Basic Concepts of Cryptography

- **Symmetric Key Cryptography**
  - Same key used for encryption and decryption
  - How to share the key securely
  - Cannot address certain requirements

- **Public Key Cryptography**
  - One key for encryption, one for decryption
  - Handles several requirements like those in blockchain

Digital Signature

- A **digital code**, which can be included with an electronically transmitted document to verify
  - The content of the document is authenticated
  - The identity of the sender
  - Prevent *non-repudiation* – sender will not be able to deny about the origin of the document

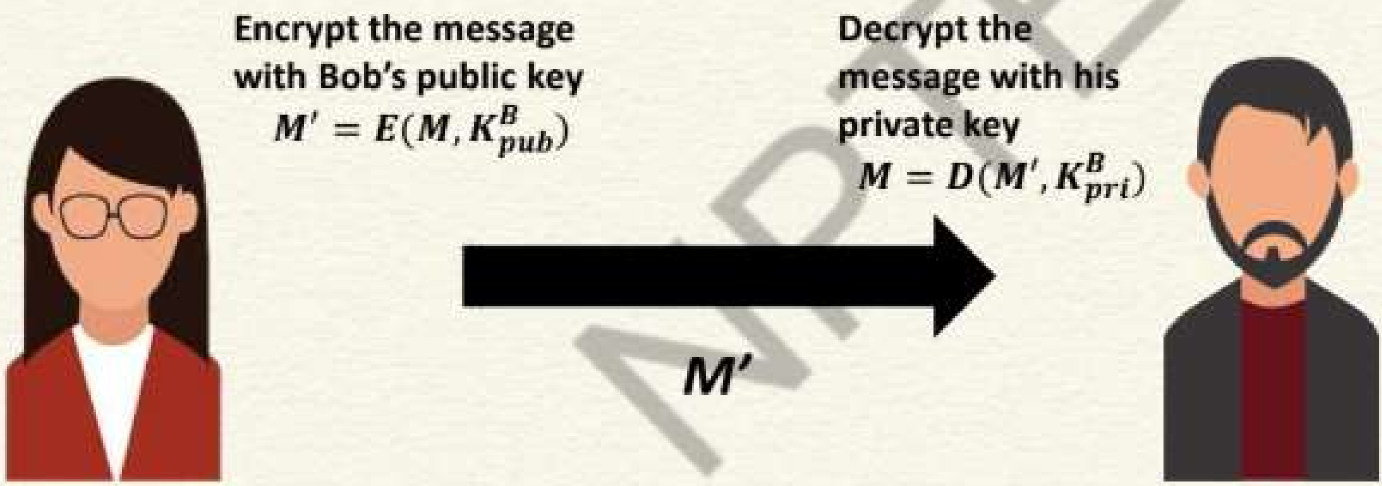
Public Key Cryptography

- Also known as **asymmetrical cryptography** or **asymmetric key cryptography**

- **Key:** A parameter that determines the functional output of a cryptography algorithm
  - **Encryption:** The key is used to convert a plain-text to a cypher-text; $M' = E(M, k)$
  - **Decryption:** The key is used to convert the cypher-text to the original plain text; $M = D(M', k)$

Public Key Cryptography

- Two keys are used
  - **Private key**: Only Alice has her private key
  - **Public key:** “Public” to everyone – everyone knows Alice’s public key



RSA Key Generation and Distribution

- Chose two distinct prime integers p and q
  - p and q should be chosen at random to ensure tight security
- Compute $n = pq$; n is used as the modulus, the length of n is called the key length
- Compute $\phi(n) = (p-1)(q-1)$ (*Euler totient function*)
- Choose an integer e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$; e and $\phi(n)$ are co-prime
- Determine $d \equiv e^{-1}(mod\ \phi(n))$: d is the *modular multiplicative inverse* of $e(mod\ \phi(n))$

  [Note $d.e \equiv 1(mod\ \phi(n))$]