# 1

What is Cryptography? = Study of mathematical techniques related to aspects of information security

Provides:

* Confidentiality = Information rendered unintelligible except by authorised entities
* Data integrity = Ensures data not altered in unauthorized manner since creation, transmission or storage
* Authentication = Verify identity of user or system that created information
* Authorisation = Upon identifying information, individual provided with key or password that allows access to a resource
* Non-repudiation = Sender cannot deny sending message

Cryptosystem = Five Tuple (P, C, K, E, D) where:

* P: finite message space (Plain texts)
* C: Finite crypto-text space (cipher texts)
* K: Finite key space
* E: Encryption function Ek : P -> C, k ∈ K
* D: Decryption function Dk : C -> P, k ∈ K
* d: Decryption Key
* e: Encryption Key

Key = Input to cryptographic function

* Security of cryptosystem based on key secret

Symmetric cryptography

* d = e or is easily computed from e
* Need for exchanging e

Diagram

Description automatically generated with medium confidence

* Types:
  + Block based ciphers = Encrypt blocks of information at a time
    - Stronger than stream ciphers but slower
    - Two attributes to look after:
      * Confusion = Relation between key and ciphertext should be complicated so key cannot be determined from ciphertext
      * Diffusion = Output depends on inputs in a complex way such as changing one bit would have a significant difference in outputs
    - Stream based ciphers = Encrypt one bit at a time
      * Mix plaintext with key stream
      * Good for real time services
      * Fast and easy to implement in hardware
      * Key combined with Initialisation Vector
* Algorithms:
  + DES
  + Triple DES
  + AES
  + IDEA
  + Blowfish
  + RC4 = Stream cipher
  + RC5 = Block cipher
  + RC6 = Speed improvement on RC5
* Advantages:
  + High speed encryption
  + Several algorithms use variable key length
* Disadvantages:
  + Difficult secure key exchange
  + Difficult key management

Asymmetric cryptography = if d <> e and computationally infeasible in practice to compute d from e

* e is public d is private
* Anyone can use e to encrypt but only those with d can decrypt
* Public Key cryptographic schemes
* Used for confidentiality, authentication or both

Diagram

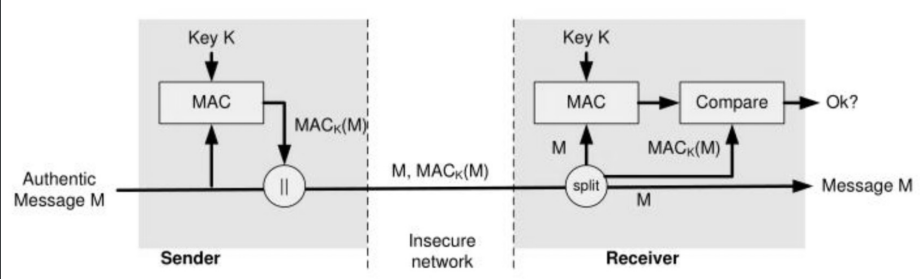
Description automatically generated

* Algorithms:
  + RSA
  + Rabin
  + El Gamal
  + Diffie Hellman
  + Elliptic Curve
* Advantages:
  + Does not require secure key exchange
  + Provides method for authentication with digital signatures
* Disadvantages:
  + Slow encryption speeds

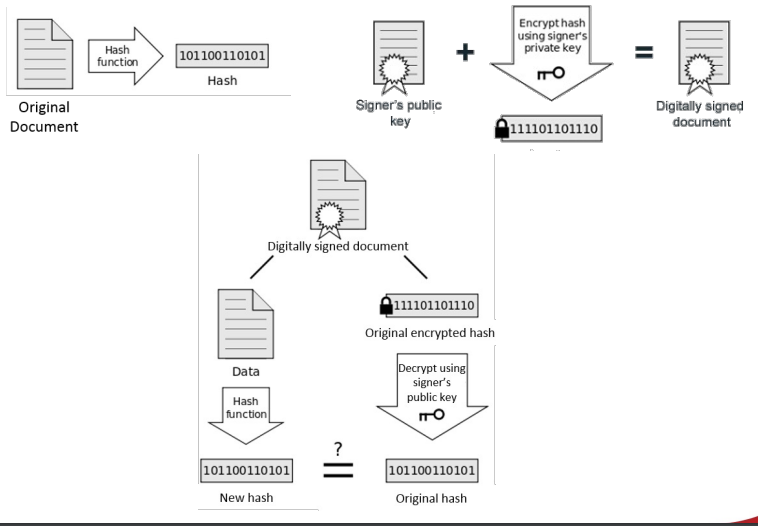
Cryptographic Hash Function *H* must provide:

* Compression
* Efficiency
* One-way
* Weak collision resistance
* Strong collision resistance

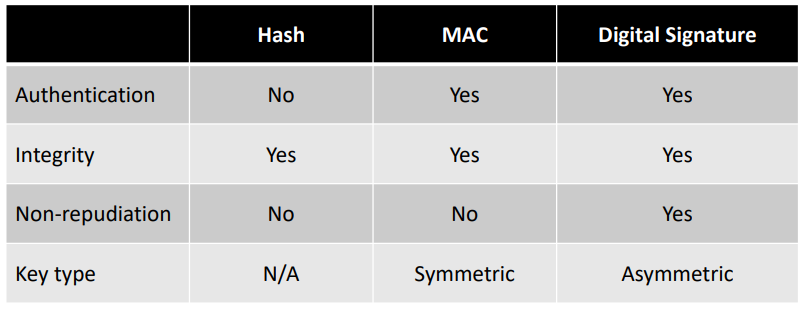
Message Authentication Codes (MAC) prevent tampering with messages



Digital Signatures



Comparison



Cryptography in Networks:

* Protects data in transit
* Link encryption
* Network Encryption
* End to end Encryption

Secure Socket Layer(SSL) Transport Layer Security (TLS)

* Provides data encryption and client/server authentication
* SSL
  + Handshake Protocol
    - Authenticates client and server
    - Set of encryption algorithms and symmetric keys
  + Data transfer
    - Encryption
    - Integrity Checking
  + Architecture
    - SSL Session
      * Client Server Association
      * Created by handshake
      * Defines set of encryption parameters
      * Possible to share among different connections
    - SSL Connection
      * Temporal as peer to peer connection
      * Associated with one SSL Session
  + SSL Handshake

1. Client sends cryptographic information to server
2. Server sends CipherSuite, Server Certificate and optional client certificate request
3. Client verifies server certificate and checks cryptographic parameters
4. Client sends secret key information encrypted with server public key (Client key exchange)
5. Client sends client certificate
6. Server verifies client certificate
7. Client sends finished message to server
8. Server sends finished message to client
9. Exchange messages (Encrypted with shared secret keys)

Cryptographic attack: Goal to discover key

* Cyber only attack = obtain ciphertext from several messages, encrypted with same encryption algorithm
* Known plaintext attack = attacker has plaintext and corresponding cipher text of 1+ messages
* Chosen plaintext attacks = attacker has plaintext and ciphertext but can choose plaintext that gets encrypted
* Chosen ciphertext attacks = choose ciphertext to be decrypted and study transformation to plain text
* Differential cryptanalysis = Look at statistical differences when encrypting different messages with the same key
* Side-channel attack = Gathering ‘outside’ information, 1995 RSA private key uncovered by measuring the relative time of crypto operations
* Social engineering attacks = Non-technical attacks that are carried out on people

Birthday Attack = Brute force attacks based on birthday problem

* 2+ people out of 23 have a 50% chance to share a birthday
* Raising group to 70 increases probability to 99.9%
* Used to find collisions of hash functions

# 2 Security Fundamentals

top aspects of information security are:

* Confidentiality = Ensuring information is accessible only to those who have access
* Integrity = Safeguarding accuracy and completeness of information and processing methods
* Availability = Availability = ensuring authorised users have access to information and associated assets when required
* Other definitions include anonymity, pseudonymity, unlinkability, copy protection, information flow control, and data protection/personal data privacy.
* Aspects of integrity and availability protection include rollback, authenticity, non-repudiation, and audit.
* Common questions regarding security include whether a system is secure and what factors affect security.
* Security engineering focuses on building systems to remain dependable in the face of malice, error, or mischance and involves tools, processes, and methods.
* It is important to design, implement, and test systems properly and to protect the right things in the right way.

# 3

# 4

# 5

# 6

# 7

# 8

# 9

# 10