SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

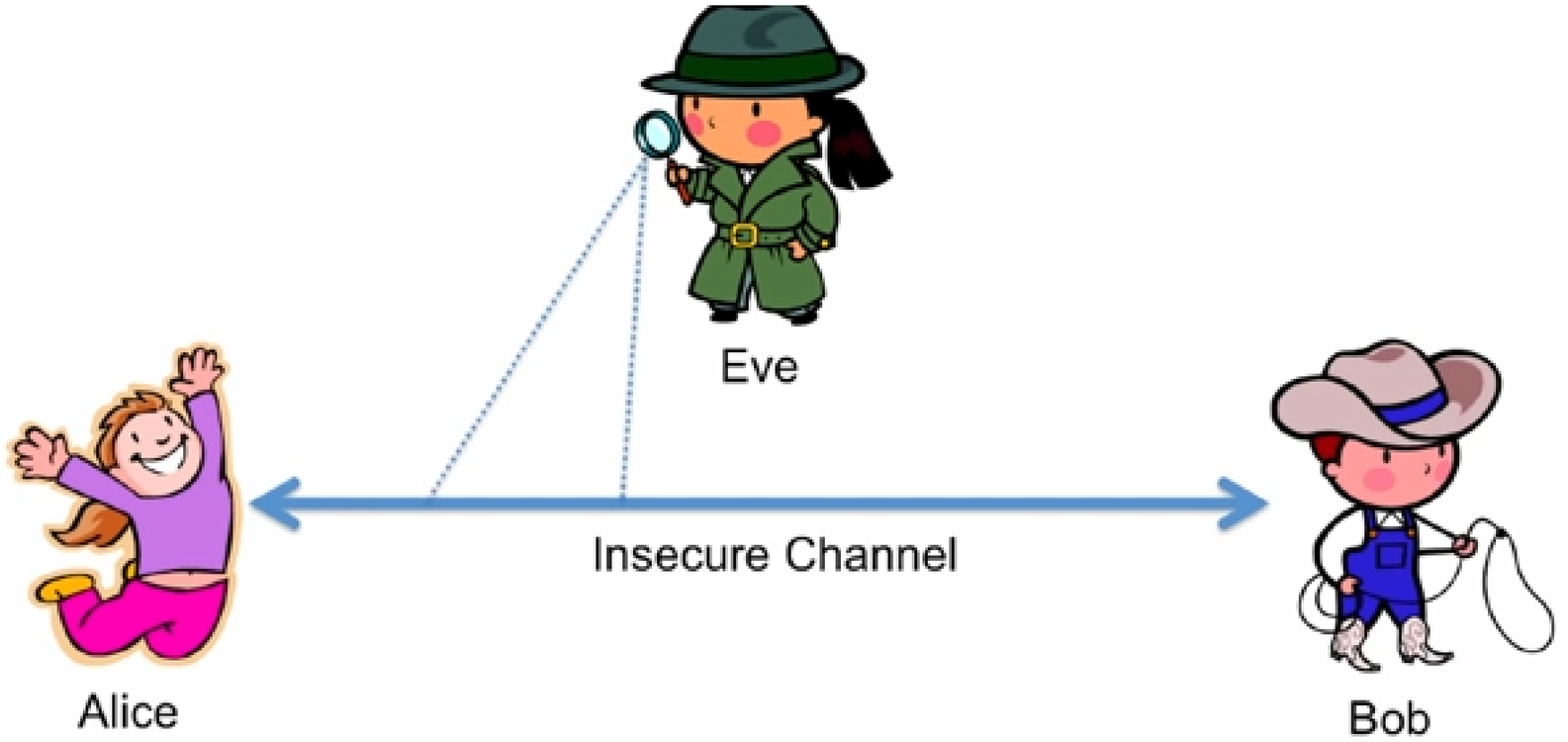
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

COURSE NAME : 19CS503 Cryptography and Network Security

III YEAR & V SEMESTER

Unit 3- Public Key Cryptography

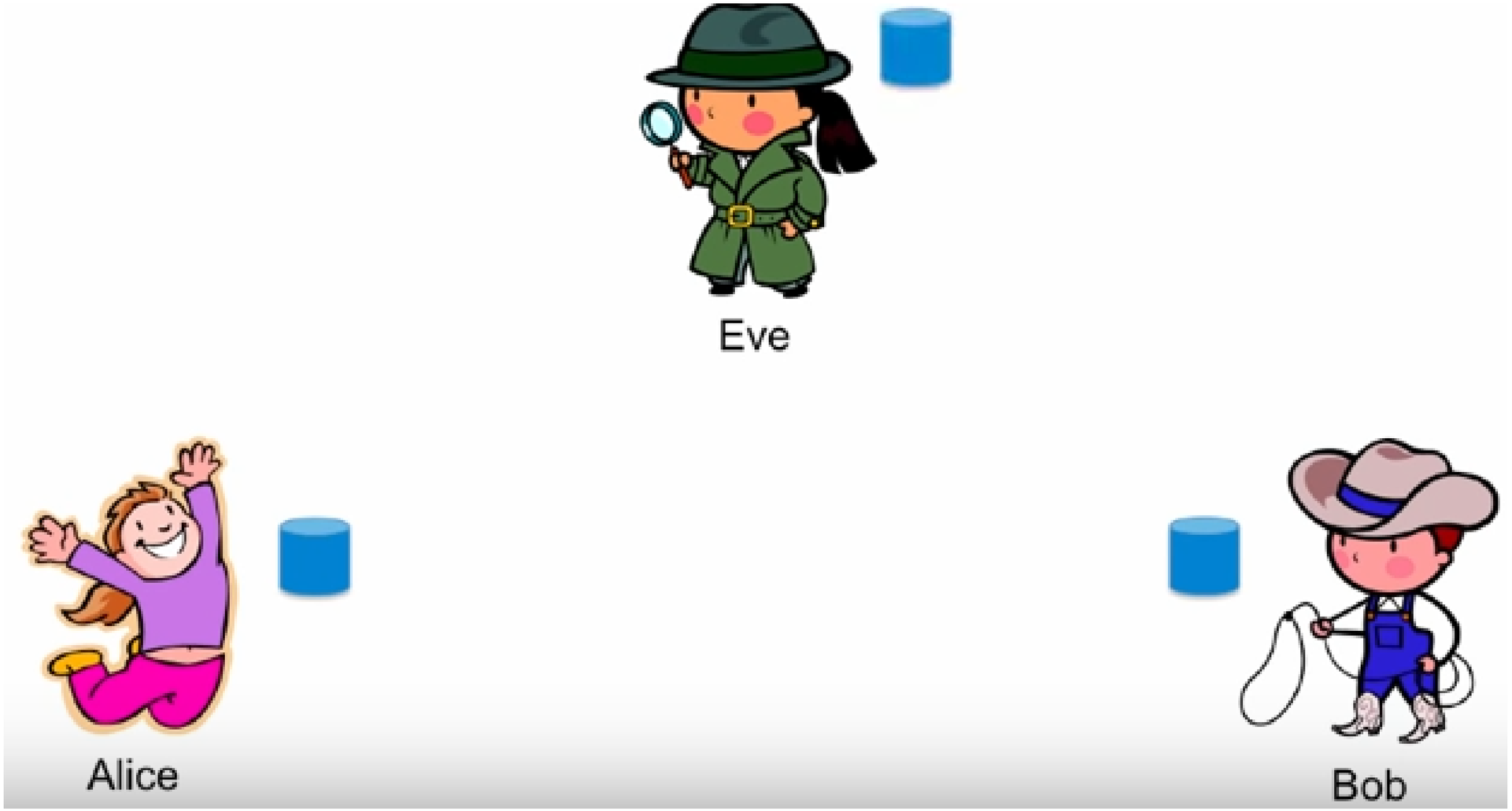
Topic : Diffie Hellman Key exchange


Eve
Insecure Channel
Alice
Bob

Diffie Hellman Key Exchange

- Diffie & Hellman in 1976 along with the exposition of public key concepts
  - Securely Exchange keys
- a public-key distribution scheme
  - cannot be used to exchange an arbitrary message
  - rather it can establish a common key
  - known only to the two participants
- value of key depends on the participants (and their private and public key information)
- based on exponentiation in a finite (Galois) field (modulo a prime or a polynomial) - easy
- security relies on the difficulty of computing discrete logarithms (similar to factoring) – hard

Diffie Hellman – Colors Analogy



Analogy continued..

- Eve can’t determine the secret color because she doesn’t have the right color to mix together
- This works based on two assumptions
  - Paint is easy to mix
  - Paint is hard to unmix

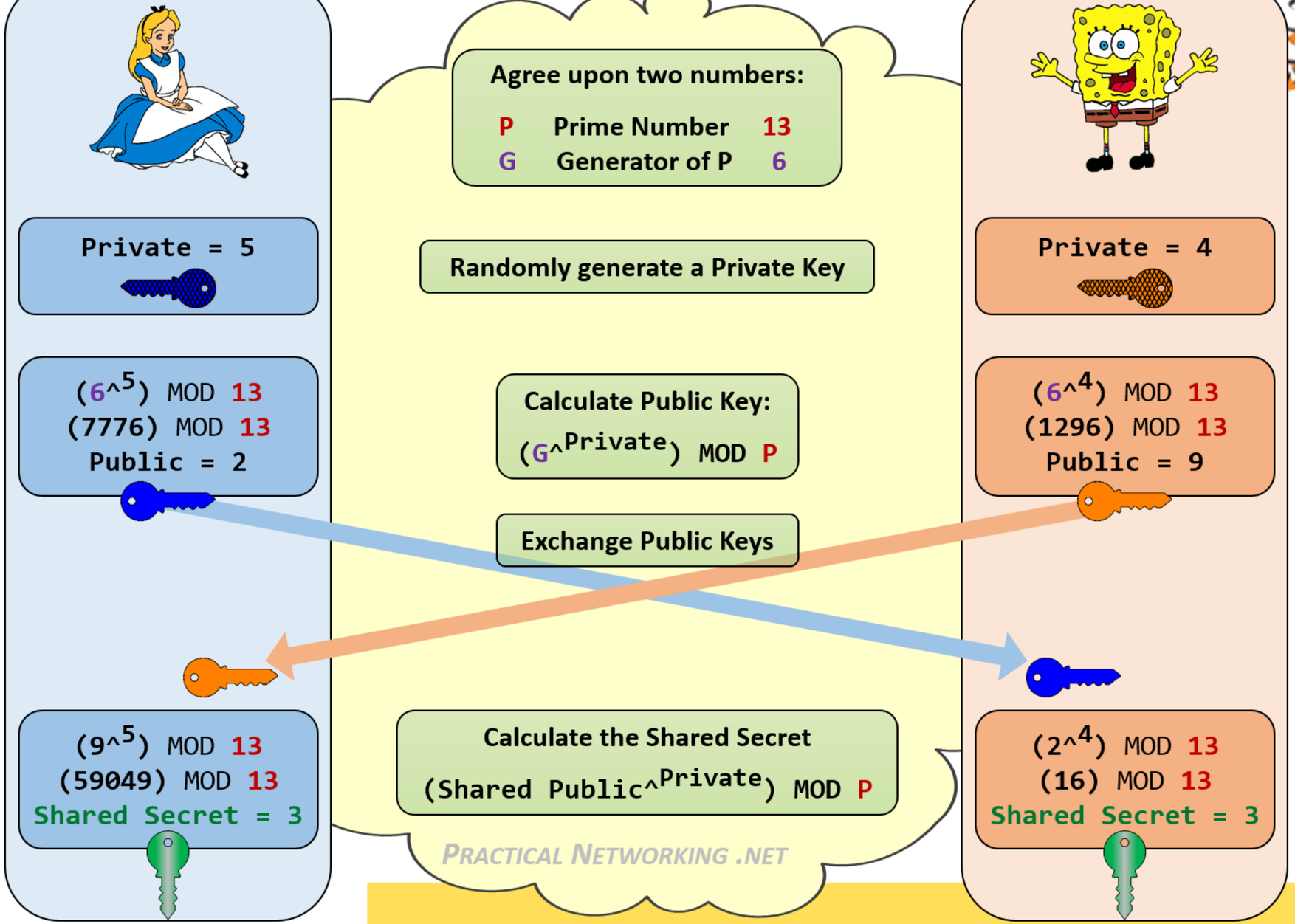
Algorithm

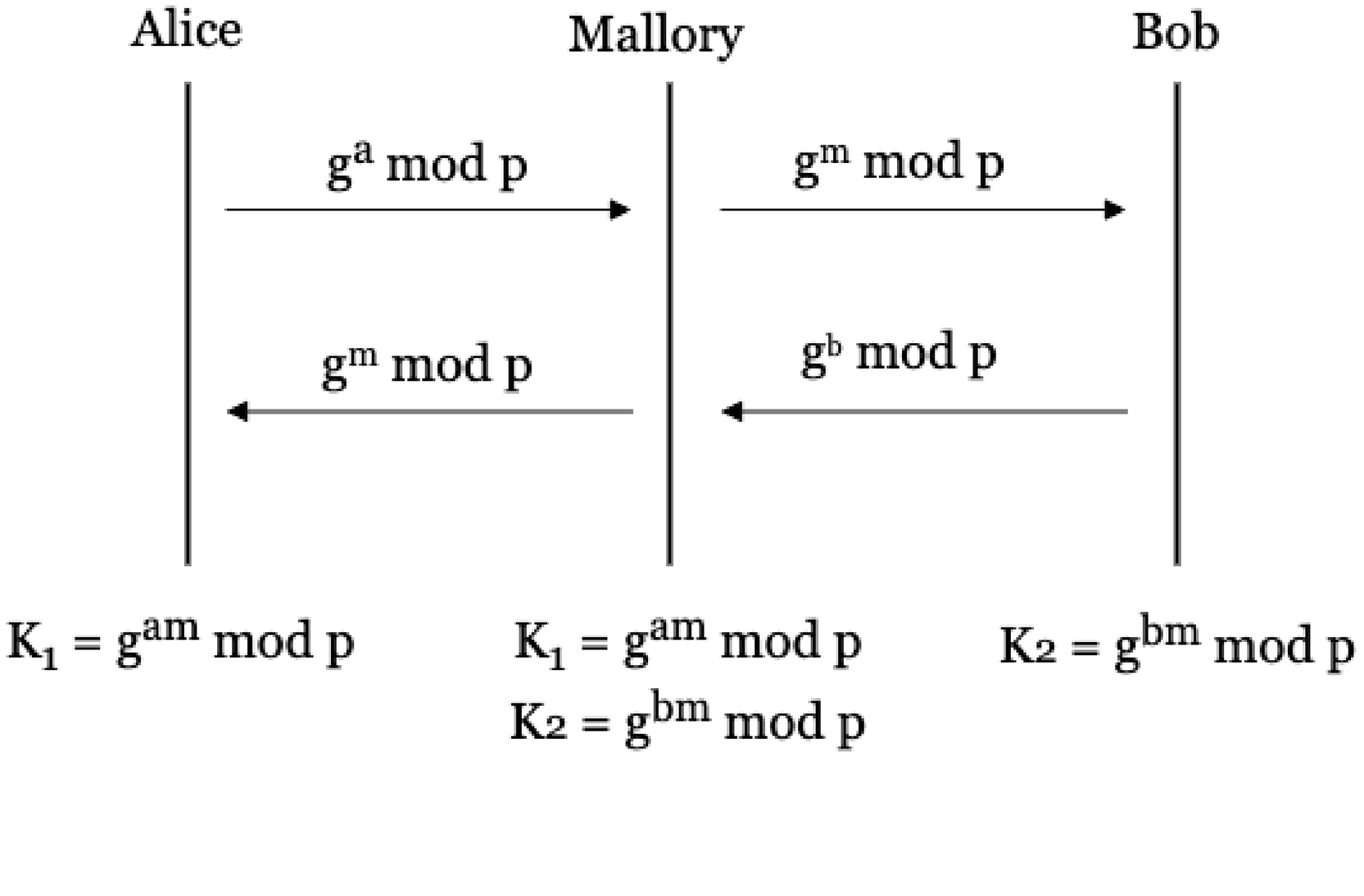
- all users agree on global parameters:
  - large prime integer or polynomial q
  - α a primitive root mod q
- each user (eg. A) generates their key
  - chooses a secret key (number): $x_A < q$
  - compute their **public key**: $y_A = \alpha^{x_A} \bmod q$
- each user makes public that key y_A

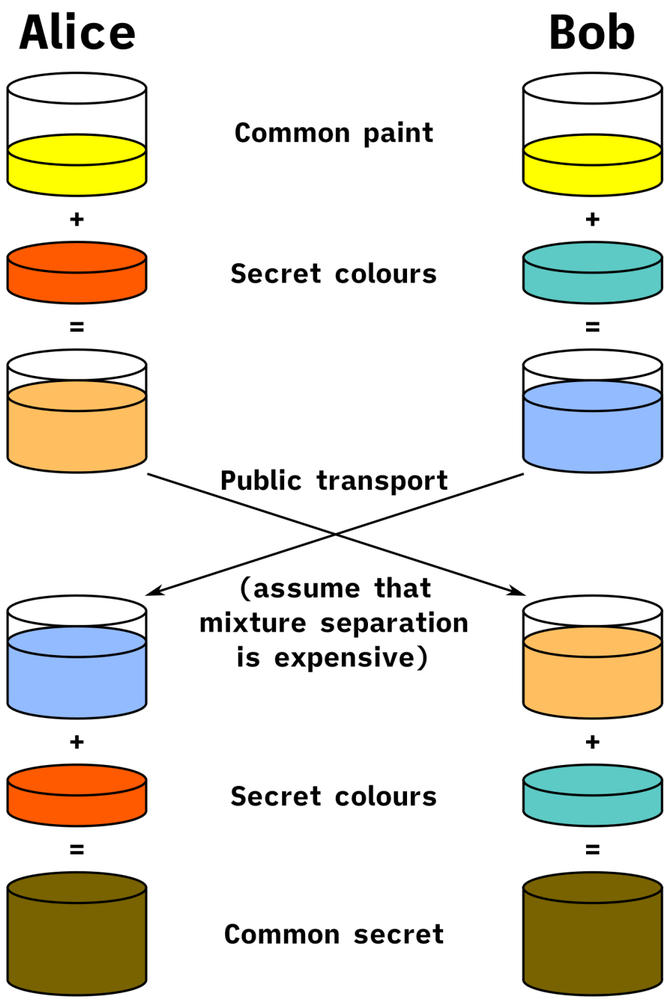
- each user (eg. B) generates their key
  - chooses a secret key (number): $x_B < q$
  - compute their **public key**: $y_B = \alpha^{x_B} \bmod q$
- shared session key for users A & B is K:

  $K = y_A^{x_B} \bmod q$ (which **B** can compute)

  $K = y_B^{x_A} \bmod q$ (which **A** can compute)


Agree upon two numbers:
P Prime Number 13
G Generator of P 6
Private = 5
Randomly generate a Private Key
Private = 4
(6^5) MOD 13
(7776) MOD 13
Public = 2
Calculate Public Key:
(G^Private) MOD P
(6^4) MOD 13
(1296) MOD 13
Public = 9
Exchange Public Keys
(9^5) MOD 13
(59049) MOD 13
Shared Secret = 3
Calculate the Shared Secret
(Shared Public^Private) MOD P
(2^4) MOD 13
(16) MOD 13
Shared Secret = 3
PRACTICAL NETWORKING .NET


Alice
Mallory
Bob
$g^a \bmod p$
$g^m \bmod p$
$g^m \bmod p$
$g^b \bmod p$
$K_1 = g^{am} \bmod p$
$K_1 = g^{am} \bmod p$
$K_2 = g^{bm} \bmod p$
$K_2 = g^{bm} \bmod p$



Diffie-Hellman Key Exchange

Alice

Bob

Bob and Alice know and have the following :
$p = 23$ *(a prime number)* $g = 11$ *(a generator)*

Alice	Bob
Alice chooses a secret random number a = 6	Bob chooses a secret random number b = 5
Alice computes : $A = g^a \bmod p$ $A = 11^6 \bmod 23 = 9$	Bob computes : $B = g^b \bmod p$ $B = 11^5 \bmod 23 = 5$
Alice receives B = 5 from Bob	Bob receives A = 9 from Alice
Secret Key = $K = B^a \bmod p$	Secret Key = $K = A^b \bmod p$
$K = 5^6 \bmod 23 = 8$	$K = 9^5 \bmod 23 = 8$

The common secret key is : 8

N.B. We could also have written : $K = g^{ab} \bmod$

Example

- users Alice & Bob who wish to swap keys:
- agree on prime q=353 and α=3
- select random secret keys:
  - A chooses x_A=97, B chooses x_B=233
- compute public keys:
  - $y_A = 3^{97} \bmod 353 = 40$ (Alice)
  - $y_B = 3^{233} \bmod 353 = 248$ (Bob)
- compute shared session key as:

  $K_{AB} = y_B^{x_A} \bmod 353 = 248^{97} = 160$ (Alice)

  $K_{AB} = y_A^{x_B} \bmod 353 = 40^{233} = 160$ (Bob)

Assessment 1

1. Which one of the following algorithm is not used i
cryptography?
a) rsa algorithm
b) diffie-hellman algorithm
c) electronic code book algorithm
d) dsa algorithm

2. Which is the key exchange algorithm used in CipherSuite parameter?
a) RSA
b) Fixed Diffie-Hellman
c) Ephemeral Diffie-Hellman
d) Any of the mentioned

REFERENCES

1. William Stallings, Cryptography and Network Security, 6 th Edition, Pearson Education, March 2013.

THANK YOU