) $\{m, K_B^-(H(m))\}$

Asymetoic

(C) $\{m, K_A^-(H(m))\}$

(D) $\{m, K_A^+(H(m))\}$

A

B

A. A

B. B

C. C

D. D

Topic : Network Security

#Q. Consider the following two statements: i. A hash function (these are often used for computing digital signatures) is an injective function. ii. An encryption technique such as DES performs a permutation on the elements of its input alphabet. Which one of the following options is valid for the above two statements?

one to one

A. Both are false
B. Statement (i) is true and the other is false
C. Statement (ii) is true and the other is false
D. Both are true

Topic : Network Security

for(i=0; i≤n, i++)
printf(x)
n times
O(n)

$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}-$ ≤ 3 logn

#Q. Exponentiation is a heavily used operation in public key cryptography. Which of the following options is the tightest upper bound on the number of multiplications required to compute b^n mod m, 0<=b, n<=m?

$O(\frac{n}{\log n})$
$O(n)$

$b^n \bmod m$

$7^{18} \bmod 23$

7^6 7^6 7^6

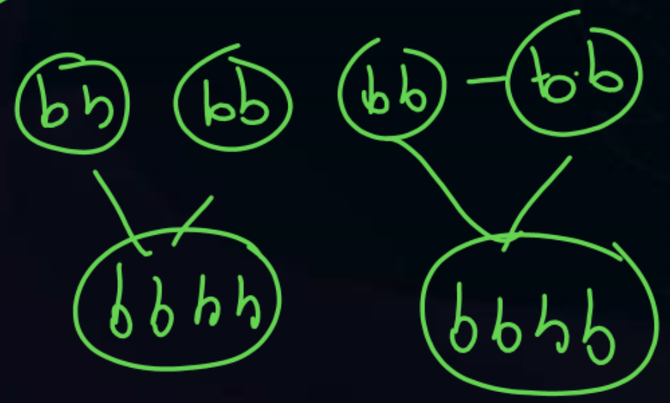
A. O(logn)

B. $O(\sqrt{n})$

C. O(n/logn)

D. O(n)

b b b b = n mod m



mod m

Topic : Network Security

#Q. MD5 is a widely used hash function for producing hash value of

A. 64 bits
B. 128 bits
C. 512 bits
D. 1024 bits

128 bits

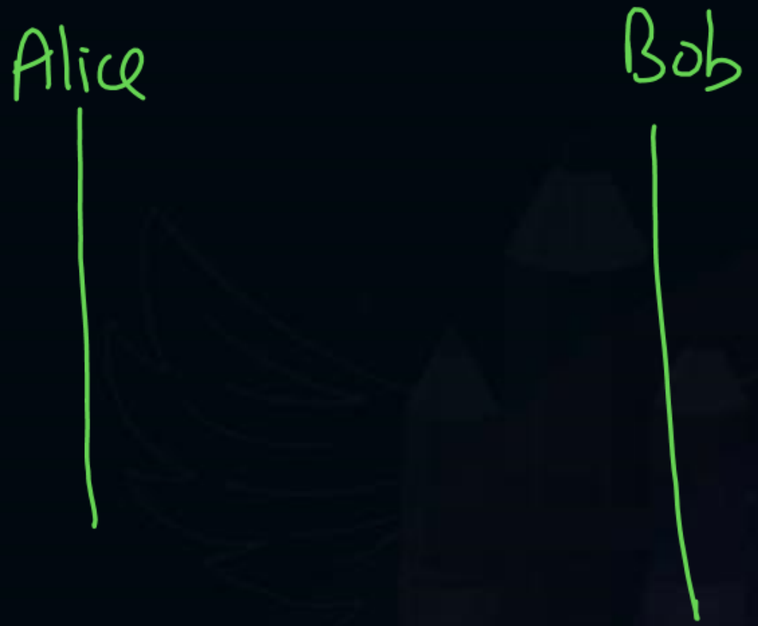
$\frac{2^7 \text{ bits}}{2^3} = 2^4 \text{ bytes}$

$= 16 \text{ bytes}$

Topic : Network Security

#Q. An attacker sits between the sender and receiver and captures the information and retransmits to the receiver after some time without altering the information. This attack is called as_____,

A. Denial of service attack
B. Masquarade attack
C. Simple attack
D. Complex attack



Topic : Network Security

- An attacker sits between customer and Banker, and captures the information from the customer and retransmits to the banker by altering the information. This attack is called as Replay attack.
- Passive Attack are in the nature of monitoring, or eavesdropping of transmissions of many types. In this attack, attacker try to gain information or the information that is being transmitted in the message.
- Masquerade Attackis a type network attack where the attacker pretends to be an authorized user of a system in order to gain access.
- Denial of Service Attack(DoS) is atype of network attack in which attacker shut down a machine or network, making it inaccessible to its intended users.

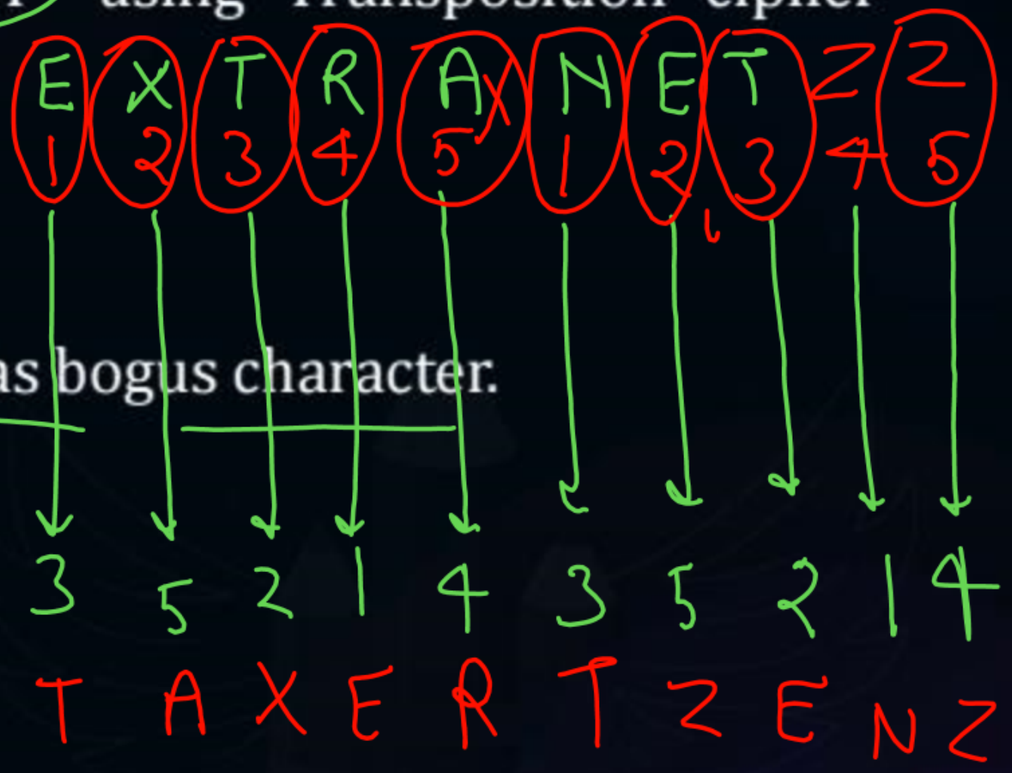
Topic : Network Security

#Q. Encrypt the plain text Message "EXTRANET" using Transposition cipher technique with the following key:

3	5	2	1	4	(Cipher text)
1	2	3	4	5	(Plain text)

A. TAXERTZENZ
B. EXTRANETZZ
C. EZXZTRZANZET
D. EXTZRANZETZ

Plaintext



Using 'Z' as bogus character.

Topic : Network Security

#Q. SHA-1 is a

SHA-1 ⟹ Message Digest

A. encryption algorithm
B. decryption algorithm
C. key exchange algorithm
D. message digest function

Topic : Network Security

#Q. Advanced Encryption Standard (AES) is based on

A. Asymmetric key algorithm
B. Symmetric key algorithmn
C. Public key algorithm
D. Key exchange

Topic : Network Security

#Q. Hashed message is signed by a sender using

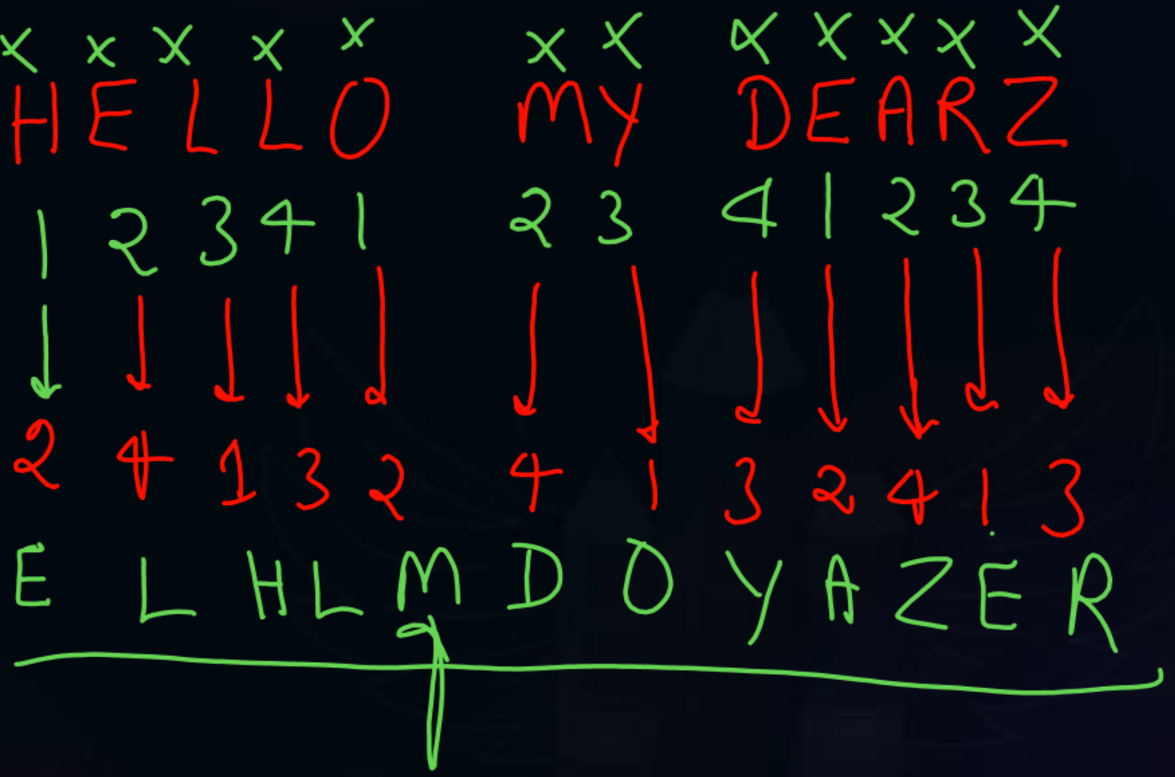
A. his public key
B. his private key
C. receiver's public key
D. receiver's private key

Topic : Network Security

#Q. Encrypt the Message "HELLO MY DEARZ" using Transposition Cipher with

Key { Plain Text 2 4 1 3 ; Chipher Text 1 2 3 4 }

A. HLLEO YM AEDRZ
B. EHOLL ZYM RAED
C. ELHL MDOY AZER
D. ELHL DOMY ZAER



THANK - YOU