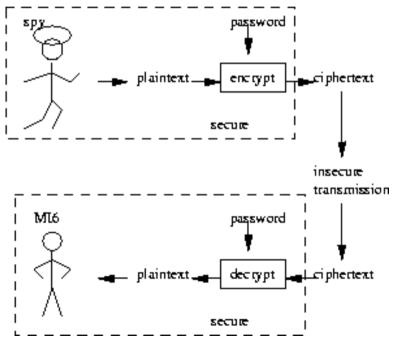
Blockchain Cryptography

Introduction to Cryptography

Cryptography is an important aspect when we deal with network security. 'Crypto' means secret or hidden.



Source: Stanford

Types of Cryptography

- Symmetric aka Private Key Cryptography
- Asymmetric aka Public Key Cryptography

Symmetric Cryptography

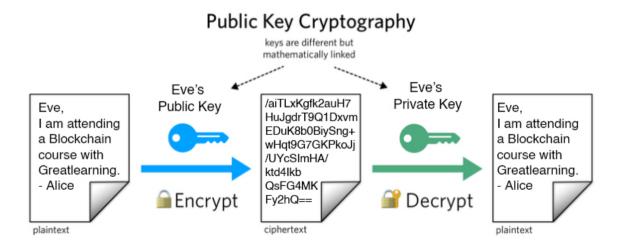
Alice

- 1. Construct m
- 2. Compute c = F(m, k)
- 3. Send c to Bob

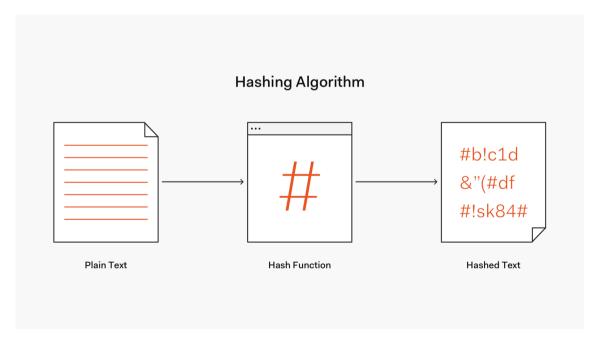
Bob

- 4. Receive c from Alice
- 5. Compute $d=F^{-1}(c, \mathbf{k})$
- 6. m = c

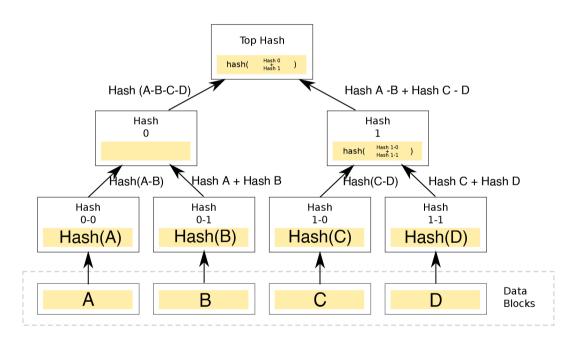
Asymmetric Cryptography



Hashing



Merkle Trees



Thank You