SNS COLLEGE OF ENGINEERING
Kurumbapalayam(Po), Coimbatore – 641 107
An Autonomous Institution
Accredited by NAAC-UGC with 'A' Grade
Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

DEPARTMENT OF INFORMATION TECHNOLOGY

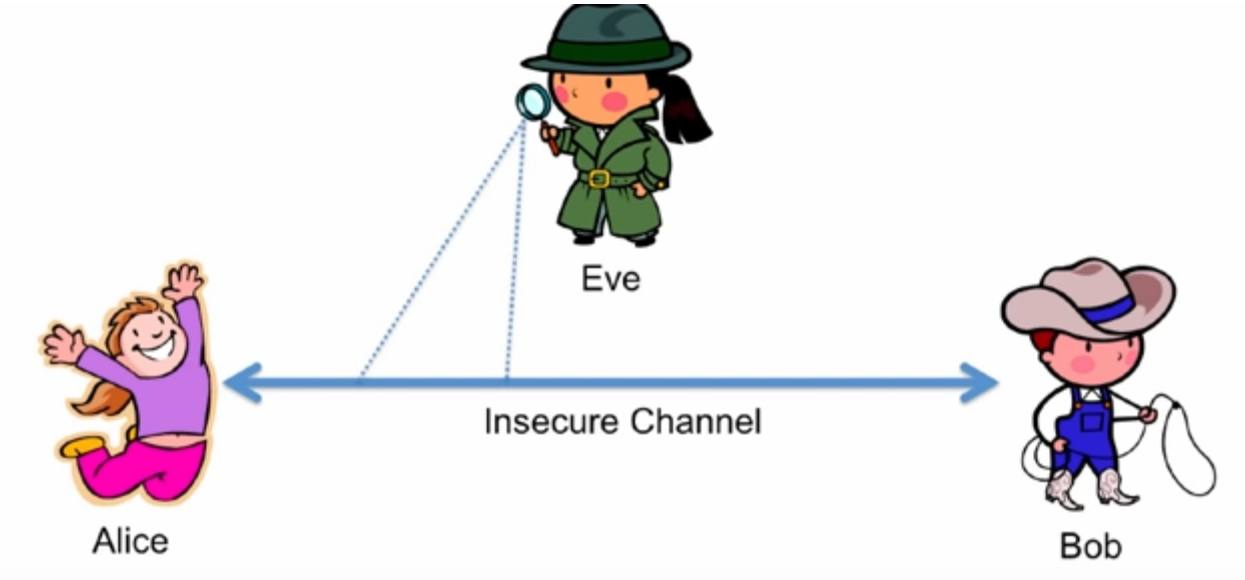
Course Code and Name : 19IT602– CRYPTOGRAPHY AND CYBER SECURITY

III YEAR / VI SEMESTER

Unit 3: ASYMMETRIC KEY CRYPTOGRAPHY

Topic : Diffie Hellman key exchange

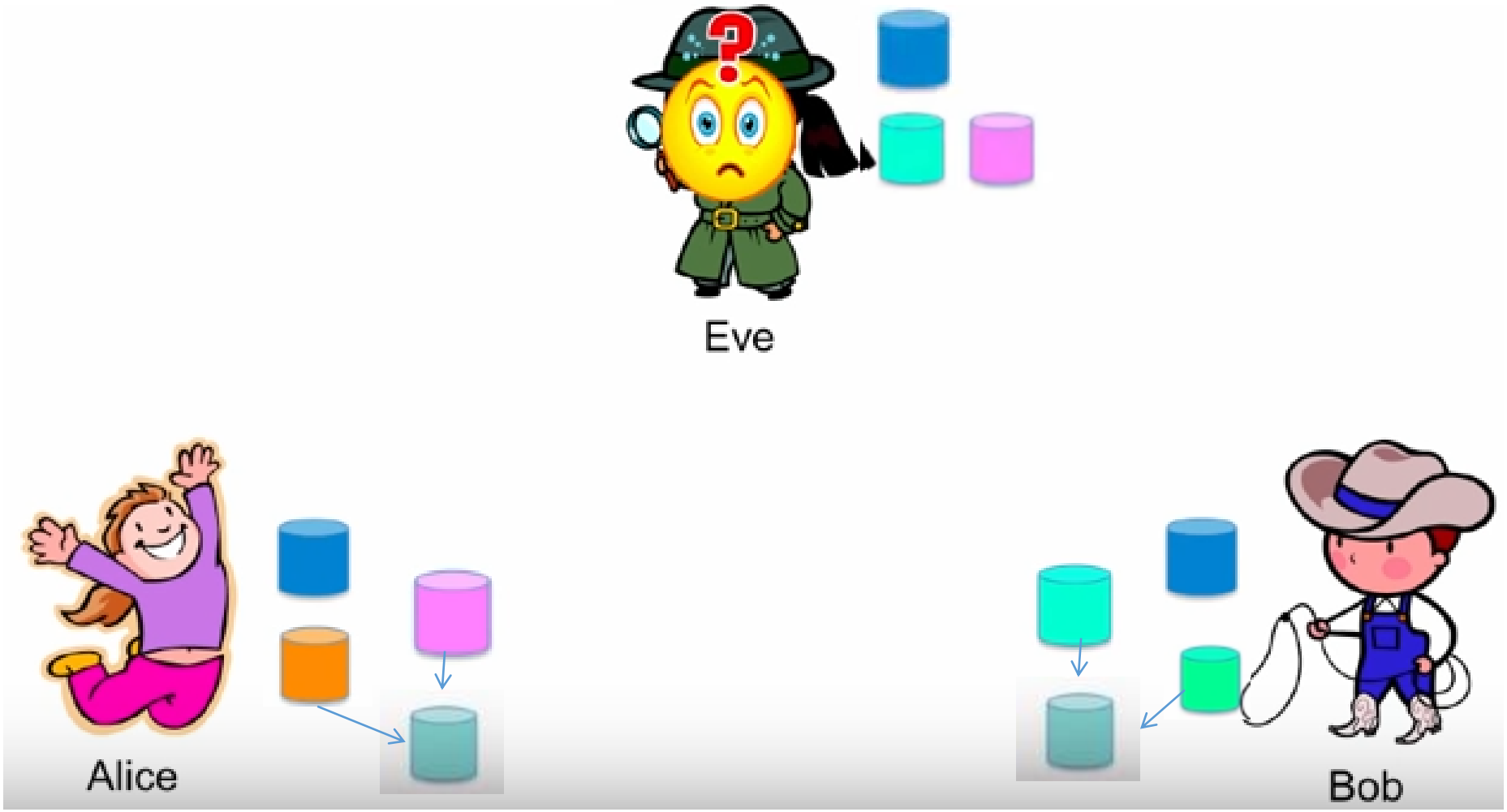
Problem with the network



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)

Example

- users Alice & Bob who wish to swap keys:
- agree on prime $q=353$ and $\alpha=3$
- 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:

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

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

Thank You