BLOCKCHAIN TECHNOLOGY

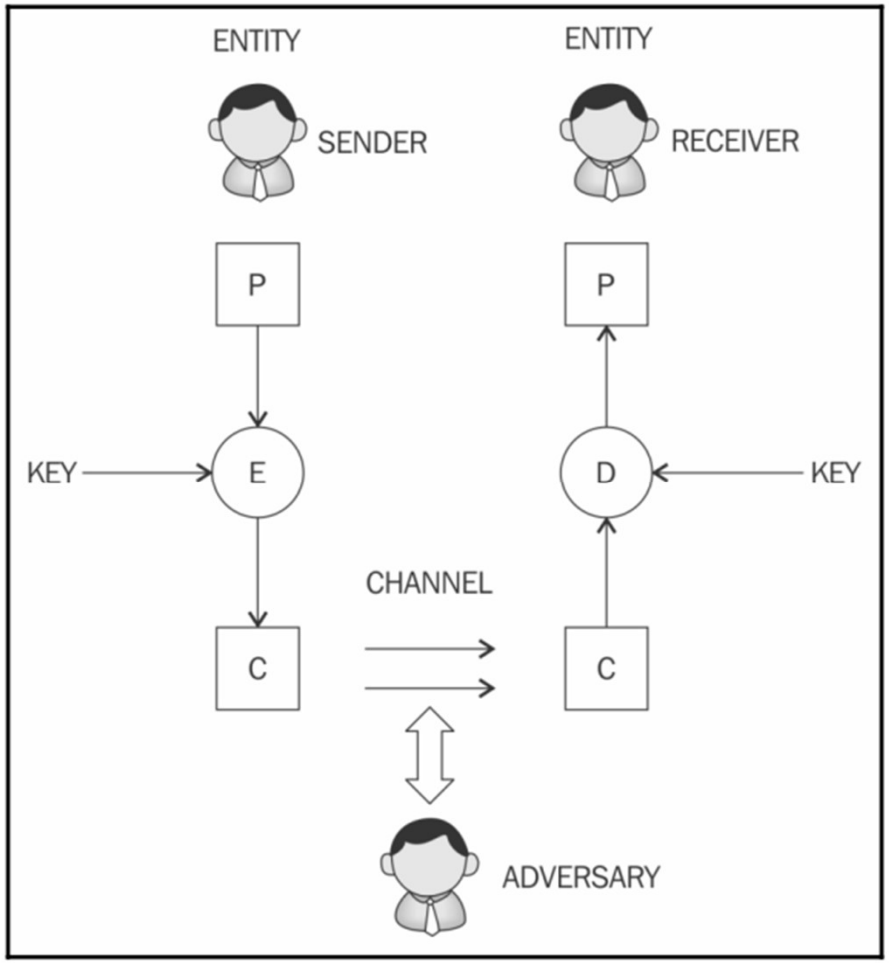
Symmetric Cryptography

Introduction

- Cryptography
  - the science of making information secure in the presence of adversaries.
  - under the assumption that limitless resources are available to adversaries.
- Ciphers
  - algorithms used to encrypt or decrypt data
    - The data is meaningless to adversary without decryption
      - which requires a secret key.

Introduction

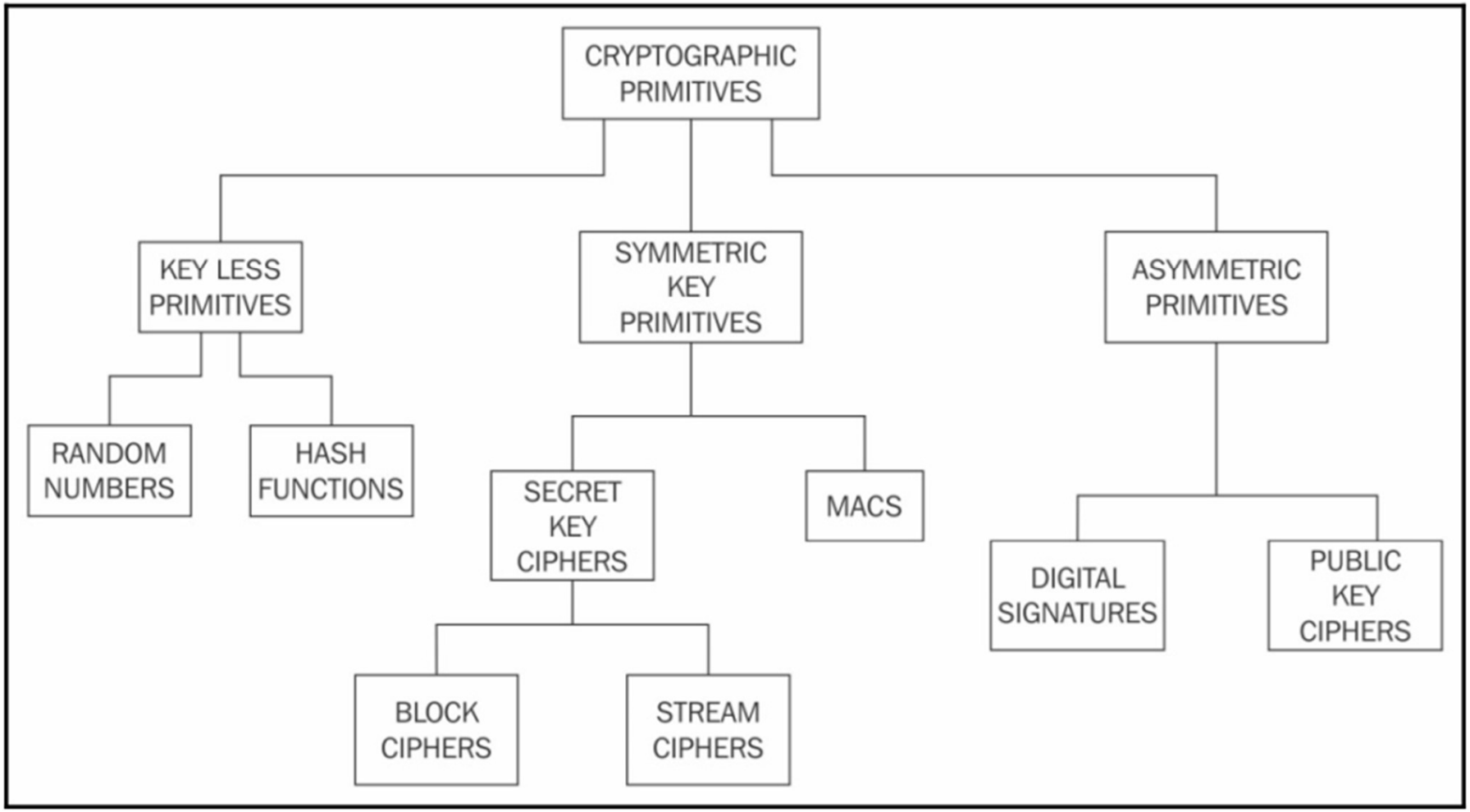
- Cryptography



Introduction

- Cryptography
  - primarily used to provide a confidentiality service
    - the assurance that information is only available to authorized entities
  - also provides other security services
    - Integrity
      - the assurance that information is modifiable only by authorized entities
    - Authentication
      - The assurance about the identity of an entity or the validity of a message
    - Non-repudiation
      - the assurance that an entity cannot deny a previous commitment or action
    - Accountability
      - the assurance which states that actions affecting security can be traced back to the responsible party

Taxonomy of Cryptographic primitives

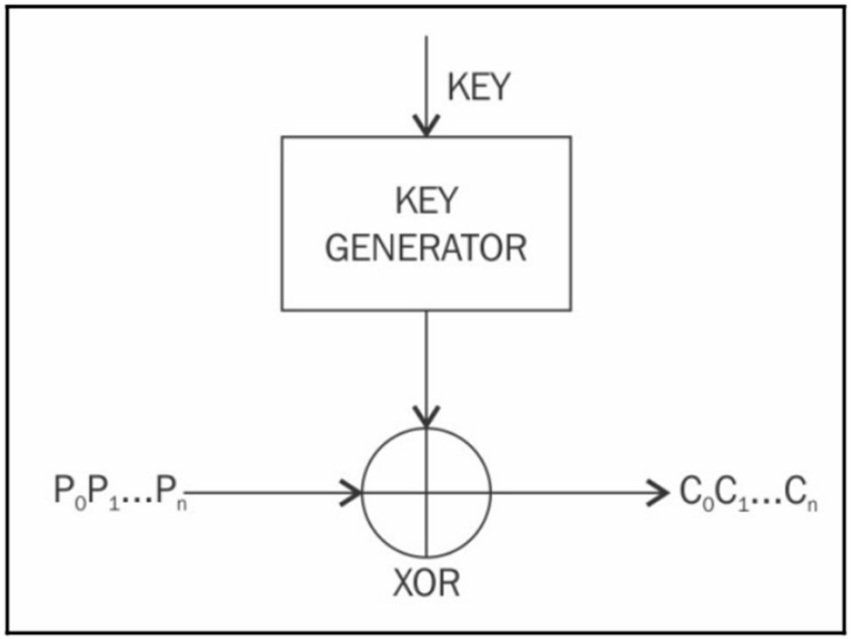


Symmetric cryptography

- Symmetric cryptography
  - Uses the same key both encryption and decryption
  - Also known as shared key cryptography
    - The key must be established or agreed upon before the data exchange occurs
  - Another name: secret key cryptography
  - Two types of symmetric ciphers
    - stream ciphers
      - E.g., RC_4 and A_5
    - block ciphers.
      - E.g., Data Encryption Standard (DES) and Advanced Encryption Standard (AES)

Symmetric cryptography

- Stream ciphers
  - apply encryption algorithms on a bit-by-bit basis to data using a keystream.
  - encryption and decryption are the same function
    - they are simple modulo-2 additions or XOR operations.

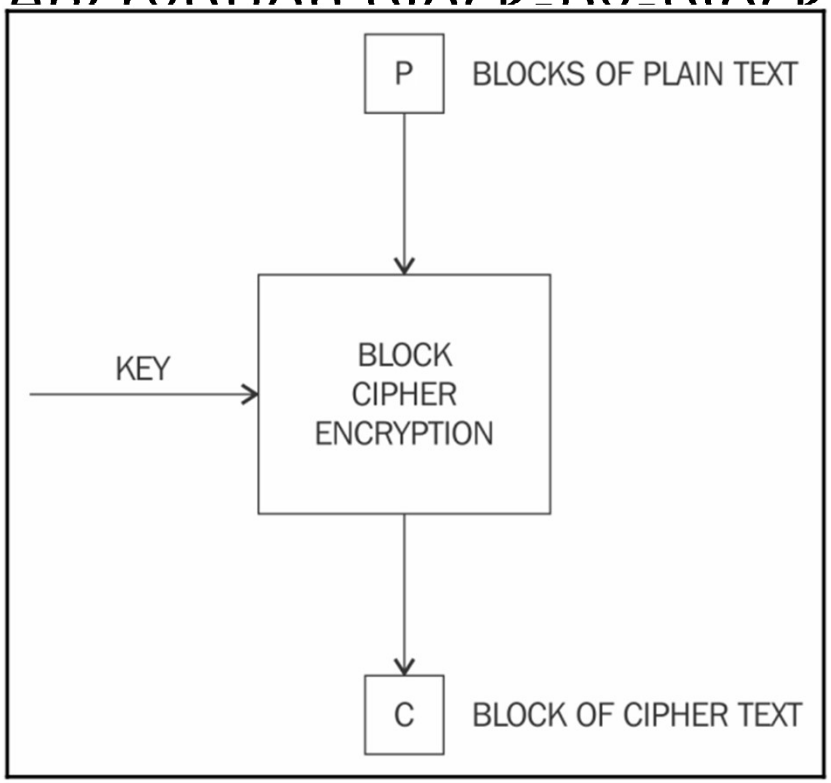


Symmetric cryptography

- Stream ciphers
  - Two types
    - synchronous stream ciphers
      - the keystream is dependent only on the key
    - asynchronous stream ciphers
      - have a keystream that is also dependent on the encrypted data
  - The fundamental requirement is the security and randomness of keystreams

Symmetric cryptography

- Block ciphers
  - break up the data to be encrypted into blocks of a fixed length
  - apply the encryption block-by-block



Symmetric cryptography

- Block ciphers
  - combine multiple rounds of repeated operations to achieve
    1. Confusion
       - makes the relationship between the encrypted text and plaintext complex
       - is achieved by substitution
       - In practice, A in plaintext is replaced by X in encrypted text.
       - In modern algorithms, it is performed using lookup tables called S-boxes
    - diffusion

Symmetric cryptography

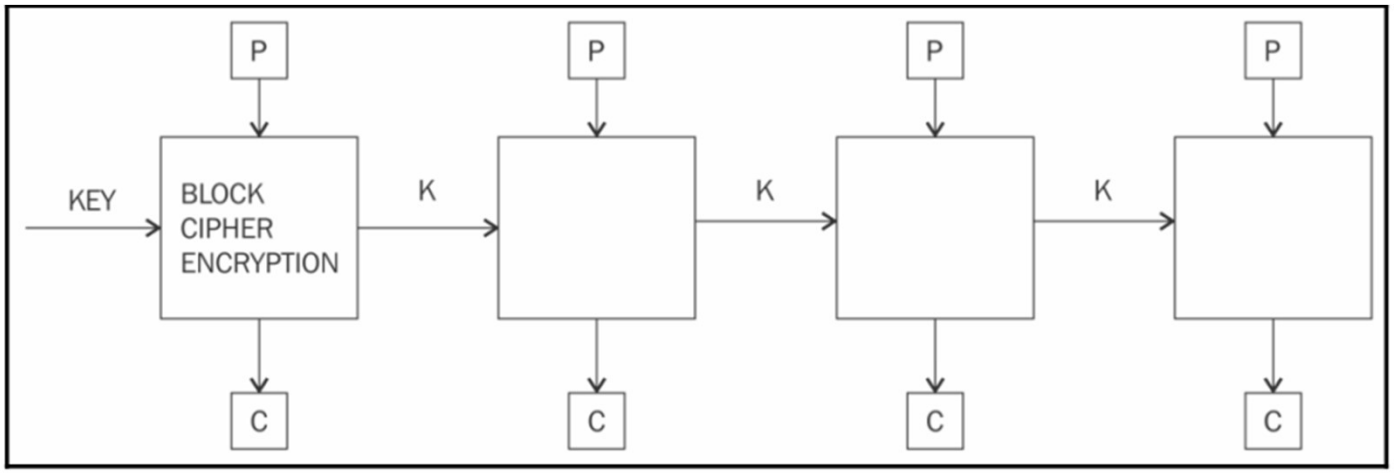
- Block ciphers
  - combine multiple rounds of repeated operations to achieve
    2. Diffusion
       - spreads the plaintext statistically over the encrypted data
       - ensures that
         - even if a single bit is changed in the input text
         - it results in changing at least half (on average) of the bits in the ciphertext

Symmetric cryptography

- Block ciphers
  - multiple modes of operation
    - Electronic Code Book (ECB)
    - Cipher Block Chaining (CBC)
    - Counter (CTR) mode

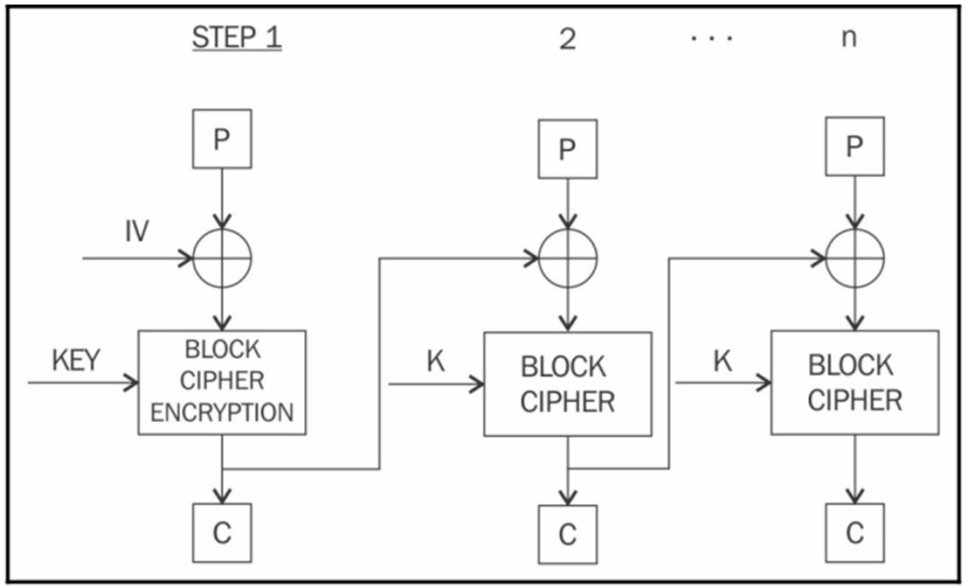
Symmetric cryptography

- Block ciphers
  - Electronic Code Book (ECB)
    - the most straightforward mode
    - applying the encryption algorithm one-by-one to each block of plaintext.
    - should not be used in practice
      - it is insecure and can reveal information



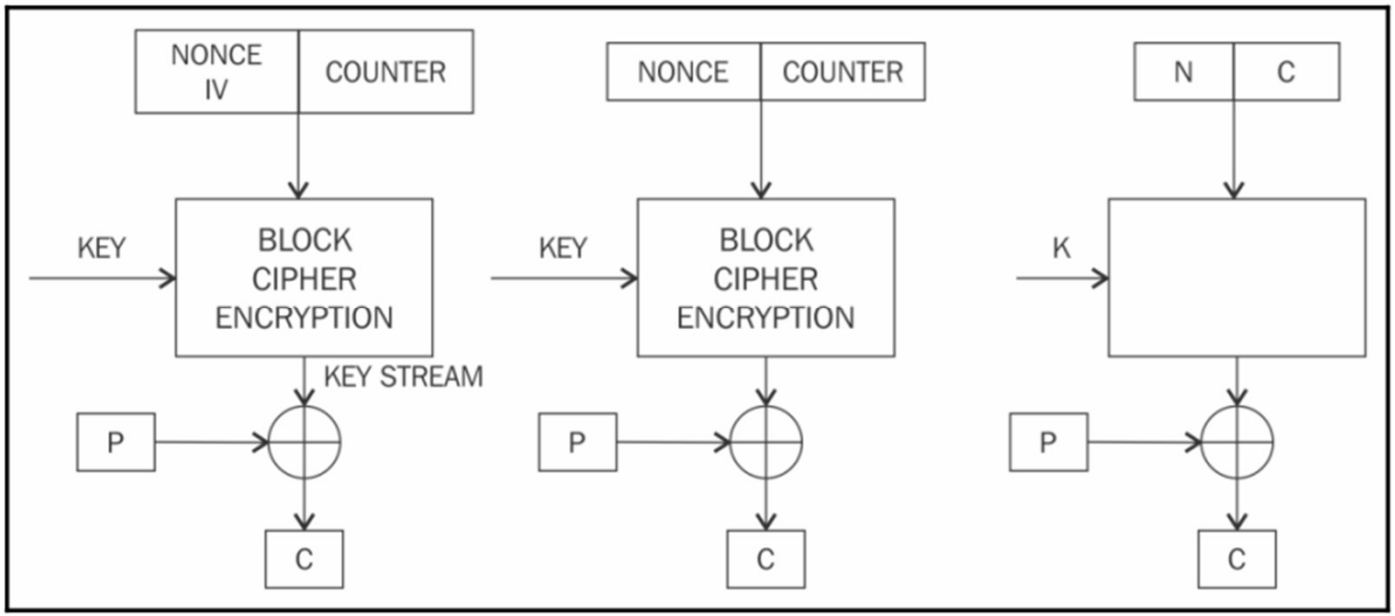
Symmetric cryptography

- Block ciphers
  - Cipher Block Chaining (CBC)
    - each block of plaintext is XOR'd with the previously-encrypted block
    - uses the Initialization Vector (IV) to encrypt the first block.
      - recommended that the IV be randomly chosen



Symmetric cryptography

- Block ciphers
  - Counter (CTR) mode
    - effectively uses a block cipher as a stream cipher.
    - a unique nonce is supplied that is concatenated with the counter value to produce a keystream



Symmetric cryptography

- Data Encryption Standard
  - introduced by the U.S. National Institute of Standards and Technology (NIST)
  - it was in widespread use during the 1980s and 1990s.
  - it did not prove to be very resistant to brute force attacks

Symmetric cryptography

- Data Encryption Standard
  - uses a key of only 56 bits
    - which raised some concerns
  - This problem was addressed with the introduction of Triple DES (3DES)
    - proposed the use of a 168-bit key
      - three 56-bit keys
      - the same number of executions of the DES algorithm
      - making brute force attacks almost impossible
    - other limitations
      - Slow performance
      - 64-bit block size

Symmetric cryptography

- Advanced Encryption Standard (AES)
  - In 2001, an encryption algorithm named Rijndael was standardized as Advanced Encryption Standard (AES).
  - So far, no attack has been found against AES that is more effective than the brute-force method.
  - The original version of Rijndael permits different key and block sizes
  - In the AES standard
    - only a 128-bit block size is allowed
    - key sizes of 128-bit, 192-bit, and 256-bit are permissible