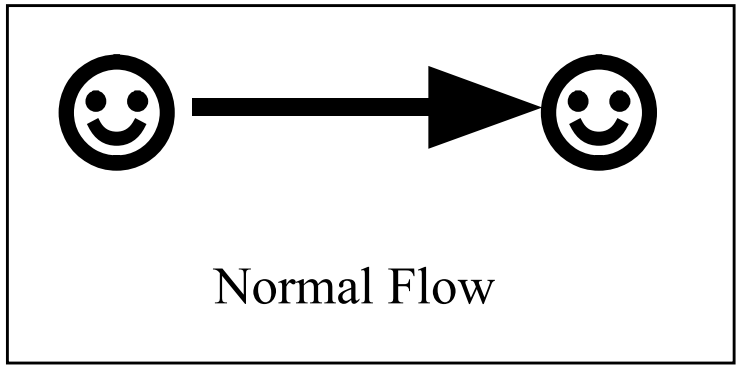
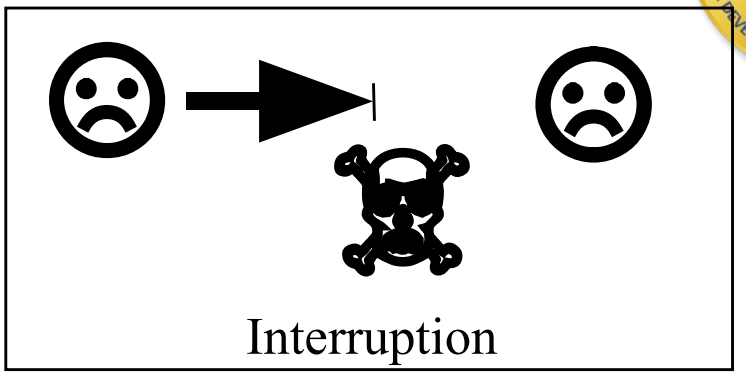
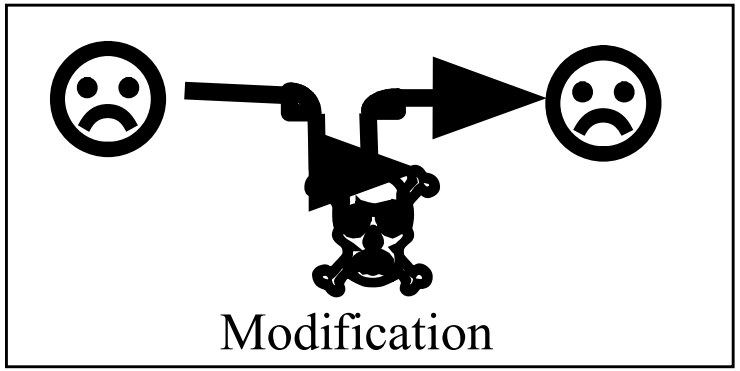
Understanding Cryptography behind Blockchain Technology

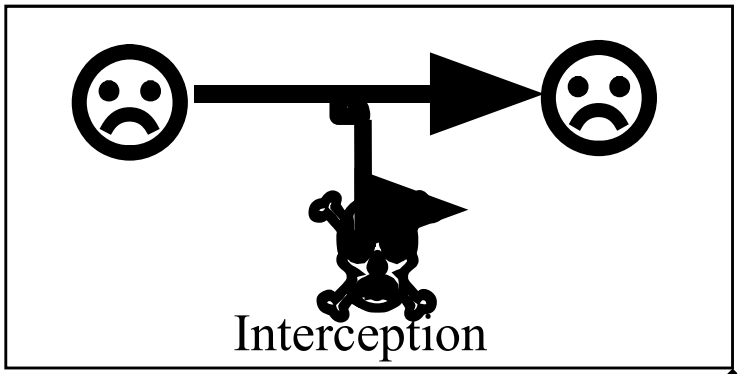
By
Ravi Kishore K,
C-DAC, Hyderabad

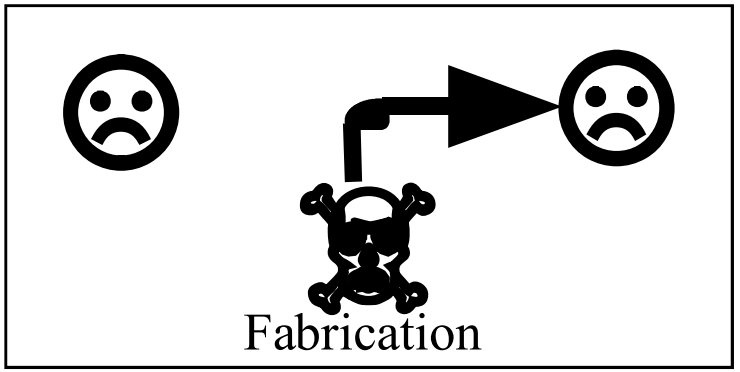
Network Security Issues

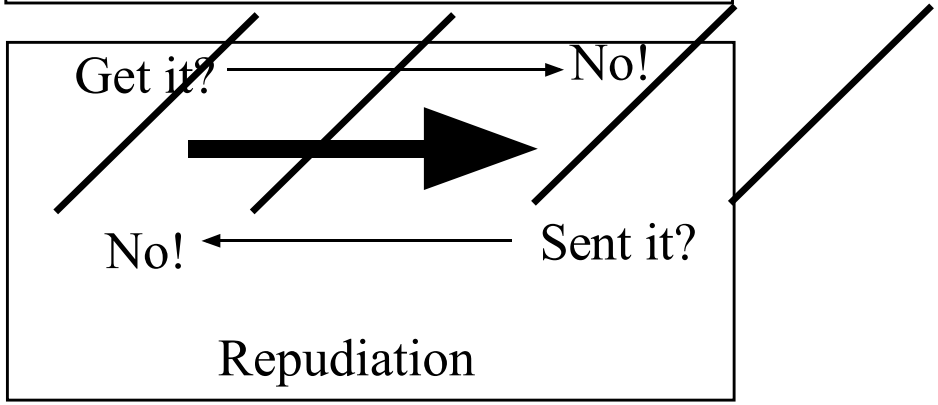












Network Security Services

Requirement

Availability

Integrity

Confidentiality

Authenticity

Non Repudiation

Security Mechanisms

- Confidentiality - Encryption
- Integrity - Hashing
- Non-Repudiation - Digital Signatures
- Authentication - Digital Certificates

Basic Terminology

Cryptology

Branch of maths that studies the mathematical foundation of cryptographic methods

Cryptography

Art of secret (crypto) writing (-graphy)

Cryptanalysis

Art of breaking ciphers

Basic Cryptography Terminology

- **Plaintext** - the original message
- **Ciphertext** - the coded message
- **Cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **Encipher (encrypt)** - converting plaintext to ciphertext
- **Decipher (decrypt)** - recovering plaintext from ciphertext
- **Cryptography** - study of encryption principles/methods
- **Cryptanalysis (code breaking)** - the study of principles/ methods of deciphering ciphertext *without* knowing key
- **Cryptology** - the field of both cryptography and cryptanalysis

Cryptographic Algorithms

Types of Cryptographic Algorithms

- Secret key cryptography or Symmetric Key
- Public key cryptography or Asymmetric Key
- Hash functions

Types of Cryptosystems

- Secret Key or Symmetric Cryptography

  DES, IDEA, AES etc

  Advantages: *fast, cipher text secure*

  Disadvantages: *must distribute key in advance, key must not be divulged*

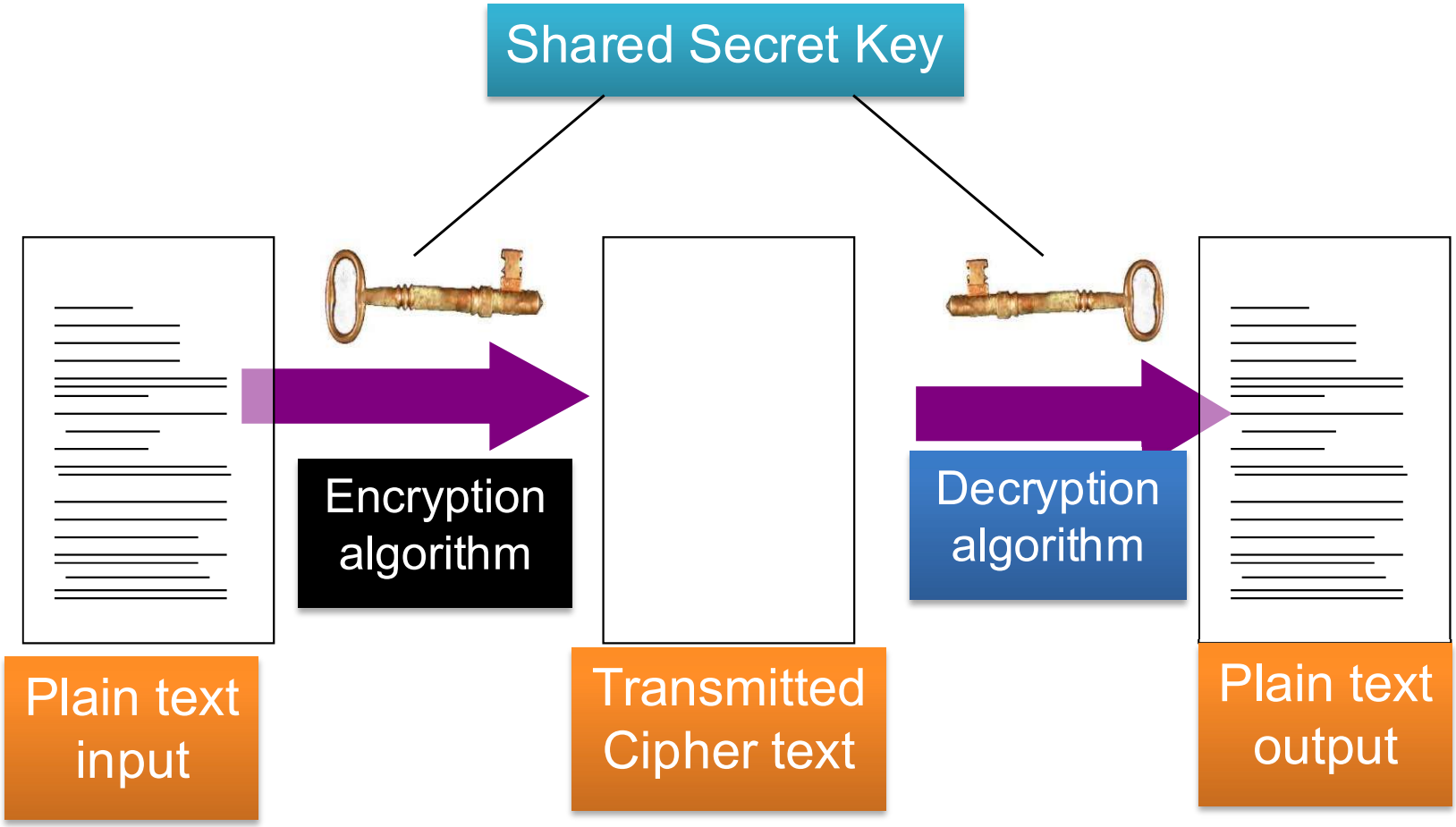
- Public-key or Asymmetric Cryptography

  RSA, Diffie-Hellman key agreement protocol

  Advantages: *public key widely distributable, does digital signatures*

  Disadvantages: *slow*

Secret Key Algorithms



Confidentiality

Types

- Block Cipher: Operates on a block of message or plaintext at a time

  Ex: DES, IDEA,AES etc
- Stream Cipher: Operates on each character in the message or text individually

  Ex: RC4, SEAL, A5/1 (used in GSM)

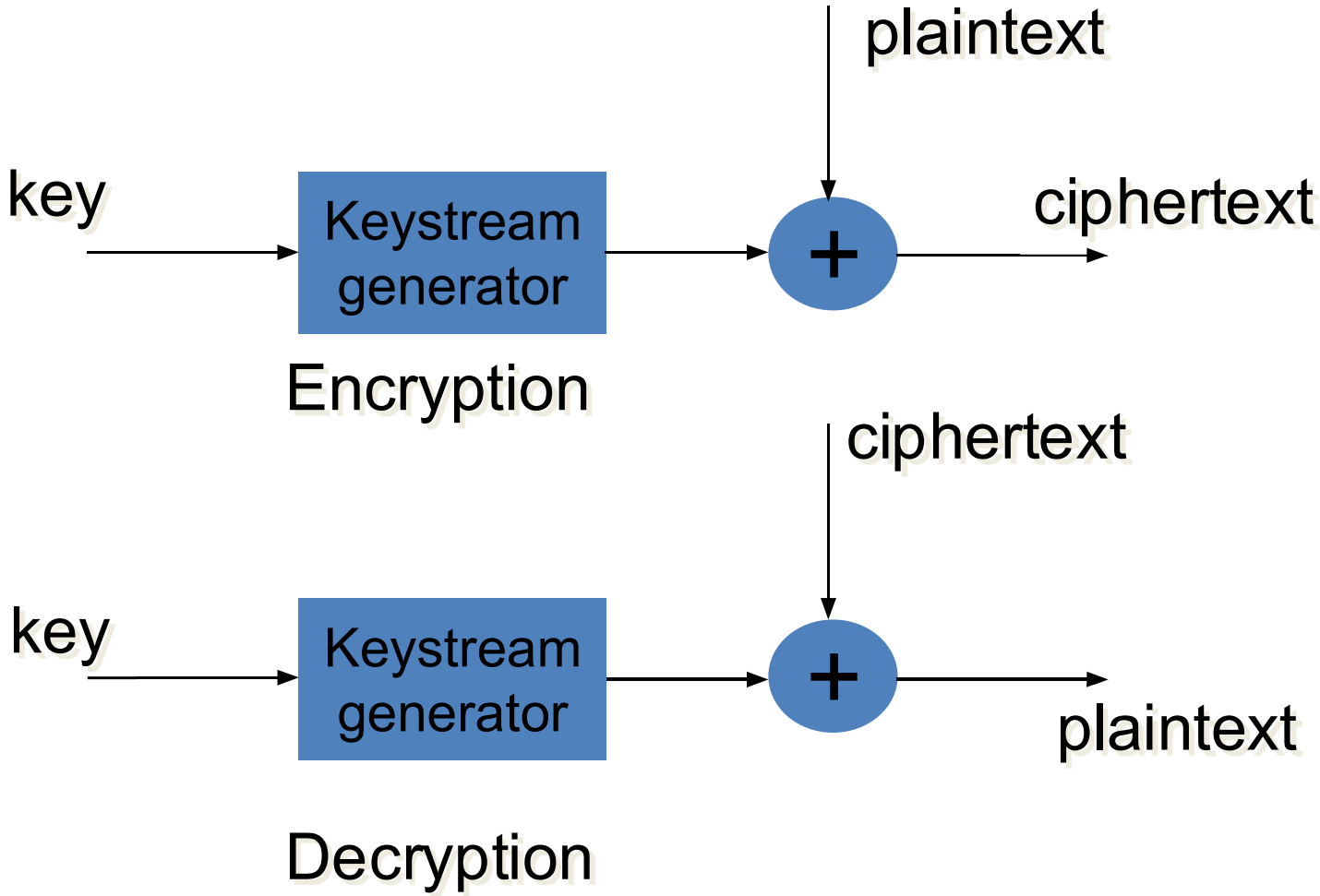
Other Secret key algorithms

- IDEA (International Data Encryption Algorithm)
  - 128 bit key, 8 rounds
- Blowfish
  - Variable key length. (up to 448 bits). Generally 128 bit key used. 16 rounds.
  - Easy to implement and high execution speed
- AES (Advanced Encryption Standard)
  - Variable block length (128, 192, 256 bits)
  - Variable key length (128, 192, 256 bits)
  - Ease of implementation in software and hardware.

Stream Cipher

- A pseudo random no. generator continuously generates bits known as running key or keystream.
- xoring the keystream to the plain text produces the cipher text.
- e.g. RC4, SEAL, A5/1 (used in GSM)

Stream Cipher

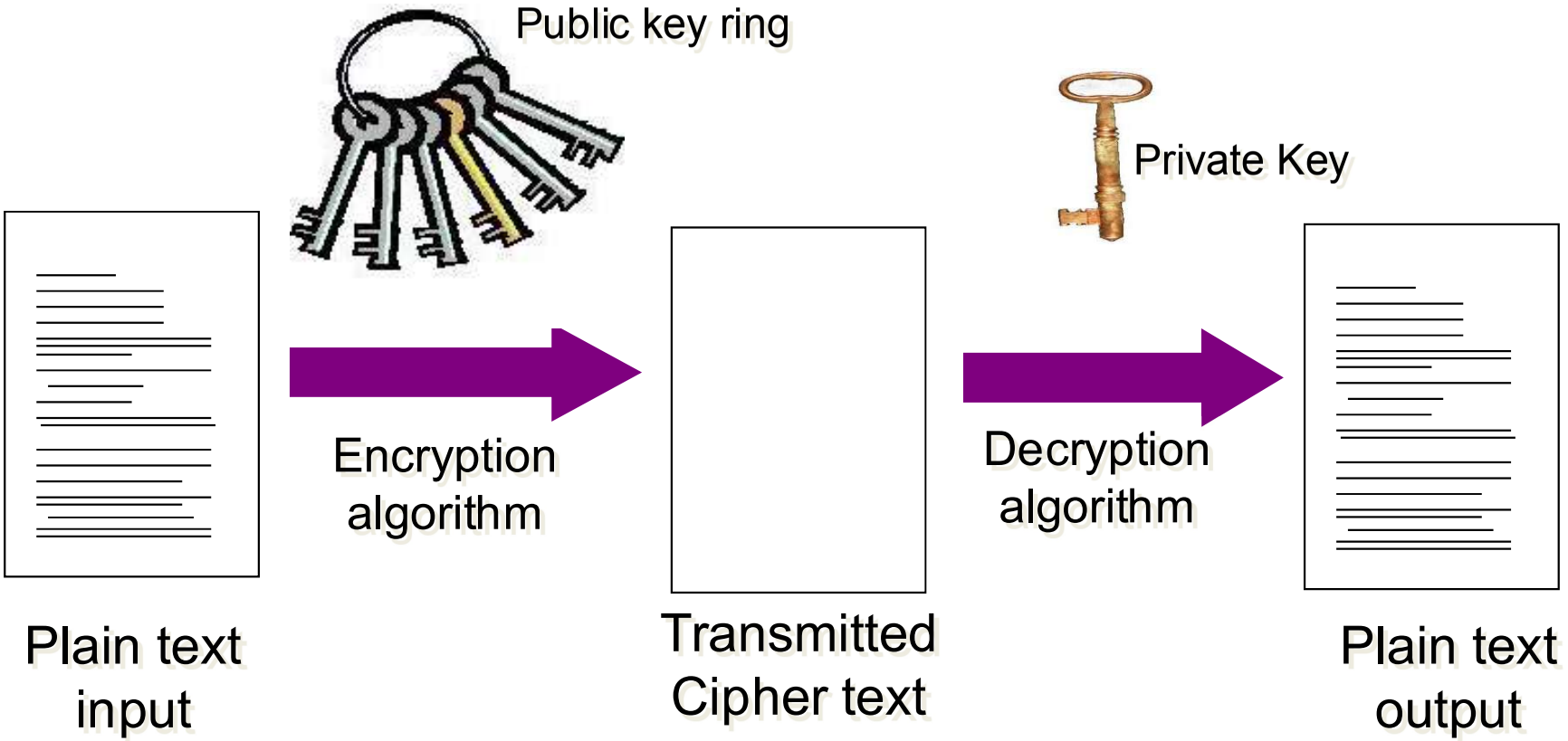


Keystream Generator is a pseudo random generator like linear feedback shift register

Key Distribution

- Symmetric schemes require both parties to share a common secret key
- Issue is how to securely distribute this key
- Often secure system failure due to a break in the key distribution scheme

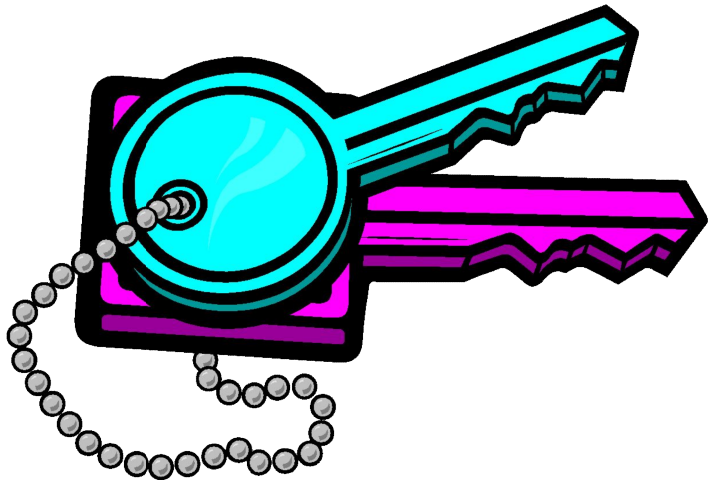
Public Key Algorithms



Confidentiality

Public Key Cryptography

- Uses two keys: private & public
- Used for
  - Confidentiality
  - Authentication
  - Key distribution



Public Key Cryptography

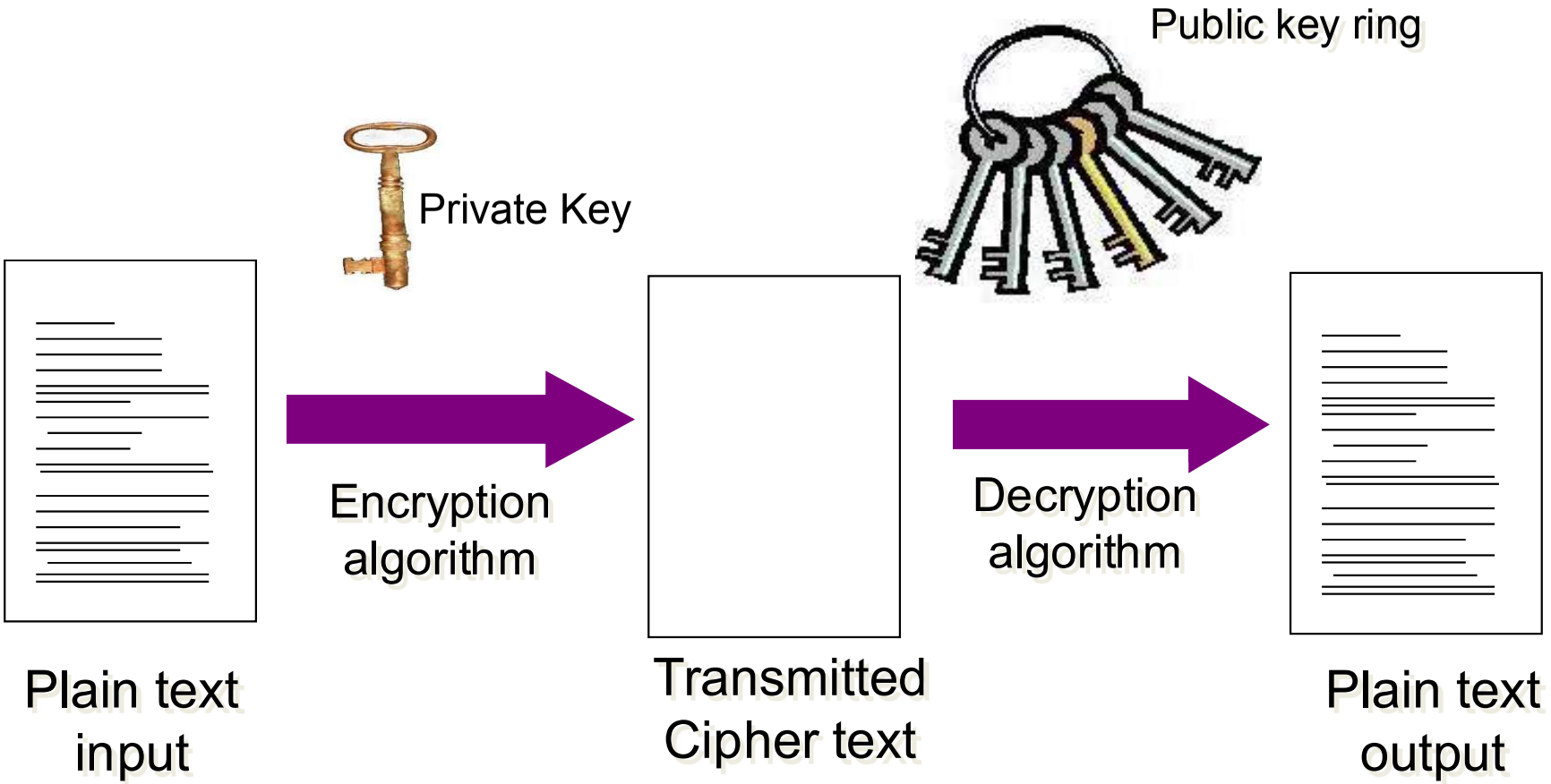
Confidentiality

- The sender encrypts using public key of receiver
- Only the receiver can decrypt the cipher message with his private key

Strength of Cryptographic Algorithms
Identify the weakest links

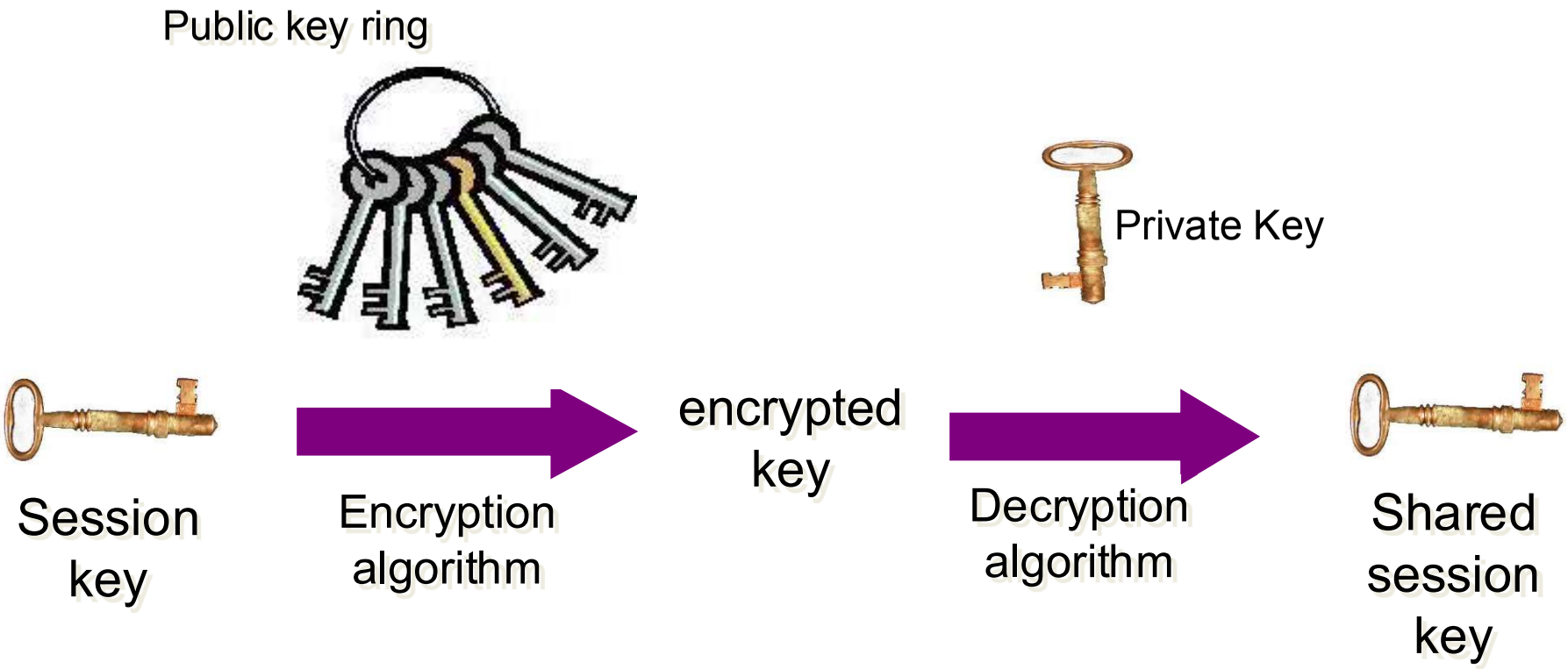
- Key length: key can be broken by brute force attack. For a 32 bit key, max. possible combinations are 2^{32}. Hence size of key is crucial.
  - Symmetric algorithms: key size currently used is 128 bits
  - Public key algorithms: require much larger key sizes since an extra structure i.e. public key is available to cryptanalyst. Hence keys with 1024 bits and more are safer.

Public Key Algorithms



Authentication

Public Key Algorithms



Key Exchange

Symmetric vs. Asymmetric

- Asymmetric
  - Fastest implementation of RSA (asymmetric) can encrypt kilobits/sec
    - 2048-bit key
- Symmetric
  - Fastest implementation of DES (symmetric) can encrypt megabits/sec
    - 56-bit key

The Hybrid Model

Very common practice: hybrid symmetric and asymmetric

- Asymmetric encryption is used to share a secret key, which is then used for symmetric encryption
- Advantages
  - Speed of symmetric, flexibility of asymmetric

Integrity

- Encryption protects only against passive attack

- Integrity
  - A message digest is computed which is appended to message using hash functions.

Hash Functions

- Hash function s Map any sized data to a fixed size

- Example: H(x)=x%n where x and n are integers and % is the modular (remainder after division by n) operations. x can be of any arbitrary length, but H(x) is within the range l [0..n-1]

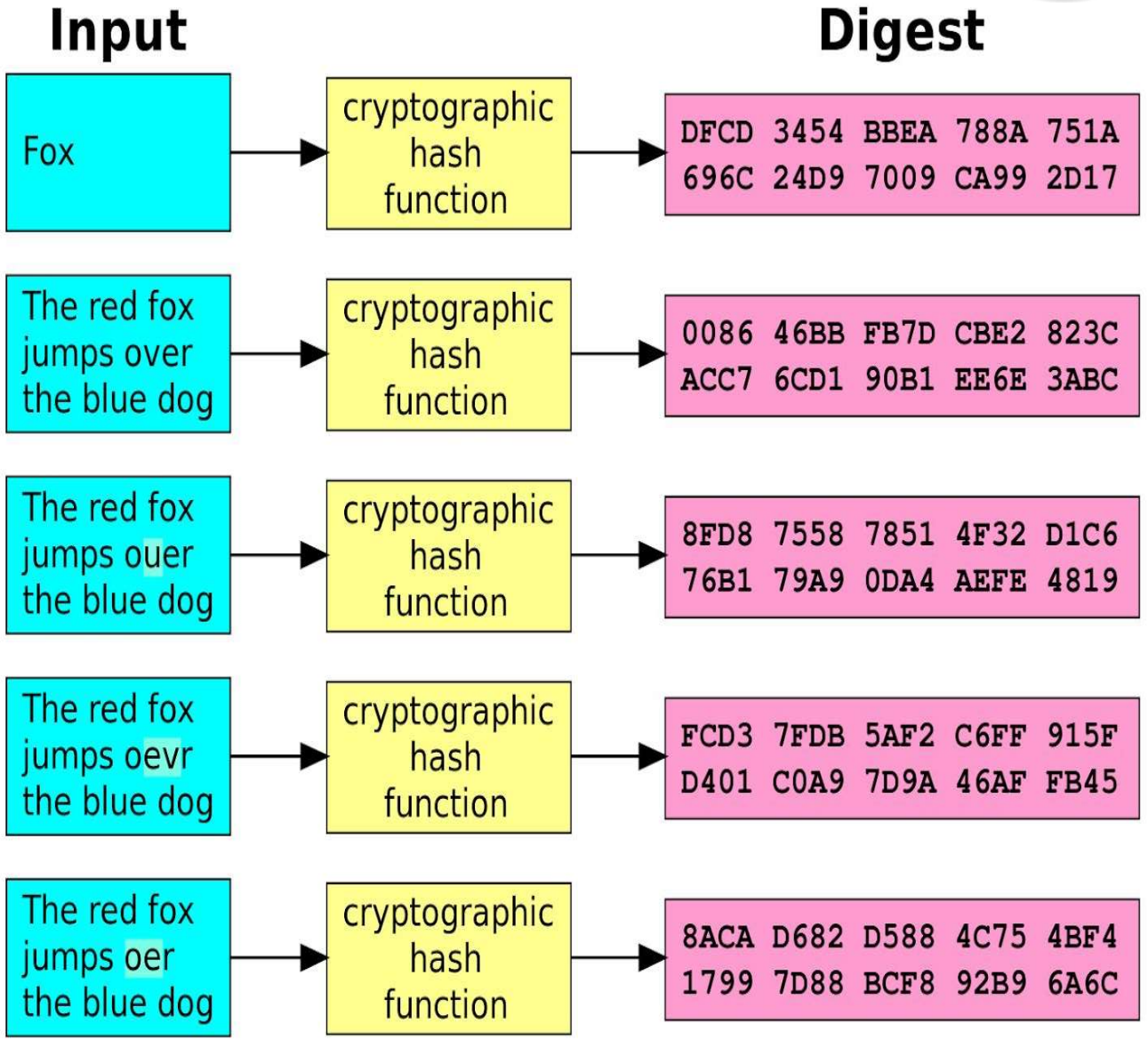
Cryptographically Secured Hash Functions

- One way, given x, we can compute H(x), but given H(x), no deterministic algorithm can compute x

- For two different x_1 and x_2, $H(x_1)$ and $H(x_2)$ should be different

Cryptographically Secured Hash Functions

- Examples: MD5, SHA256
- x is called the **message** and H(x) is called the **message digest**
- A small change in the data results in a significant change in the output – called the **avalanche effect**



Cryptographic Hash Function: Properties

- Collision-Free
  - If two messages are different then their message digest also differs
- Hiding
  - Hide the original message (Avalanche effect)
- Puzzle-friendly
  - Give X and Y, find out k such that Y=H(X||k) – used to solve the mining puzzle in Bitcoin PoW

Hash Function – SHA256

- SHA256 is used in Blockchain
- Secure Hash Algorithm (SHA) that generates 256 bit message digest
- A part of SHA-2 group of algorithms, a set of cryptographic hash functions designed by United States National Security Agency (NSA)

Purpose of Digital Signature

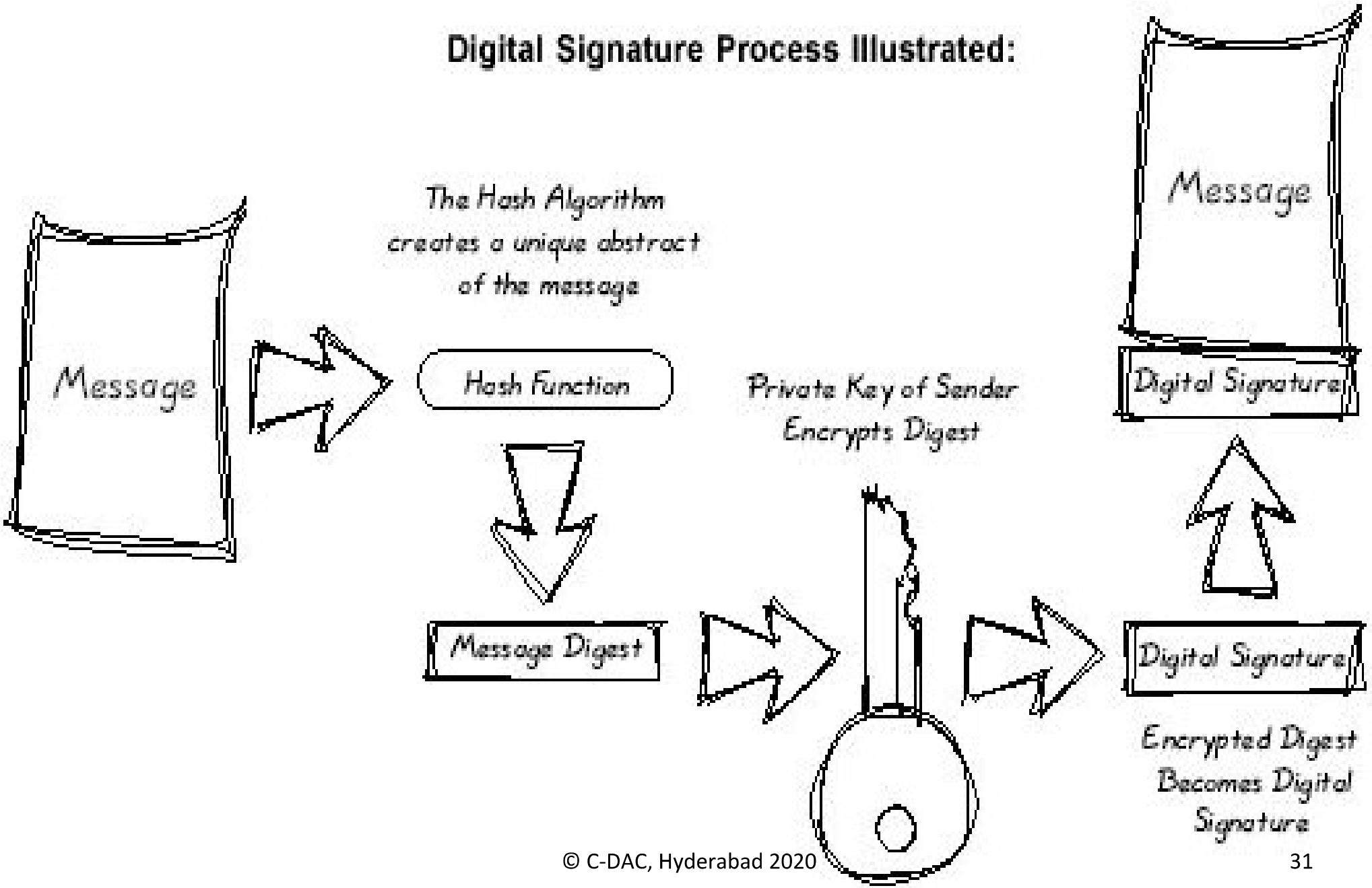
- Only the signing authority can sign a document, but everyone can verify the signature
- Signature is associated with the particular document
  - Signature of one document cannot be transferred to another document

How Digital Signature is Generated?

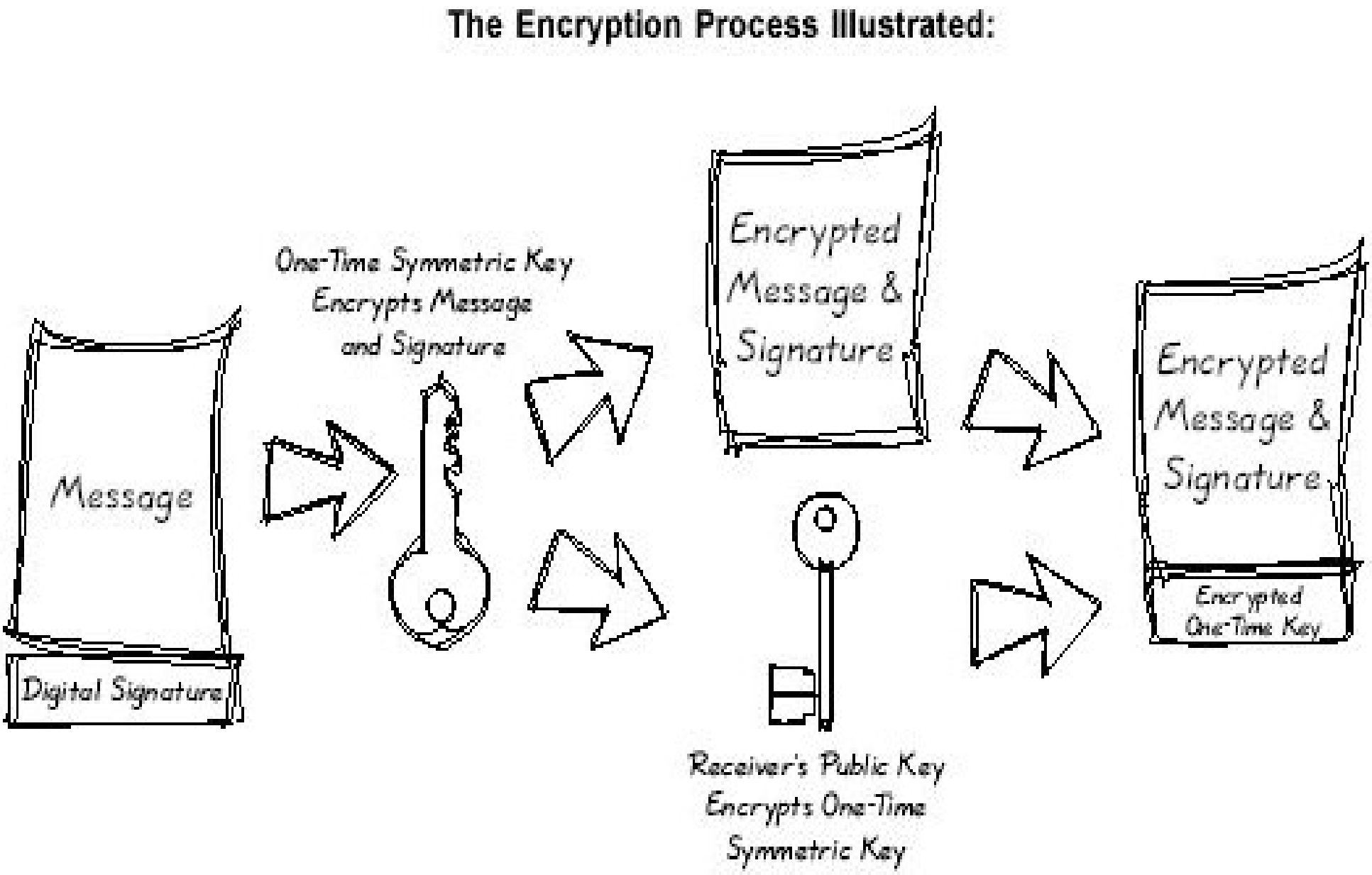
An authentication mechanism which enables the creator of a message to attach a code that acts as a signature

- Encrypt a small block of bits that is a function of the document (authenticator), using sender's private key.
- This serves as signature that verifies origin and content.
- SHA-1 or other hash functions can be used as this function.

Digital Signature Process Illustration



Encryption Process Illustration



Digital Certificates

- An answer to Internet trust problem
- Trusted 3rd parties issue certificates to people or companies who prove their ID

Digital Certificates – Manage Key

- Used for distribution of public keys.
- Public key certificate consisting of public key and user ID of key owner is signed by a trusted third party.
- The third party is called Certificate Authority(CA).

Digital Certificates

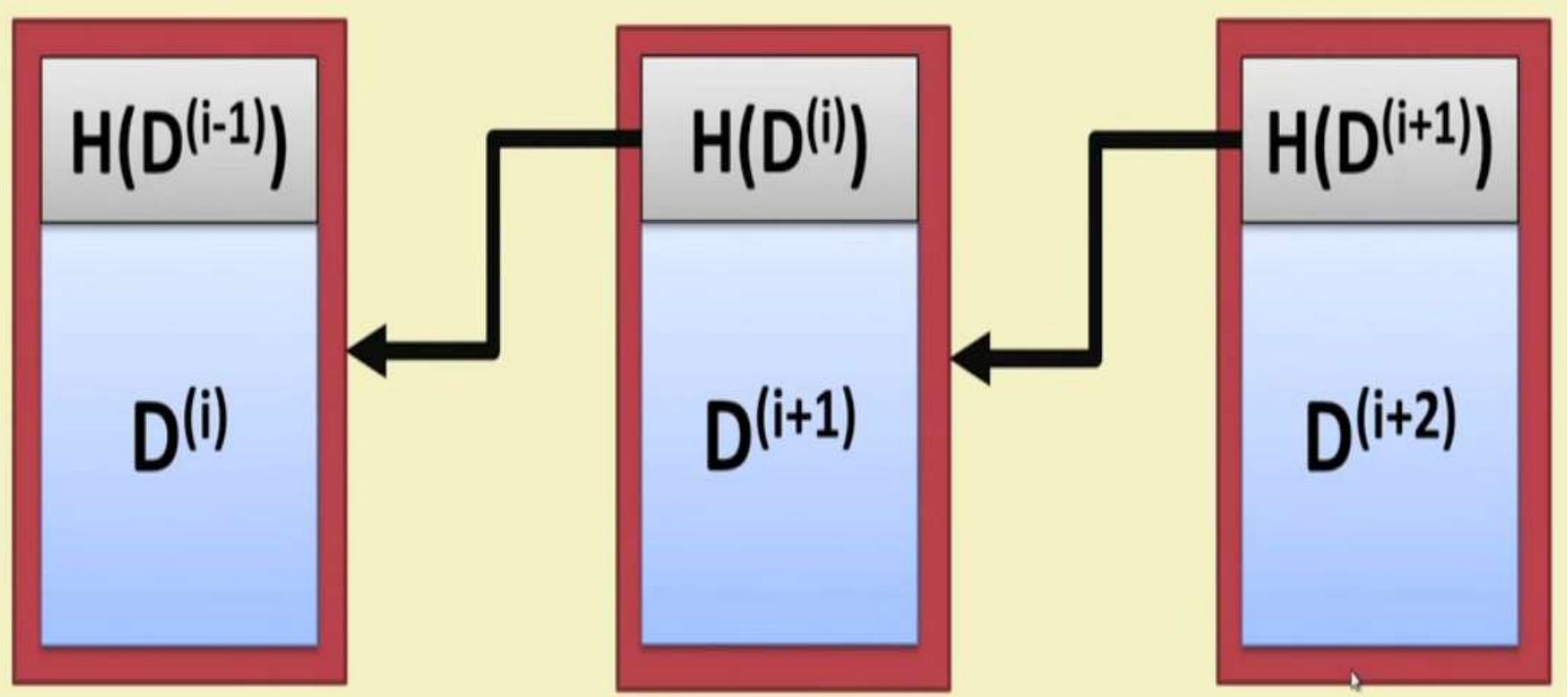
- A Digital Certificate typically contains
  - Owner's public key
  - Owner's name
  - Expiration date of the public key
  - Name of the issuer (CA that issued the Digital ID)
  - Serial number of the Digital ID
  - Digital signature of the issuer
  - X.509

Crypto Nonce and Timestamp

- A **nonce** is an arbitrary number that can be used just once. It is often a random / pseudo random number issued in protocol messages to avoid replay attacks

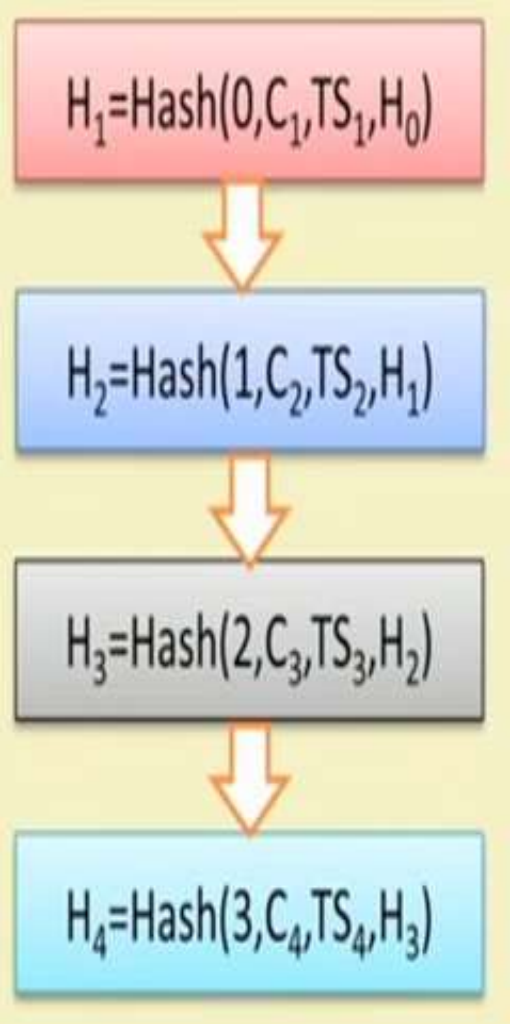
- A **Timestamp** is the time at which an event is recorded by a computer, not the time of the event itself. It helps to prevent replay attacks

Detect Tampering from Hash Pointers – Hashchain

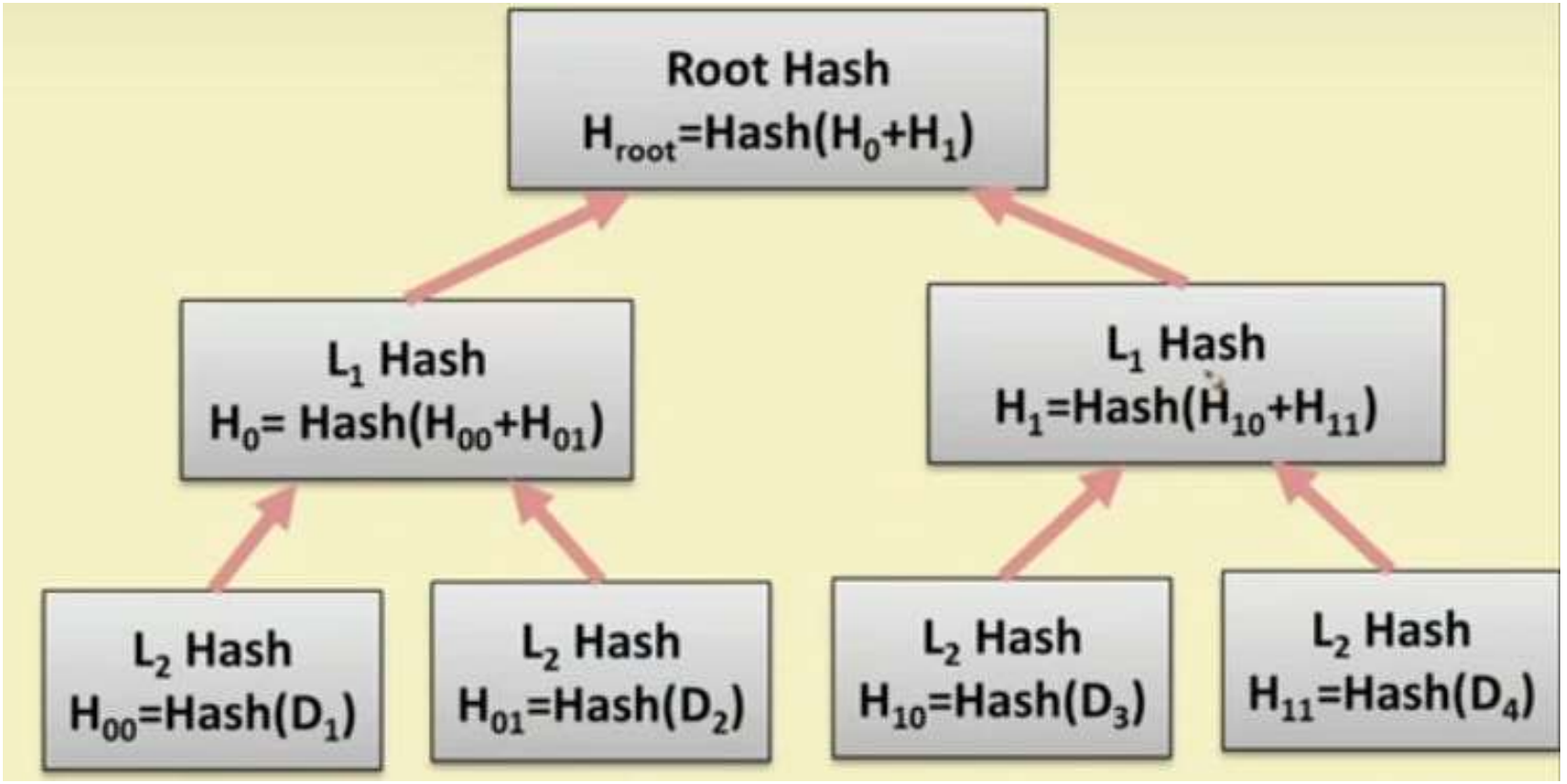


Cryptographically Secured Chain of Blocks

- The first use – **timestamp a digital document (Harber and Stometta, 1991)**
  - A sequence of timestamps [TS1, TS2, TS3, …] denoting when the document is created or edited
  - Whenever a client access a document, construct a block consisting of the sequence number of access, client ID, timestamp, a hash value from the previous request and the entire thing is hashed to connect it to the previous blocks



Merkle Trees (Ralph Merkle, 1979)

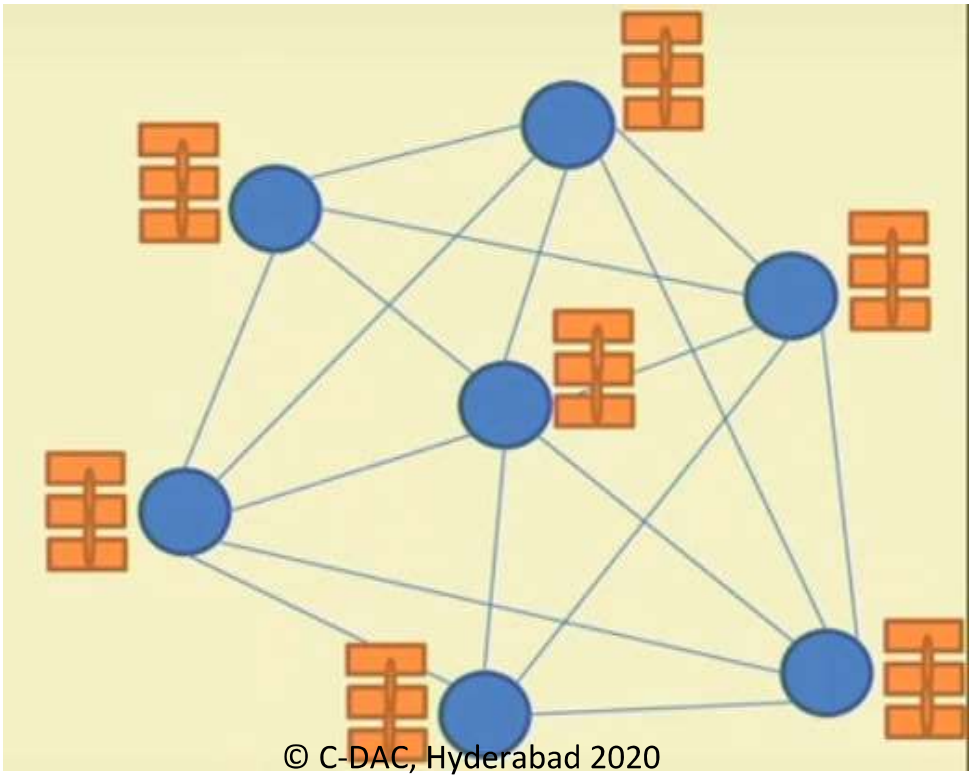


Uses of Merkle Trees

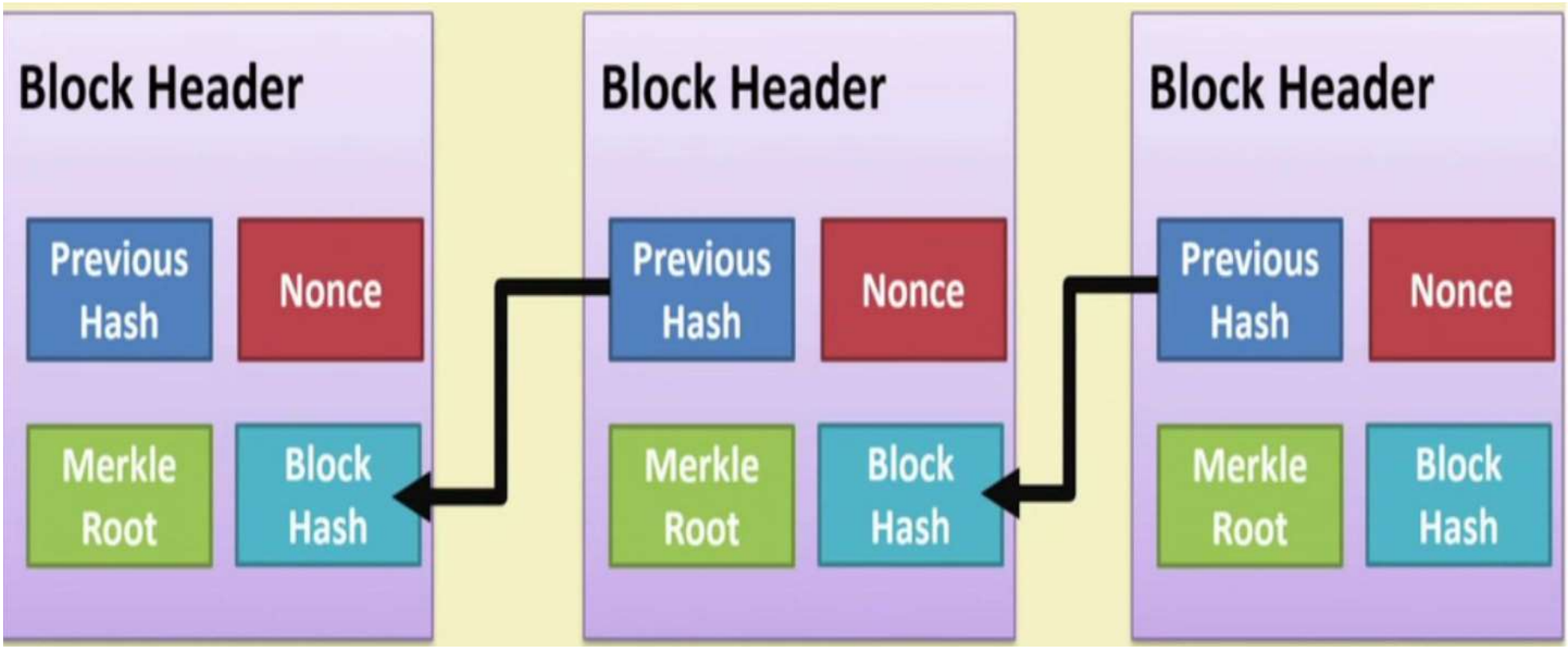
- Bayer, Harber and Stometta used Merkle Tree in 1992 for timestamping and verifying a digital document – improved the efficiency by combining timestamping of several documents into one block
- Peer to Peer Networks: Data blocks received in undamaged and unaltered, other peers do not lie about a block
- Bitcoin implementation – shared information are unaltered; no one can lie about a transaction

What is a Blockchain?

- A decentralized computation and information sharing platform that enables multiple authoritative domains, who do not trust each other, to cooperate, coordinate and collaborate in a rational decision making process.
- Every node maintains a local copy of the database and they are identical.



Blockchain as a Hashchain



Digital Signature in Blockchain

- Used to validate the origin of a transaction
  - Prevents non-repudiation
    - Alice cannot deny her own transactions
    - No one can claim Alice's transaction as his/her own transaction
- Bitcoin uses Elliptic Curve Digital Signature Algorithm (ECDSA)
  - Based on elliptic curve cryptography
  - Supports good randomness key generation

Puzzle Friendly

- Say M is chosen from a widely spread distribution; it is computationally difficult to compute k, such that Z=H(M||k), where M and Z are known a priori.

- A Search Puzzle (used in Bitcoin Mining)
  - M and Z are given, k is the search solution

- Puzzle friendly property implies that random searching is the best strategy to solve the above puzzle

Summary

Understanding Cryptography behind Blockchain Technology

- Importance of Cryptographic algorithms
- Types and Services offered by them
- Digital Signatures
- Digital Certificates
- Secured Chain of Blocks / Hashchain
- Merkle Tree
- How Cryptography is used in Blockchain

Thank You