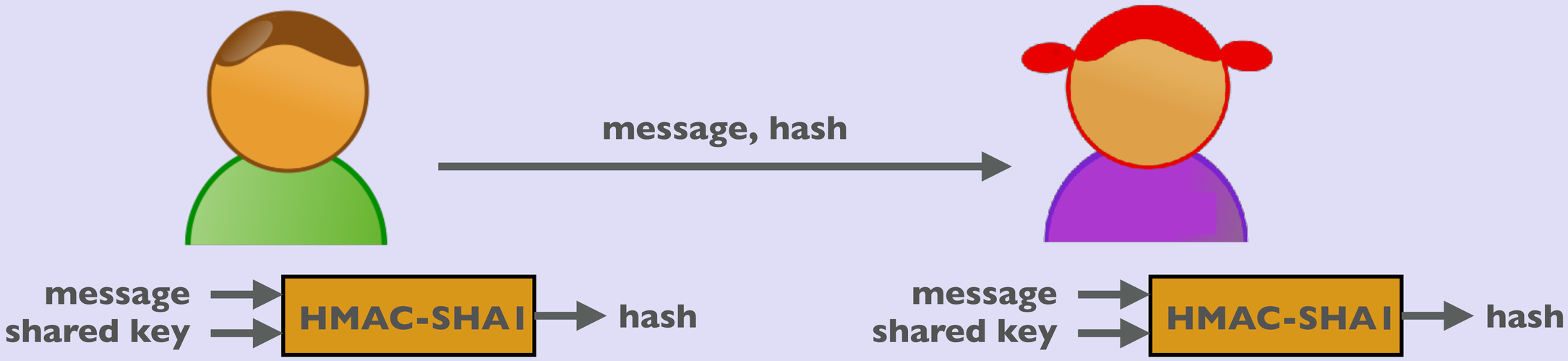
BLOCKCHAIN TUTORIAL 30

HMAC



INTRO

- In this tutorial I will explain what HMAC is.

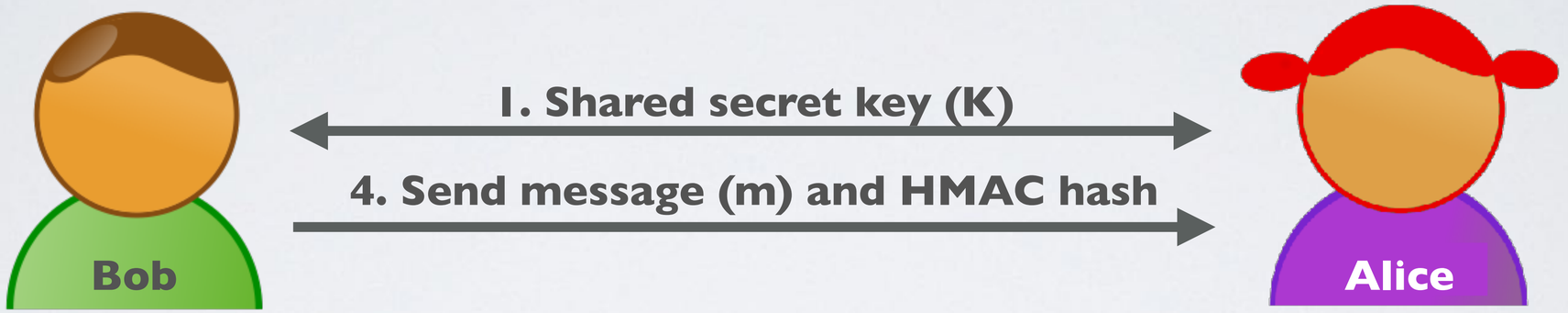
HMAC

- HMAC stands for Hashed-based Message Authentication Code and is used to verify the integrity and authenticity of a message.

- HMAC can be used with any iterative cryptographic hash function e.g., MD5, SHA-1, SHA-256, SHA-512 in combination with a shared secret key.
  If used with MD5, it is called HMAC-MD5.
  If used with SHA-1, it is called HMAC-SHA1.
  etc.
  More info: https://www.ietf.org/rfc/rfc2104.txt

- Once the HMAC hash is calculated, the message must be sent alongside the HMAC hash.

HOW HMAC IS USED



3. Bob calculates HMAC hash

5. Alice calculates HMAC hash

6. Alice verifies the
message integrity and authenticity by:
received HMAC hash == calculated HMAC hash

HMAC

- To compute HMAC over a message m the following steps are applied:
  HMAC (K,m) = H((K ⊕ opad) ‖ H((K ⊕ ipad) ‖ m))

- HMAC is constructed by hashing the XOR of the secret key K with the outer padding opad concatentated with the hash of the secret key K XORed with the inner padding ipad concatenated with the message.

- The values opad and ipad are constants and were arbitrarily chosen by the HMAC designers.

- opad is the byte value 0x5C repeated B times.
  ipad is the byte value 0x36 repeated B times.
  Where B is the blocksize in bytes of the underlying hash function (MD5, SHA-1, etc.)

HMAC

- To compute HMAC in a more “understandable" way:
  HMAC (K,m) = H((K ⊕ opad) ‖ H((K ⊕ ipad) ‖ m))

- inner_key = K ⊕ ipad
  outer_key = K ⊕ opad

- inner_hash = H(inner_key ‖ m)

- HMAC(K,m) = H(outer_key ‖ inner_hash)