⇒ Primitive Roots.

"A number 'α' is a primitive root modulo n if every number coprime to n is congruent to a power of α' modulo n"

Or

"'α' is said to be a primitive root of a prime number 'p', if $\alpha^1 \bmod p$, $\alpha^2 \bmod p$, $\alpha^3 \bmod p$, ... $\alpha^{p-1} \bmod p$ are distinct"

Example 1: is 2 a primitive root of prime number 5?

Solution :→

$2^1 \bmod 5 \Rightarrow 2 \bmod 5 \Rightarrow 2$
$2^2 \bmod 5 \Rightarrow 4 \bmod 5 \Rightarrow 4$
$2^3 \bmod 5 \Rightarrow 8 \bmod 5 \Rightarrow 3$
$2^4 \bmod 5 \Rightarrow 16 \bmod 5 \Rightarrow 1$

} all are uniformly distributed distinct values

So, 2 is a primitive root of 5.

Example 2: is 3 a primitive root of prime number 7?

Solution :→ $3^1 \bmod 7 = 3$
$3^2 \bmod 7 = 9 \bmod 7 = 2$
$3^3 \bmod 7 = 27 \bmod 7 = 6$
$3^4 \bmod 7 = 81 \bmod 7 = 4$
$3^5 \bmod 7 \Rightarrow 5$
$3^6 \bmod 7 \Rightarrow 15$

all values are distinct so, 3 is primitive root of 7

Example : is 2 a primitive root of prime number 7 ?

Solution:

$2^1 \bmod 7 = 2 \bmod 7 = 2$
$2^2 \bmod 7 = 4 \bmod 7 = 4$
$2^3 \bmod 7 = 8 \bmod 7 = 1$
$2^4 \bmod 7 = 16 \bmod 7 = 2$
$2^5 \bmod 7 = 2^4 \times 2^1 \bmod 7 = 2 \times 2 \bmod 7 = 4 \bmod 7 = 4$
$2^6 \bmod 7 = 2^5 \times 2^1 \bmod 7 = 4 \times 2 \bmod 7 = 8 \bmod 7 = 1$

here, All values are not distinct so 2 is not primitive root of 7 and Results are also not uniformly distributed.

Example : is 2 a primitive root of 11 ?

Example: what are all primitive roots of 5

sol:→

$1^1 \bmod 5 = 1$ $2^1 \bmod 5 = 2$ $3^1 \bmod 5 = 3$ $4^1 \bmod 5 = 4$
$1^2 \bmod 5 = 1$ $2^2 \bmod 5 = 4$ $3^2 \bmod 5 = 4$ $4^2 \bmod 5 = 1$
$1^3 \bmod 5 = 1$ $2^3 \bmod 5 = 3$ $3^3 \bmod 5 = 2$ $4^3 \bmod 5 = 4$
$1^4 \bmod 5 = 1$ $2^4 \bmod 5 = 1$ $3^4 \bmod 5 = 1$ $4^4 \bmod 5 = 1$

not distinct ✗ distinct ✓ ✓ not distinct ✗

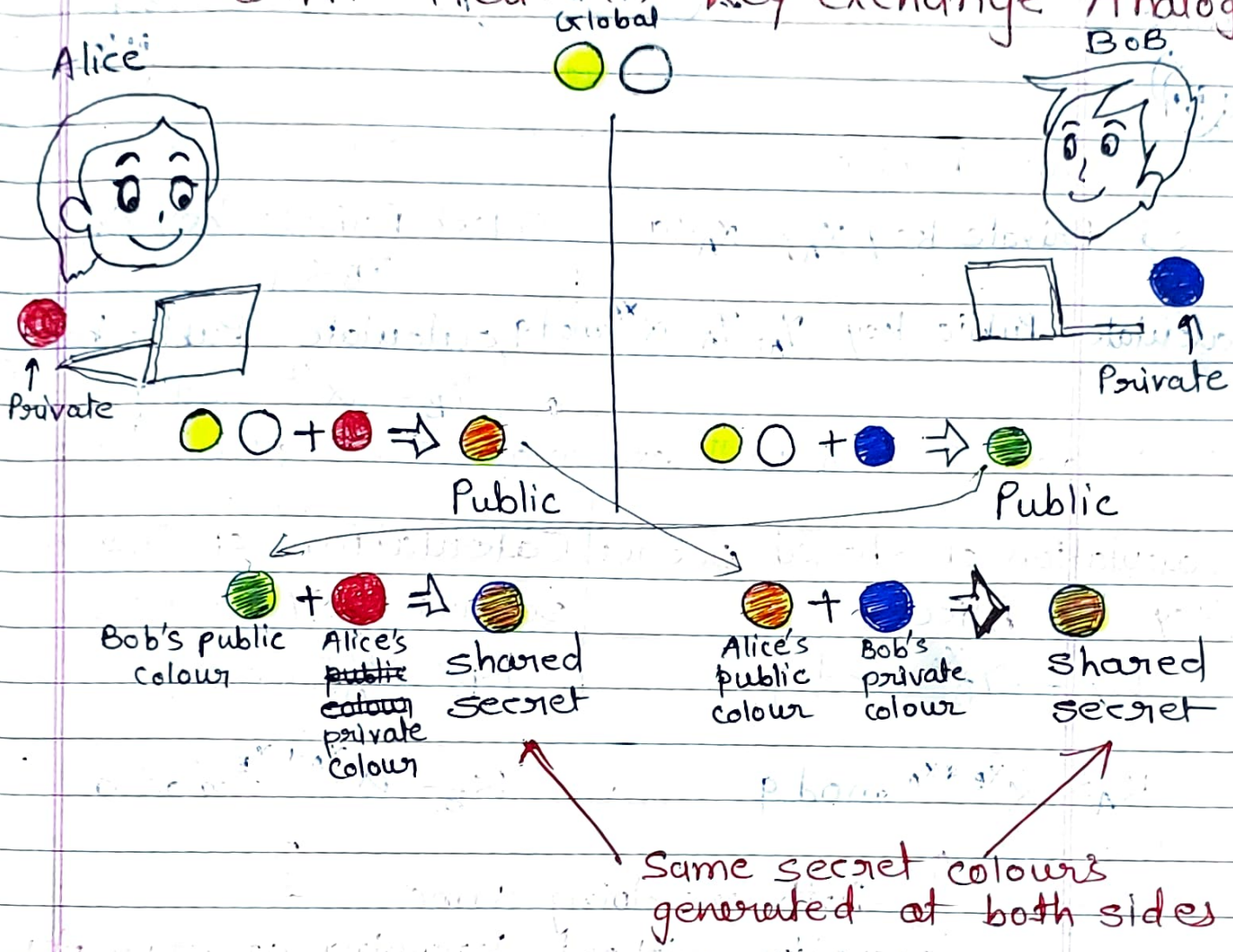
Answer: 2 and 3 are primitive roots of 5

⇒ Diffie hellman key Exchange Algo.

Need for Diffie-hellman key exchange

→ Two parties with no prior knowledge
→ Insecure channel.
→ Jointly established a shared secret key.

Diffie-Hellman key exchange Analogy



Global is the colours on which both have agreed.

private is the colours which is not shared with any one.

public is the colour which is generated by adding global colours to private colour

public colour of Receiver + own privatekey = shared secret key

Diffie - Hellman key Exchange Algo.

Global Public Elements
q - prime number
α - primitive root of q
and $\alpha < q$

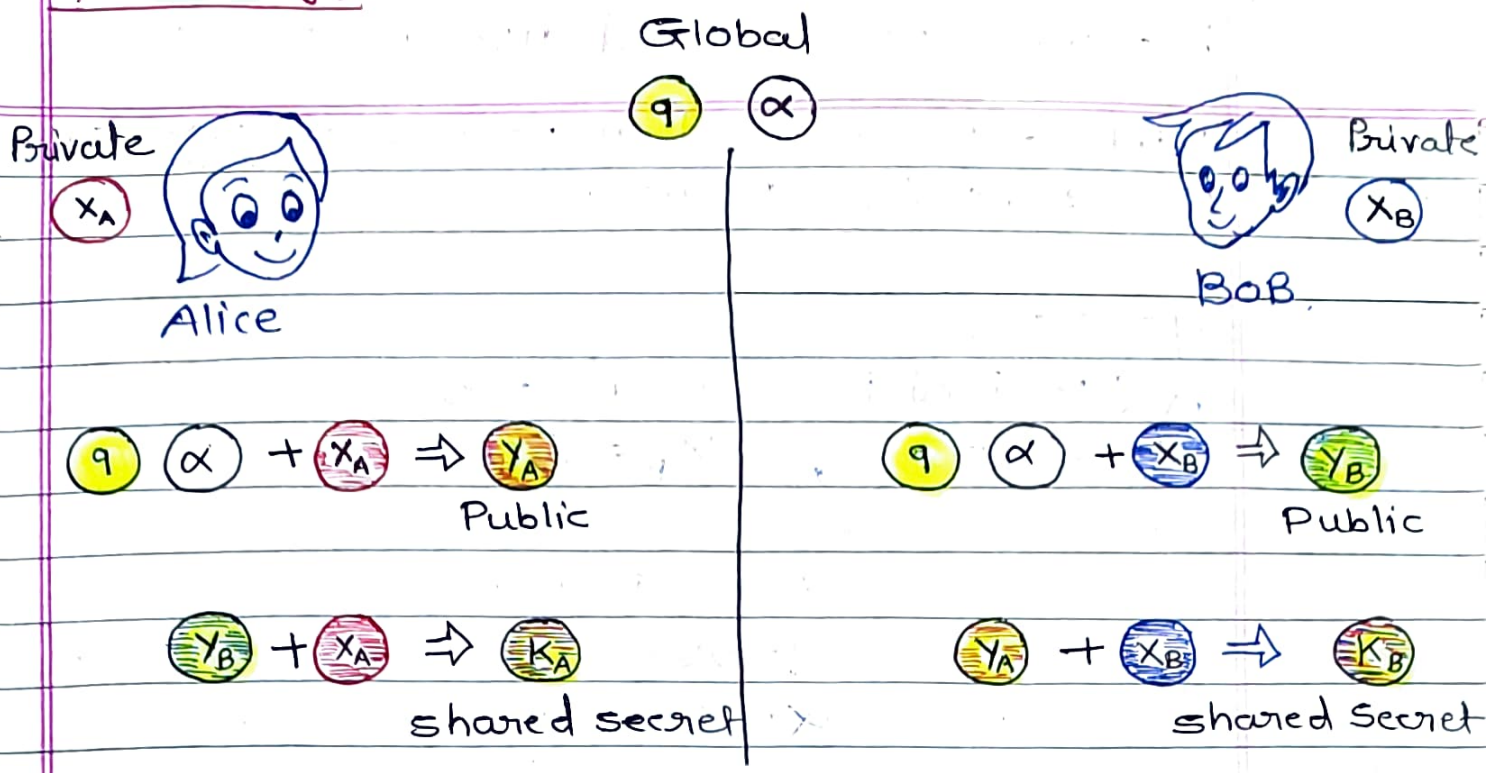
key generation by Alice	key generation by bob
Select Private key X_A; $X_A < q$	Select Private key X_B $X_B < q$
Calculate Public key Y_A; $Y_A = \alpha^{X_A} \bmod q$	calculate Public key Y_B $Y_B = \alpha^{X_B} \bmod q$

Both alice & bob will exchange their public keys.

Calculation of Shared secret key by Alice.	Calculation of Shared secret key by Bob.
$K_A = Y_B^{X_A} \bmod q$	$K_B = Y_A^{X_B} \bmod q$
$K_A = \alpha^{X_B * X_A} \bmod q$	$K_B = \alpha^{X_A * X_B} \bmod q$
Substitute value of Y_B	Substitute value of Y_A

↑ Both are doing same operation without knowing other parties private key. ↑

Analogy :→



Example: Suppose that two parties A & B wish to setup a common secret key (D-H key) between themselves using the DiFFie-Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A choose 2 and party B chooses 5 as their respective secrets. Their D-H key is 4

Global Elements

$q = 7,\ \alpha = 3$

Alice

private key $X_A = 2;\ 2 < 7$

Public key $Y_A = 3^2 \bmod 7 = 2$

BOB

private key $Y_B = 5,\ 5 < 7$

public key $Y_B = 3^5 \bmod 7$

$= 5$

Alice calculate secret key

$K_A = Y_B^{X_A} \bmod q$

$= 5^2 \bmod 7$

$= 25 \bmod 7 = 4$

5 → Alice

2 → Bob

Bob calculate Secret Key.

$K_B = Y_A^{X_B} \bmod q$

$= 2^5 \bmod 7$

$= 32 \bmod 7$

$= 4$

Example 2: Find the Secret key shared between user A and user B using Diffie-Hellman key exchange algorithm For following values:

$q = 353$

α (primitive root) $= 3$

$X_A = 45$, $X_B = 50$

Global Elements.

$q = 353$

$\alpha = 3$

Alice	BoB
private key $X_A = 45$, $45 < 353$	private key $X_B = 50$
public key $Y_A = \alpha^{X_A} \bmod q$ $= 3^{45} \bmod 353$ $= 143$	public key $Y_B = \alpha^{X_B} \bmod q$ $Y_B = 3^{50} \bmod 353$ $= 155$
Calculation of Shared Secret key by Alice	Calculation of shared Secret key by Bob.
$K_A = Y_B^{X_A} \bmod q$	$K_B = Y_A^{X_B} \bmod q$
$K_A = 155^{45} \bmod 353$ $= 197$	$= 143^{50} \bmod 353$ $= 197$

Secret shared key is 197

$\Rightarrow 3^{45} \bmod 353$

$3 \bmod 353 = 3$
$3^2 \bmod 353 = 9$
$3^4 \bmod 353 = 81$
$3^8 \bmod 353 = 81 \times 81 \bmod 353 = 207$
$3^{16} \bmod 353 = 207 \times 207 \bmod 353 = 136$
$3^{32} \bmod 353 = 136 \times 136 \bmod 353 = 140$

$3^{45} \bmod 353 = 3^{32} \times 3^8 \times 3^4 \times 3^1 \bmod 353$
$= 140 \times 207 \times 81 \times 3 \bmod 353$
$= 143$

$\Rightarrow 3^{50} \bmod 353$

$= 3^{45} \times 3^4 \times 3^1 \bmod 353$
$= 143 \times 81 \times 3 \bmod 353$
$= 155$

$\Rightarrow 155^{45} \bmod 353$
$155 \bmod 353 = 155$
$155^2 \bmod 353 = 21$
$155^4 \bmod 353 = 21 \times 21 \bmod 353 = 88$
$155^8 \bmod 353 = 88 \times 88 \bmod 353 = 331$
$155^{16} \bmod 353 = 331 \times 331 \bmod 353 = 131$
$155^{32} \bmod 353 = 131 \times 131 \bmod 353 = 217$
$155^{45} \bmod 353 = 155^{32} \times 155^4 \times 155^1 \times 155^8 \bmod 353$
$= 217 \times 88 \times 155 \times 331 \bmod 353$
$= 197$

Example :3.

Users Alice and bob use the Diffie-Hellman key exchange technique with a common prim $q=941$ and Primitive root $\alpha = 627$

a. if Alice selects her private key as 347 what is Alice's public key?

b. if bob selects his private key as 781, what is bob's public key?

c. What is the shared secret key?

Solution :→

Given Data

$\alpha = 627$

$q = 941$

$X_A = 347$

$X_B = 741$

To Find

Y_A

Y_B

K

Global elements.

$q = 941$

$\alpha = 627$

Alice

Select private Key $X_A = 347$

Calculate public key

$Y_A = 627^{347} \bmod 941 = \boxed{390}$

Calculate shared secret key.

$K_A = Y_B^{X_A} \bmod q$

$= 691^{347} \bmod 941$

$\boxed{K_A = 470}$

Bob.

Select private key $X_B = 781$

Calculate public Key $Y_B = 627^{781} \bmod 941$

$= \boxed{691}$

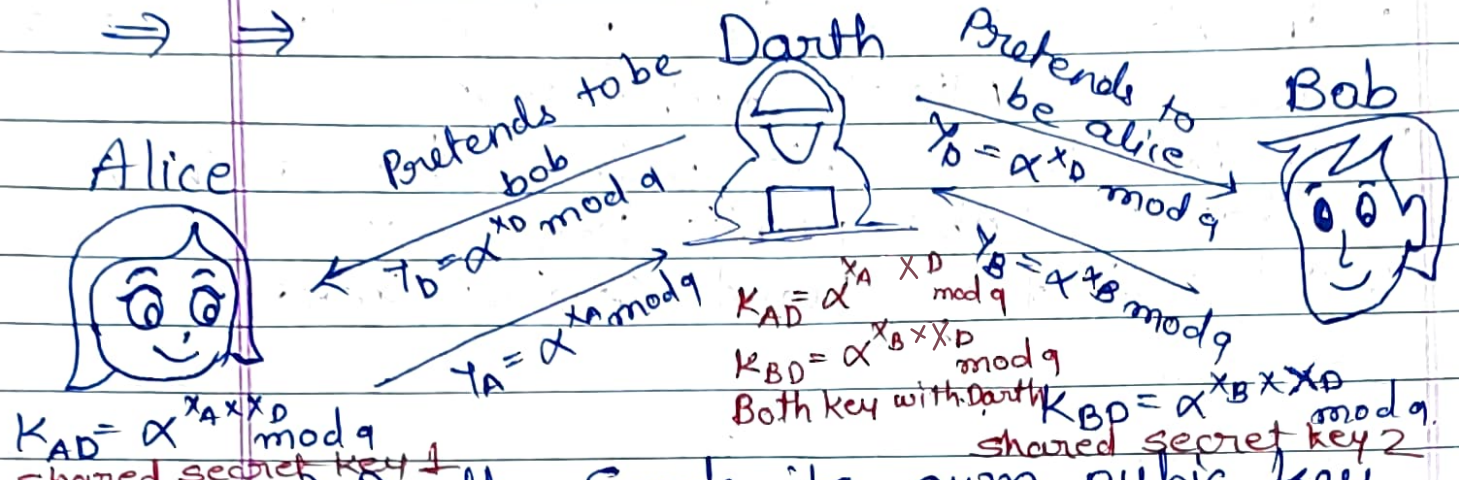
Calculate shared secret key.

$K_B = Y_A^{X_B} \bmod q$

$= 390^{781} \bmod 941$

$\boxed{K_B = 470}$

⇒ Diffie Hellman key exchange
→ Man in the Middle Attack



⇒ Darth Sends its own pubic key with alice pretending to be bob.

⇒ alice will Sends its own public key

⇒ Both calculates therir sheared secret key.

⇒ here bob will have both shared secret key.

⇒ Now Darth can decrypt all the msg from Alice & Read/update & Re encrypt using another key & send it to BoB.

⇒ Serious attack in diffie hellman key exchange.

Applications of Diffie hellman key exchange

⇒ Secure Shell :→ (SSH)
- → its a cryptographic network protocol
- → used for doing n/w related services securely over un-secured network.
- → client ←→ Server.

⇒ Transport layer Security (TLS)/ secure socket layer (SSL)

⇒ Https.

⇒ Public key Infrastructure (PKI)
- → Roles, Procedures, policies, H/W, S/W needed to create manage distribut use, store & Revoke digital certifica
- → PKI is used by ecommerce, e banking & email confidentiality.
- → Diffie hellman with RSA or other cryptography related algo. are used

⇒ Internet key Exchange. (IKE)
- → used to setup security associations in IPSec protocol suite.

⇒ Internet Protocol Security (IPSec)
- → N/W layer Security protocol.
- → its a n/w protocol suit which uses cryptographic service to protect communicat over ip network. → for keyexchange Diffie-hell & elliptic curve used

⇒ Though Diffie hellman is vulnerable to man-in-the middle attack it has very strong mechanism for key exchan so it is widely used.

⇒ ⇒ Limitations

⇒ Non authenticated key agreement protocol.

→ Alice & bob was not aware of Dearth's existance or interrupt

⇒ poor authentication.

⇒ Man-in-the middle attack.

⇒ cant be used for encrypting messages.