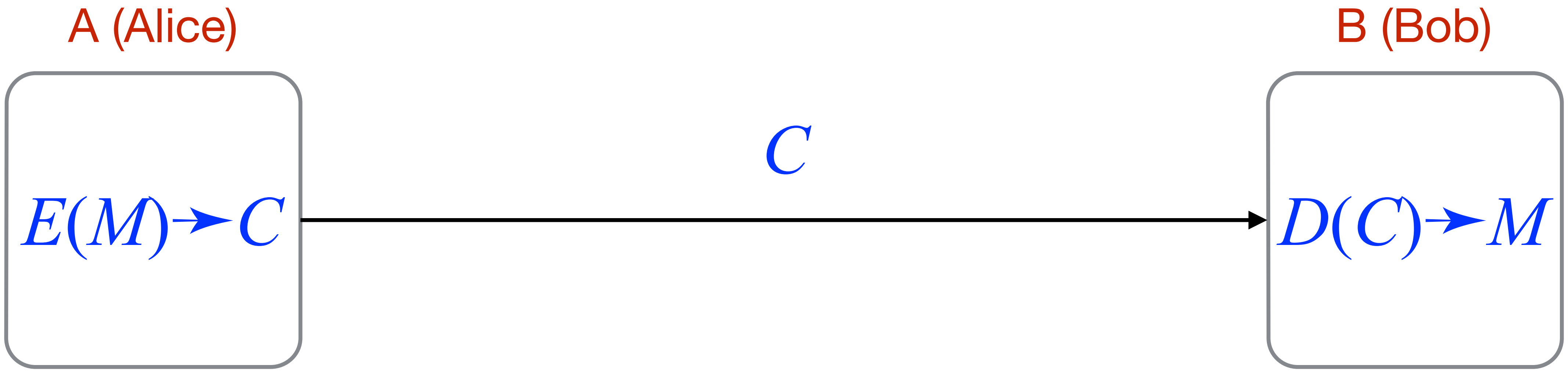
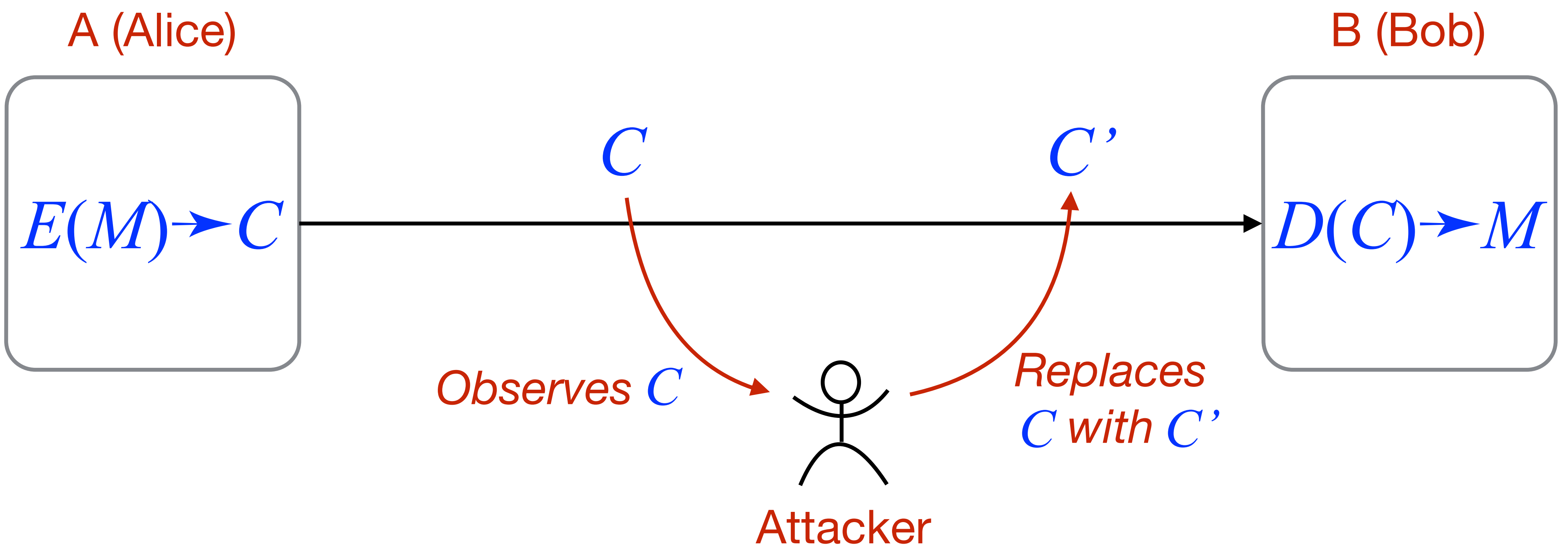
Encryption



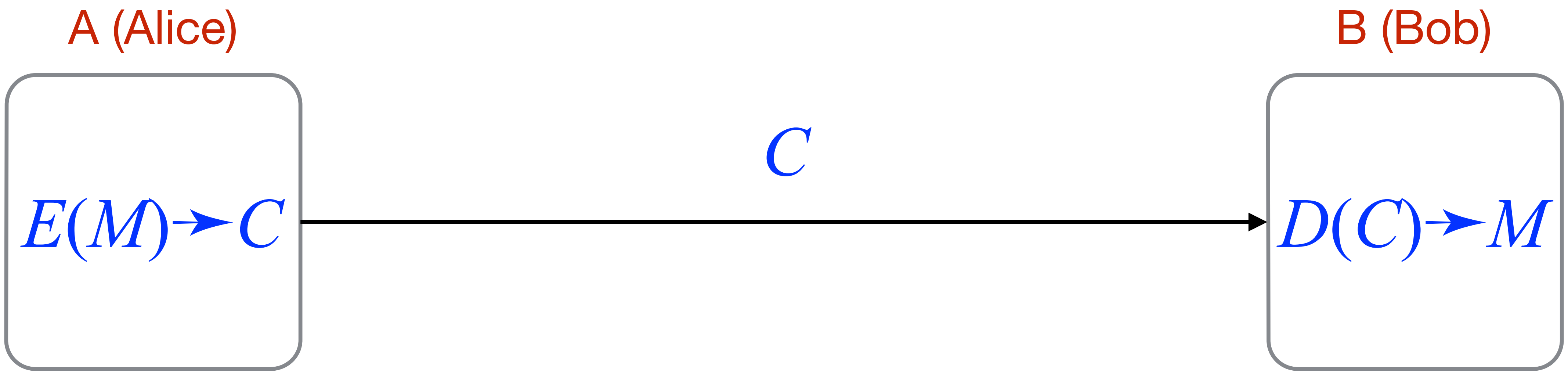
- M - message, C - ciphertext (encrypted text)
- Encryption: $E(M) \rightarrow C$
- Decryption: $D(C) \rightarrow M$

Encryption - Attacks



- Passive attack: message observed
- Active attack: message replaced or modified

Encryption Categories



A (Alice)

$E(M) \rightarrow C$

C

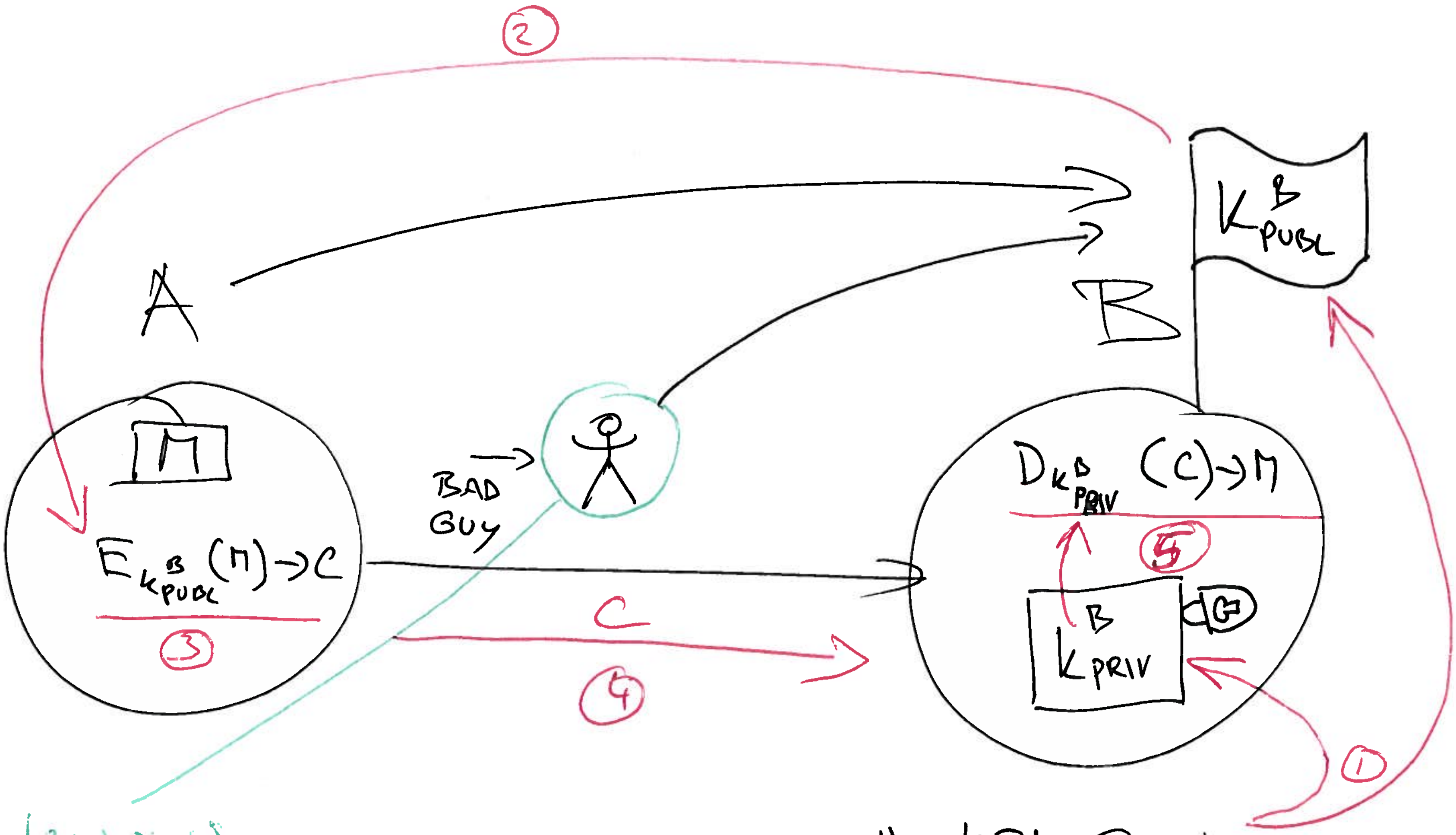
B (Bob)

$D(C) \rightarrow M$

A. Secret methods: $E(\ )$ and $D(\ )$

B. Public methods, secret key: $E_k(\ )$ and $D_k(\ )$

C. Public methods, public and private keys: $E_{pubk}(\ )$ and $D_{privk}(\ )$



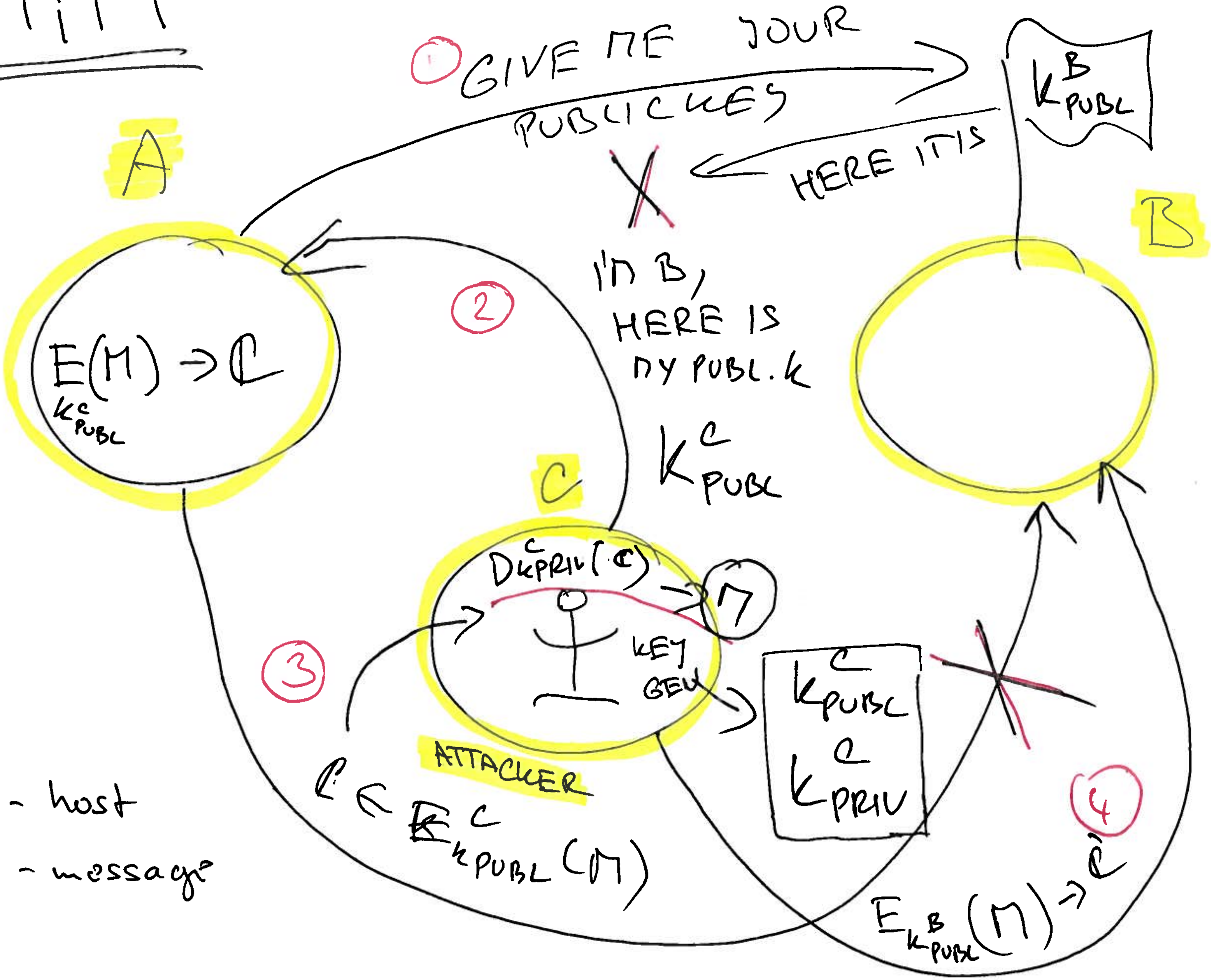
KNOWS
- $E(\cdot)$ and $D(\cdot)$
- C
- K B PUBL

1) KEY GEN.
   → k^B_{PUBL}, k^B_{PRIV}
2) A GETS K^B_{PUBL}
3) $E_{k^B_{PUBL}}(M) \to C$
4) SEND C
5) $D_{k^B_{PRIV}}(C) \to M$

Key Exchange Problem

- Everything hinges on A getting B’s public key...
  - once that’s done, all is set
- **Man-in-the-middle (MITM)** attack
- Needed:
  - authentication
  - message integrity

MiM



C - host

ℭ - message

Encryption Methods

- **Cæsar** (substitution) cipher
  - ... frequency analysis
- “Unbreakable” cipher
- **DES** - Data Encryption Standard
  - 1977, symmetric key, 56-bit key, 64-bit data blocks
- **AES** - Advanced Encryption Standard
  - 1998, symmetric key, 128,192, and 256-bit keys, 128-bit data blocks

UNBREAKABLE CIPHER

M 01011010111 .....

K 11010110110 ......

$\boxed{E}$ XOR

C 10001100001 . . .

K 11010110110 . . .

$\boxed{D}$ XOR

M 01011010111