SWINBURNE UNIVERSITY OF TECHNOLOGY

# Theory of Blockchain

## Session 4:

## Asymmetric Cryptography - Part 2

Module 3 – Basics of Zero Knowledge

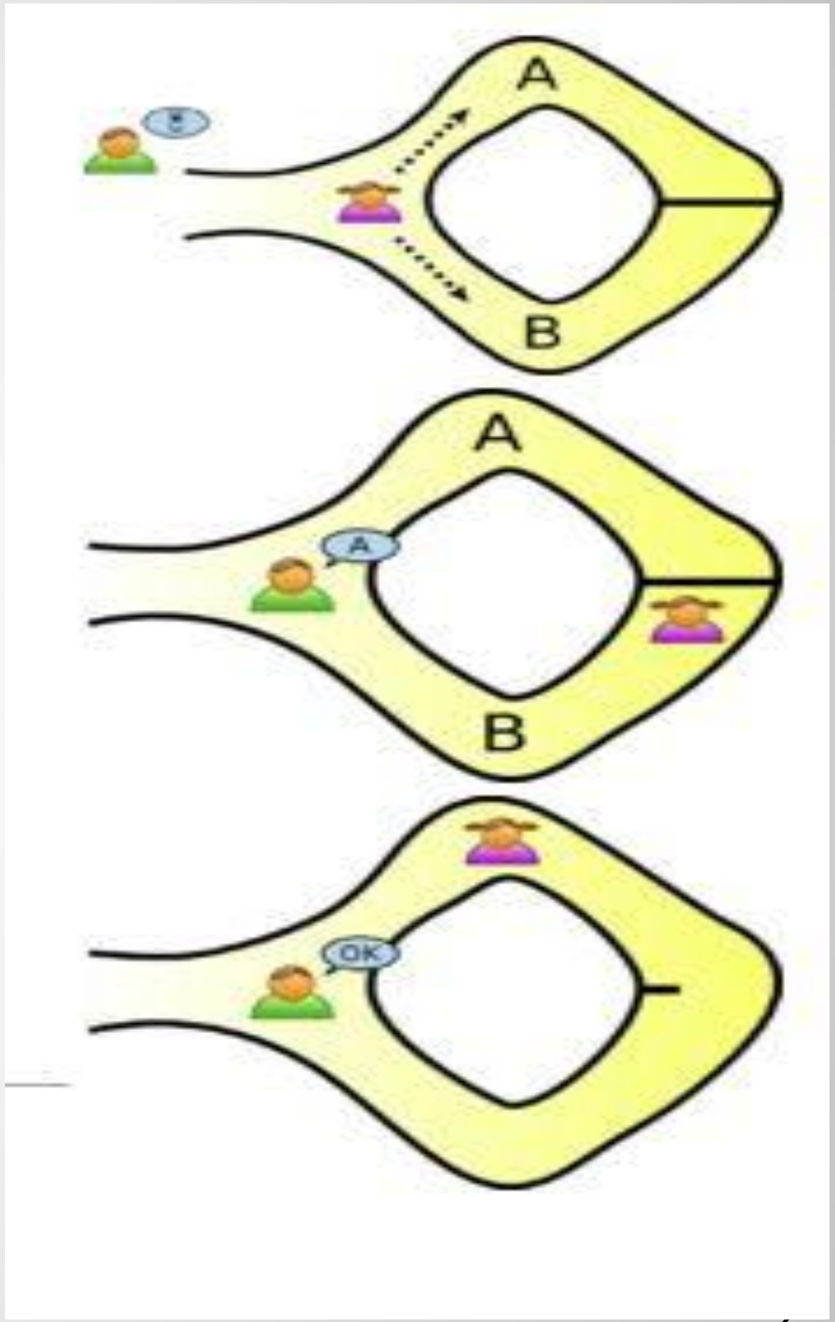
# Zero Knowledge Proof

It’s a way of proving that you know something (e.g. a key or a password), without revealing it.

**Example:**

Alice claims she knows the key to the door in the cave. Bob wants to verify.

Alice goes in first, Bob stands at the entrance and randomly shouts A or B. Alice should come back from that route.



# Zero Knowledge Proof

- ZKPs are based on challenge-response.
- Can be iterative or non-iterative.
- Can be used for authentication without leaking information
  - There's no information going on the channel that's confidential
  - Nothing can be inferred from eavesdropping the challenge-response(s)
  - Can be robust against malicious verifiers because you don't give away your password or anything related to it.

Robust to Dictionary Attack

# Example

- given a value $Y$, a large prime $p$ and a generator $g$, Alice wants to prove that she knows a value $x$ such that $g^x \, mod \;\; p = Y$ , without revealing $x$ . (basically the response to a discrete logarithm problem)

This could be used for authentication if Alice gave the verifiers her $y$ beforehand.

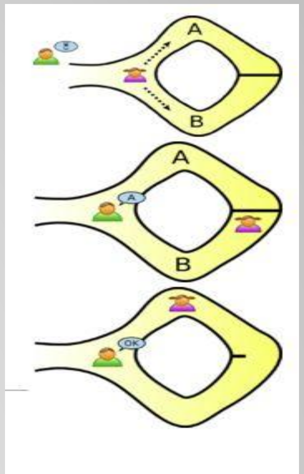
# Example

- in each round, Alice generates a random number $r$, computes $C = g^r \ mod \ p$ and discloses this to Bob.
- After receiving $C$, Bob randomly issues one of the following two requests: he either requests that Alice discloses
  1. the value of $r$ , or
  2. the value of $(x + r) \ mod \ (p - 1)$
- With either answer, Alice is only disclosing a random value, so no information is disclosed by a correct execution of one round of the protocol.

# Example

- Bob can verify either answer;
  1. if he requested $r$, he can then compute $g^r \mod p$ and verify that it matches C.
  2. If he requested $(x + r) \mod (p - 1)$, he can verify that $C$ is consistent with this, by computing $g^{(x+r) \mod (p-1)} \mod p$ and verifying that it matches $C \cdot Y \mod p$ .
- Repeated questions can authenticate Alice with high probability (1-1/2^n).
- If Alice indeed knows the value of x, she can respond to either one of Bob's possible challenges. Otherwise, it's 50/50.
  - Alice can cheat if she knows what question is being asked.

# Visual Presentation




Bob

Alice

$picks\ r$

$C = g^r \mod p$

$C$

$send\ r \quad or \quad x + r \ ?$

$r \quad or \quad x + r$

$g^r = C \mod p?$

or

$g^{x+r} = C.Y \mod p?$

.

.

.

# What Comes Next …

- We learned about the concept of zero knowledge.
- We saw an iterative protocol for zero knowledge proof.
- In the next module, we explain the basics of distributed ledger and consensus problem.

See you in the next video …