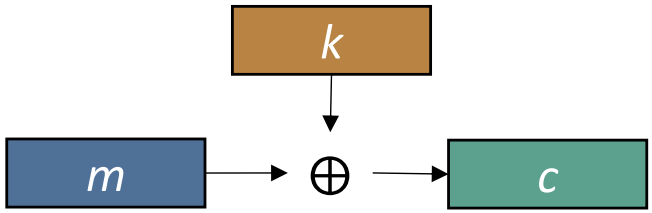
One Time Pad (OTP)

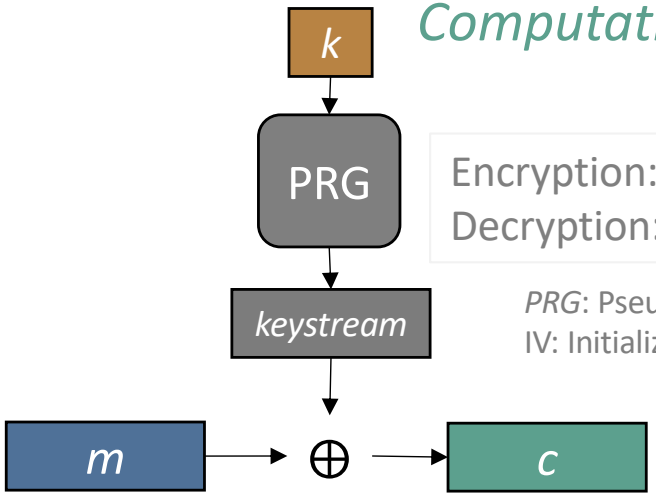
Perfect secrecy

Encryption: $c = k \oplus m$
Decryption: $m = k \oplus c$



Stream Ciphers

Computational secrecy

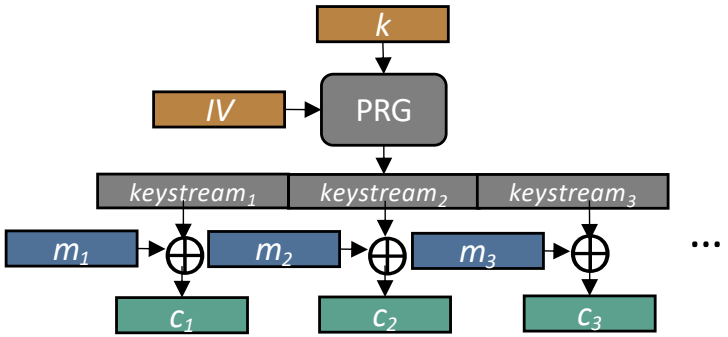


Encryption: $c = PRG(k) \oplus m$
Decryption: $m = PRG(k) \oplus c$

PRG: Pseudo-Random Generator
IV: Initialization Vector

Synchronized Mode

Encryption: $c_1 \,||c_2\,||c_3 \ldots = (IV, PRG(k,IV) \oplus m_1\,||m_2\,||m_3 \ldots)$
Decryption: $m_1\,||m_2\,||m_3 \ldots = PRG(k,IV) \oplus c_1\,||c_2\,||c_3 \ldots$
IV chosen uniformly at random



Unsynchronized Mode

Encryption: $c_i = (IV_i, PRG(k,IV_i) \oplus m_i)$
Decryption: $m_i = PRG(k,IV_i) \oplus c_i$
$IV_1, IV_2, \ldots$ chosen uniformly at random
(and thus independent)