SWINBURNE UNIVERSITY OF TECHNOLOGY

Theory of Blockchain

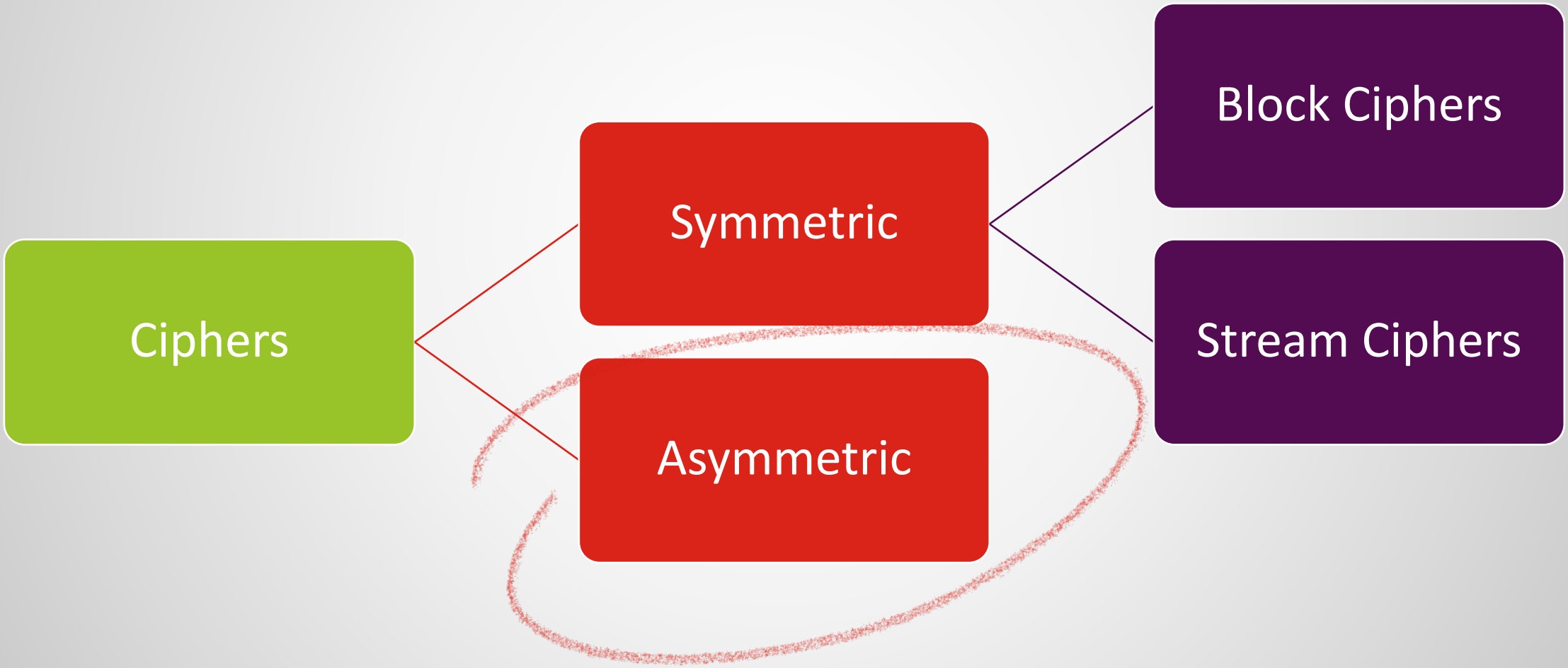
Session 3:

Asymmetric Cryptography - Part 1

Module 2 – Diffie-Hellman (DH) Key Agreement

Classification of Ciphers

Asymmetric Cryptography (Public Key Cryptography)



Diffie-Hellman (DH) Key Exchange Protocol

The goal is that two independent parties, A and B, who have had no contacts previously, can make a symmetric key using a common channel without sending the key over it.

- RSA's security was based on the difficulty of the factoring problem.

- DH's security is based on the difficulty of another mathematical problem which is so called the Discrete Logarithm problem.

Discrete Logarithm

Consider the prime number q. Among 1,…,q-1, some are called the “primitive roots” or generators since they create the whole set of 1,…,q-1 numbers by being powered to different numbers modulo q.

q=5, a=2

a=2,

a^2 mod p = 4,

a^3 mod p = 3,

a^4 mod p = 1

For any $1 \leq b \leq q-1$

Easy

i is not modulo p

$$b = a^i \ mod \ q$$

$$i = dlog_a \mathrm{b}$$

Hard

Diffie-Hellman Protocol

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

User A Key Generation	
Select private X_A	$X_A < q$
Calculate public Y_A	$Y_A = \alpha^{X_A} \bmod q$

User B Key Generation	
Select private X_B	$X_B < q$
Calculate public Y_B	$Y_B = \alpha^{X_B} \bmod q$

Generation of Secret Key by User A

$K = (Y_B)^{X_A} \bmod q$

Generation of Secret Key by User B

$K = (Y_A)^{X_B} \bmod q$

Diffie-Hellman Key Agreement

Private key part of user A

X_A

$Y_A = \alpha^{X_A} \mod q, \quad \{\alpha, q\}$

$Y_B = \alpha^{X_B} \mod q$

$K = (\alpha^{X_B})^{X_A} \mod q$
$= \alpha^{X_A X_B} \mod q$

Private key part of user B

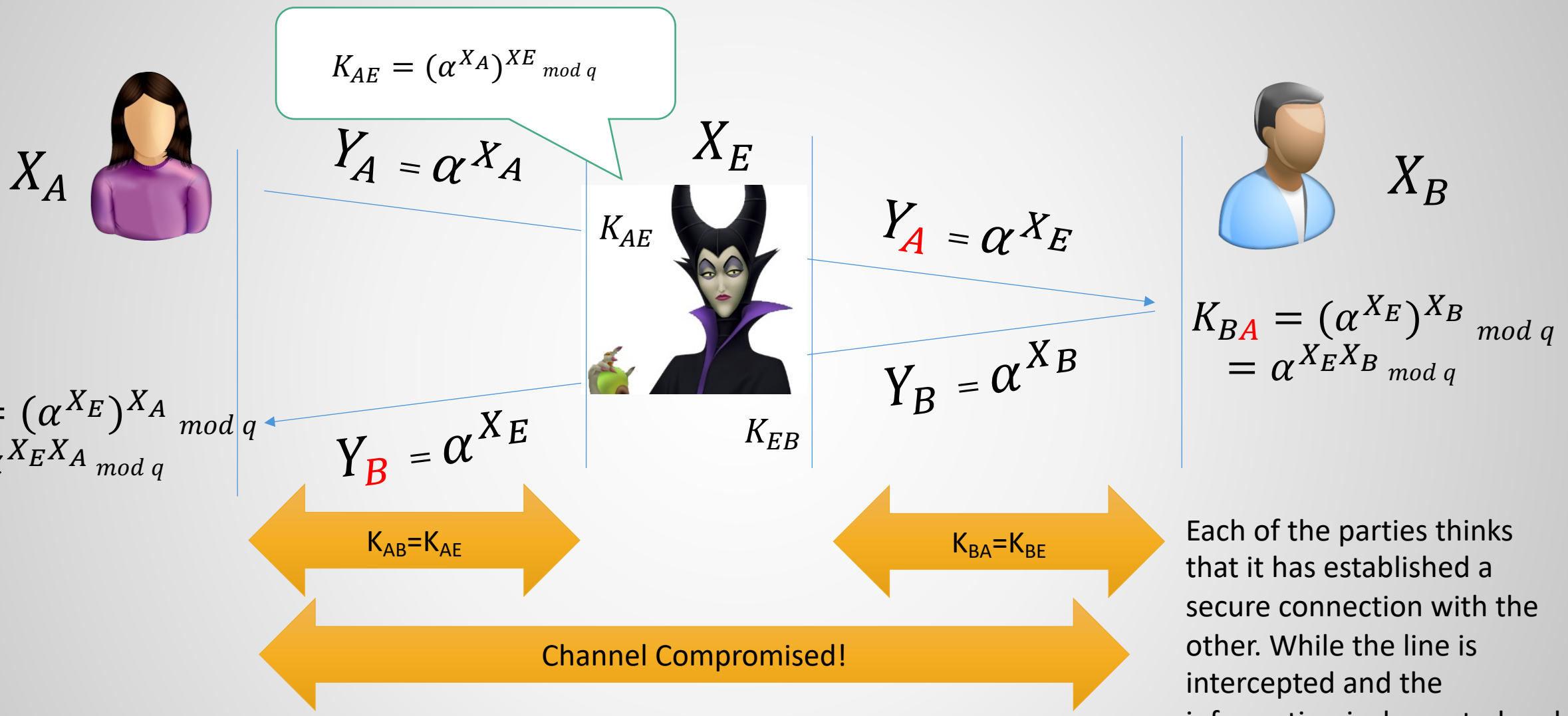
X_B

$K = (\alpha^{X_A})^{X_B} \mod q$
$= \alpha^{X_A X_B} \mod q$

Secured Channel with the Key K

q & α are both public values and can be used by any adversary

Man in the Middle Attack



Each of the parties thinks that it has established a secure connection with the other. While the line is intercepted and the information is decrypted and re-encrypted at the middle.

What Comes Next …

- We learned about the difficulty of discrete logarithm.
- We learned how Diffie-Hellman protocol creates a mutual symmetric key between two parties.
- In the next video, we explain the concept of digital signature and introduce a few famous signature algorithms.

See you in the next video …