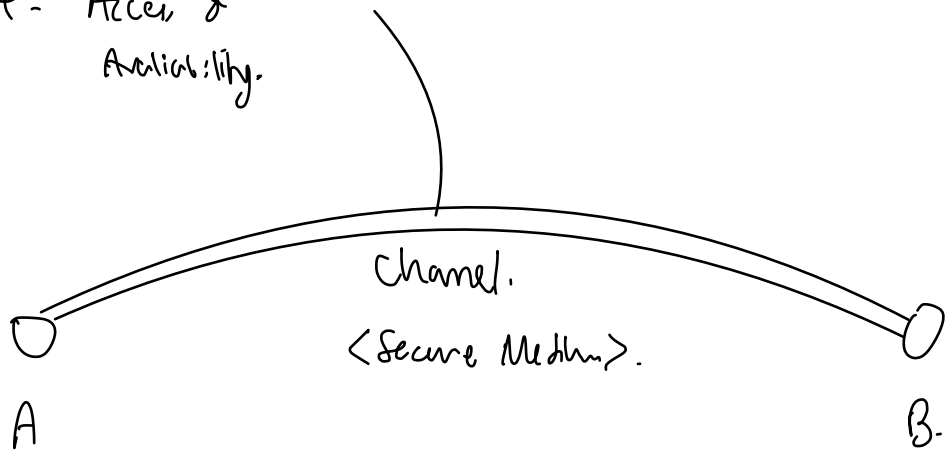
Network Security.

1. Confidentiality. → understand message only by host.
2. Authentication vs Repudiation. → identity.
3. Message integrity → no alteration should be possible without detection
4. Access & Availability.



Uses: on-line purchase.

on-line banking.

same thing: DNS servers → phishing?

Routers → routing tables. (can be spoofed).

⇓

hijack entire network

⇒ ∴ has to be secured & authenticated.

Hijacking → man-in-the-middle attack

DDOS → overwhelm a server. eg. DDOS.

Preserve confidentiality → encrypting data

K_A key K_B.

plaintext → ciphertext → plaintext.

$K_B(K_A(m)) = m$.

Symmetric key Cryptography → $K_A = K_B$ (same key.)

Asymmetric key Cryptography → $K_A \neq K_B$

Monoalphabetic cipher → Statistical analysis to break it.
→ mapping of alphabets.

Ciphertext only attack, known-plaintext attack, chosen plaintext attack.

↓

use multiple mapping!

↓

Polyalphabetic encryption → n substitution ciphers.
→ cycling pattern, different algorithm / associated keys.

Block ciphers.

- block of k bits.
- each block encrypted independently
- one-to-one mapping on each block.

k=3

1 block → 010 110 001 111
↓ 101 000 111 001

mapping is not stored as mapping.
use.
⇒ approximation of this

DES → 56 symmetric key, 64-bit blocks.

AES → 128 bit blocks.

Drawback → exchange of keys.

$K_B^- K_B^+ (A)$.

Cannot derive private key with K_B^+.

mathematical guarantee that inversion is possible.

modular math on numbers.

prime factorization prime numbers.

→ no algo

↓

expensive is very expensive → avoid

↓

combine symmetric key w public key.

① use for later part of communication. ② exchange symmetric key.

(users session key.

↓

ssh

Message integrity

- cryptographic → digest
- attacker

⇓

Hash functions.

(mapping input gives you a fingerprint)

⇓

Cryptographic hash function

⇓

hash value cannot be recreated

⇓

any small variation in message → large variation in hash value

Message Integrity.

- MAC . H(m+s)

"secret key"