# Security

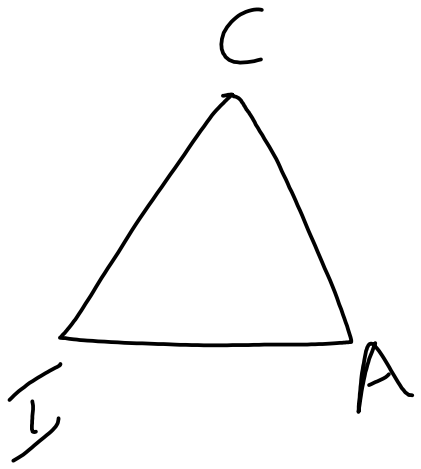
- firewalls
- VPN/Proxies
- privacy
- passwords
- encryption

## CIA Triad

Confidentiality

Integrity

Availability



# Layers (Defense in depth)

Human

Perimeter (physical)

Network

Endpoint

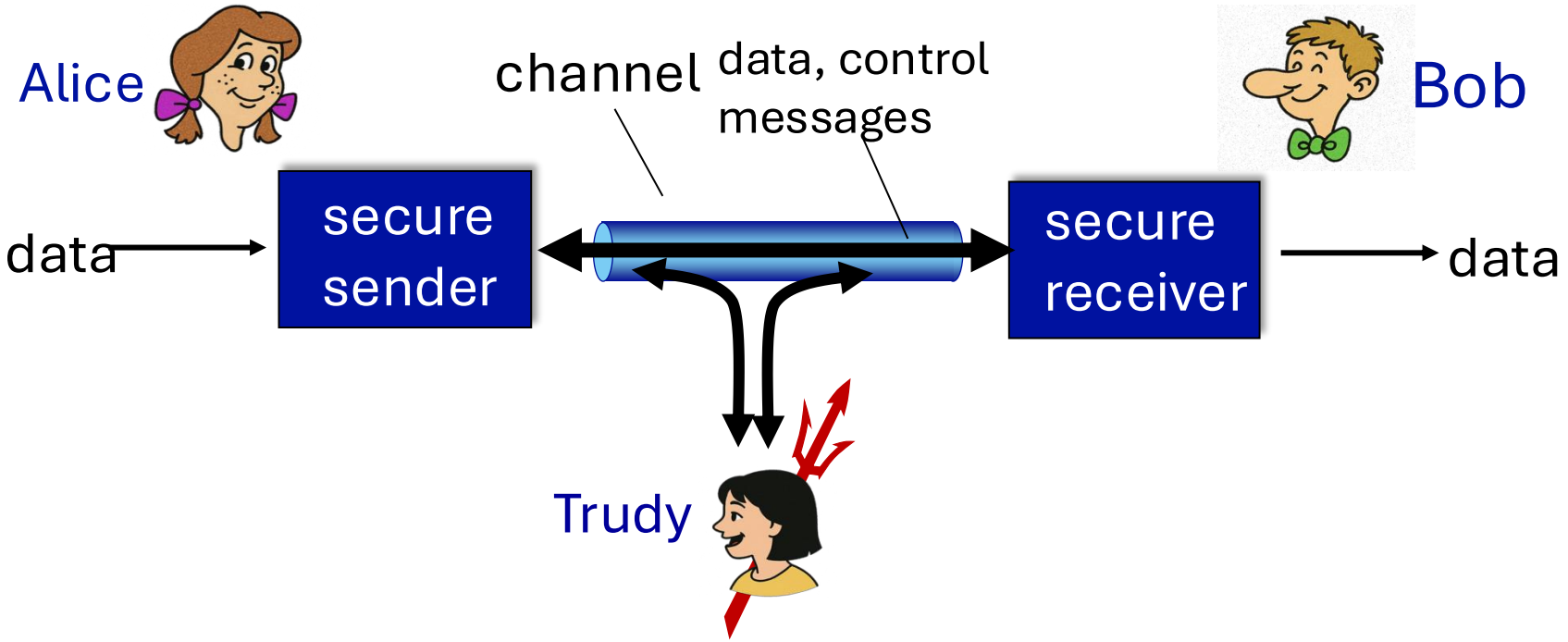
Application

Data

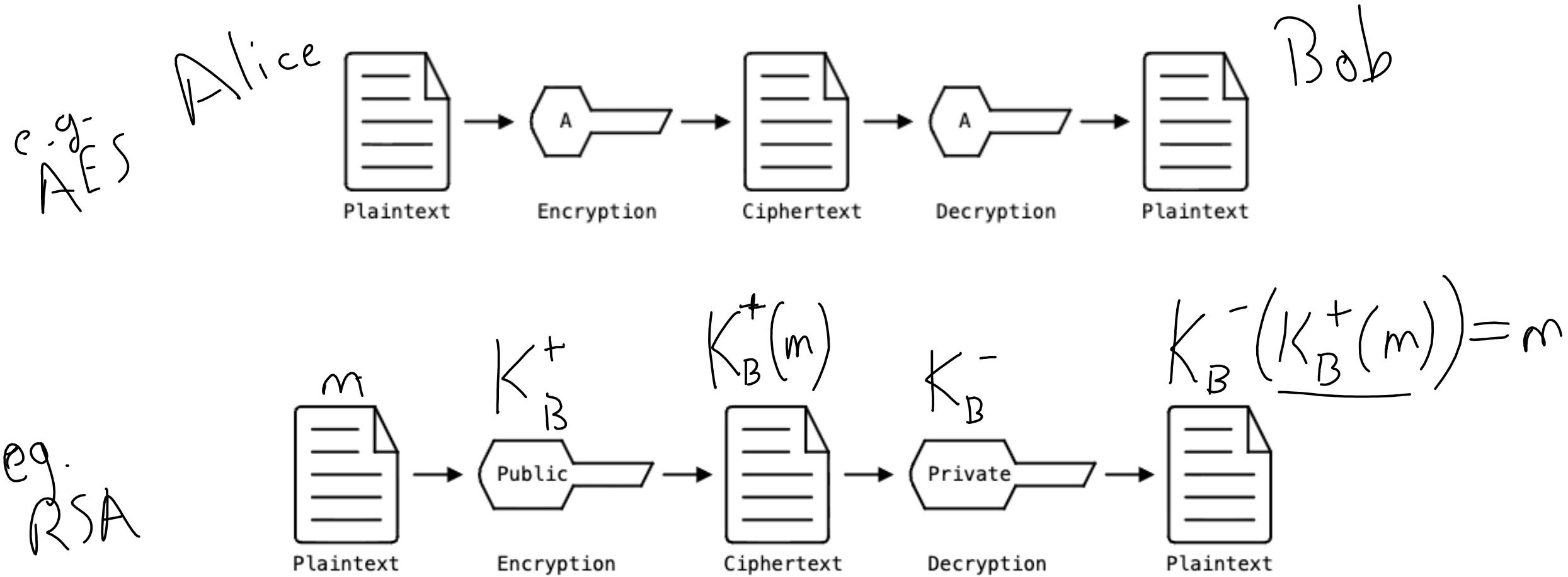
Asset

# Friends and enemies: Alice, Bob, Trudy

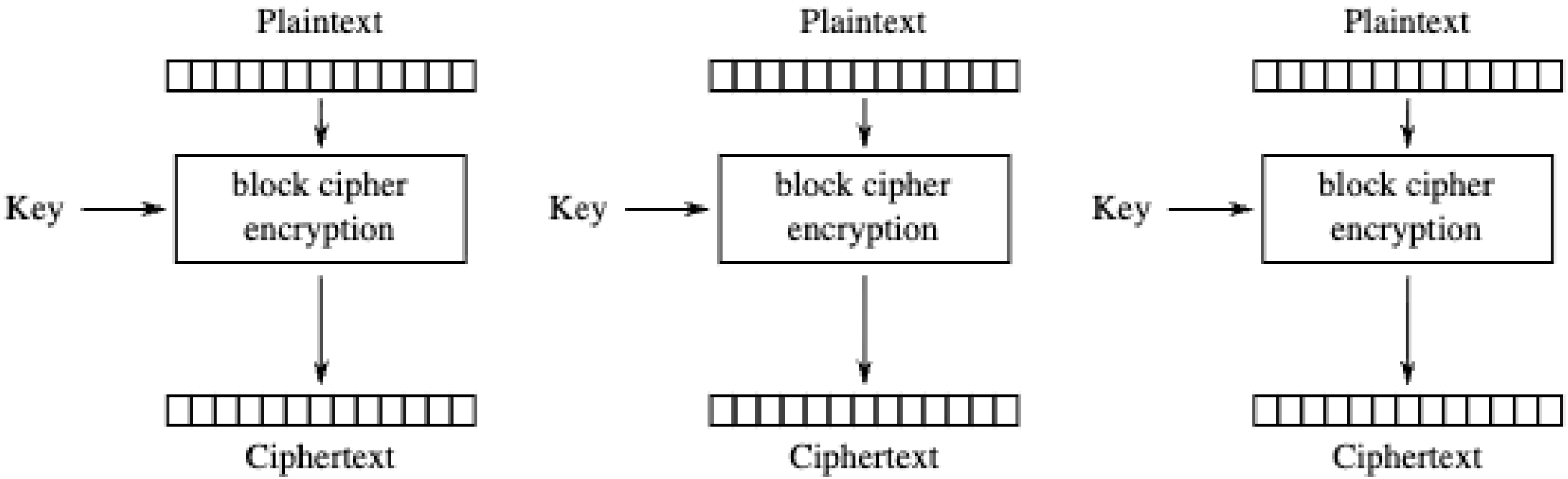
- well-known in network security world
- Bob, Alice (lovers!) want to communicate “securely”
- Trudy (intruder) may intercept, delete, add messages



# Symmetric vs. Asymmetric Encryption

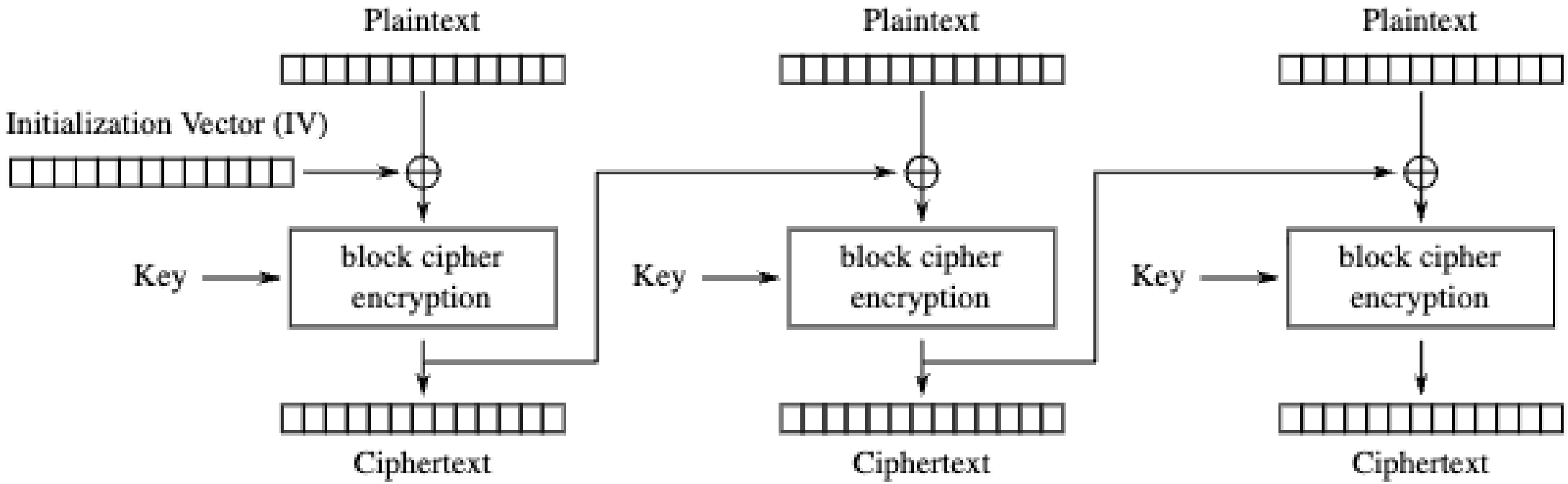


# Block Cipher: Electronic Codebook



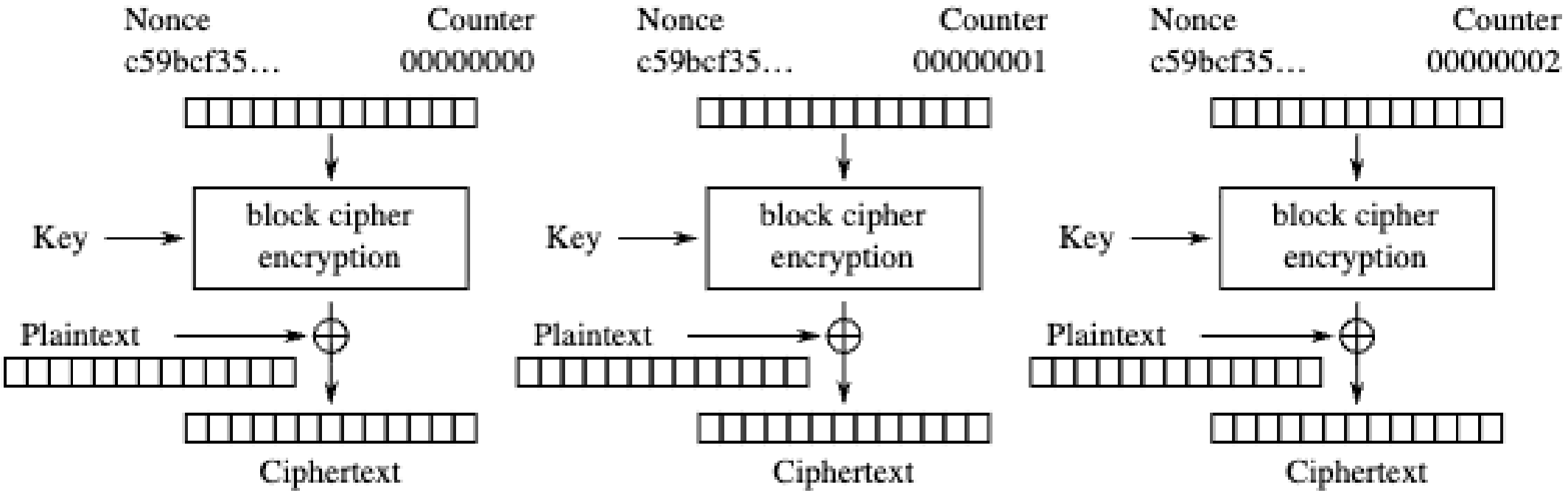

Electronic Codebook (ECB) mode encryption

# Cipher Block Chaining




Cipher Block Chaining (CBC) mode encryption

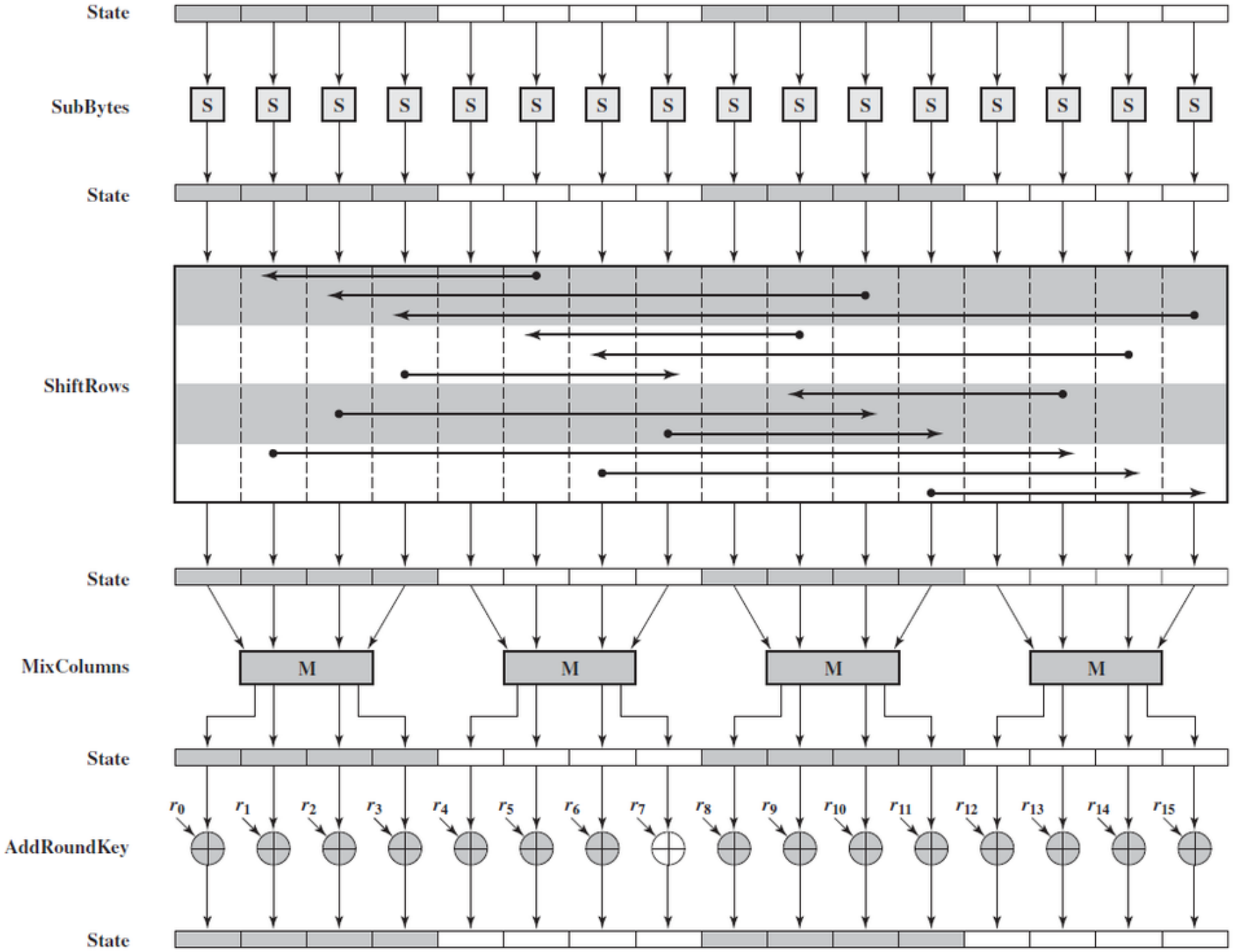
# Counter




Counter (CTR) mode encryption

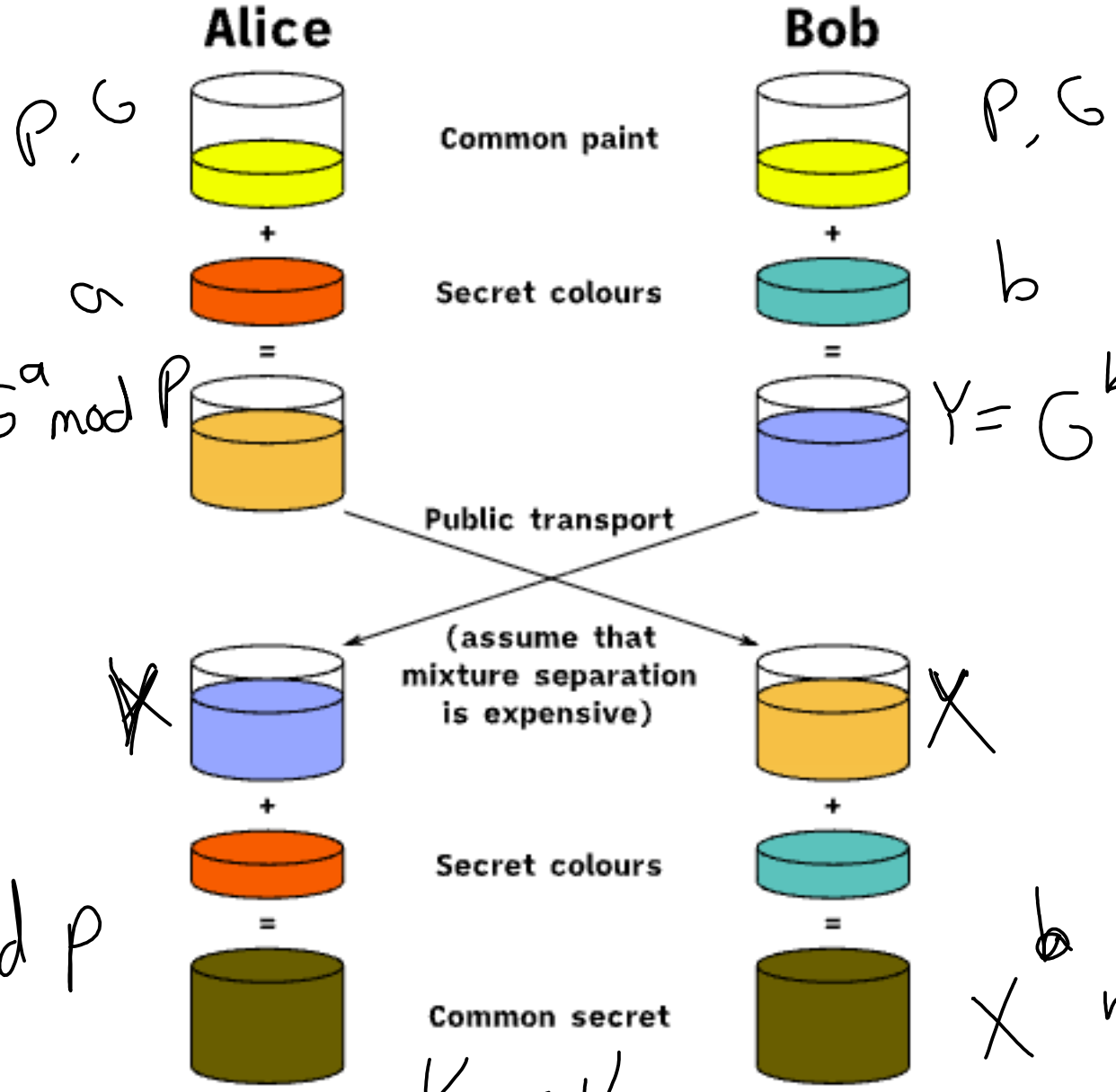
# AES

- Block 128 bits
- Keys: 128, 192, 265 bits.
- 10-14 Rounds.
- Create round keys.



# Key Exchange:

- Diffie-Hellman
- Generate a key
- Do not transmit




$P, G$

$P, G$

$a$

$b$

$X = G^a \bmod P$

$Y = G^b \bmod P$

$K_A = Y^a \bmod P$

$X^b \bmod P = K_B$

$K_A = K_B$