Stream cipher

- **Goal**: encrypt stream of arbitrary length
- **Idea**: One-time pad simulation with PRG + randomness

Stream cipher

Let G be a PRG and

Gen $k \in_R \{0,1\}^n$

Enc $k \in \{0,1\}^n$ key, IV random initialization vector, m message $c = Enc_k(m) = (IV, G(k, IV) \oplus m)$.

Dec If $c = (IV, s)$, then $Dec_k(c) = s \oplus G(k, IV)$.

- If G satisfies PRG properties, then this is (computationally) secure cipher against multiple eavesdropping

Reminder: chosen plaintext attack

Attack

Active adversary: arbitrary plaintext messages and corresponding ciphertexts avaiable

Definition (CPA indisitinguishability experiment $PrivK^{cpa}_{\mathcal{A},\Pi}(n)$)

1. $k = Gen(1^n)$
2. *Adversary* $\mathcal{A}$ *has oracle access to* $Enc_k(.)$. *Issues* m_0, m_1, $|m_0| = |m_1|$
3. $b \in_R \{0,1\} : c = Enc_k(m_b)$ *given to* $\mathcal{A}$
4. $\mathcal{A}$ *has oracle access to* $Enc_k(.)$. *Issues* $b' \in \{0,1\}$
5. $PrivK^{cpa}_{\mathcal{A},\Pi}(n) = 1$, *if* $b = b'$, *0 otherwise.*

CPA

Definition

A cipher $\Pi = (Gen, Enc, Dec)$ *is CPA-secure if* $\forall \mathcal{A}$ *PPT adversary* $\exists e(.)$ *negligible with*

$$P(PrivK^{cpa}_{\mathcal{A},\Pi}(n) = 1) \leq \frac{1}{2} + e(n).$$

Tool: pseudorandom function family

- keeps input length (n-bit strings mapped to n-bit strings)
- for fixed $k \in \{0,1\}^n$ $F_k(.)$ is a member of the family
- a.k.a. keyed function
- a random element from the family is indistinguishable from a truly random function

CPA-secure cipher

CPA-security from PRF

Let F be a PRF, furthermore

Gen $k \in_R \{0,1\}^n$

Enc $c = Enc_k(m) = (r, F_k(r) \oplus m)$.

Dec For $c = (r, s)$, let $Dec_k(r, s) = F_k(r) \oplus s$.

Theorem

If F has the PRF property, then this $\Pi = (Gen, Enc, Dec)$ is CPA-secure.

Block ciphers

- **Goal**: encryption of fixed length message (block)
- **Idea**: strengthen PRF construction

Tool: strong pseudorandom permutation family (strong PRP)

- similar to PRF, but additionally:
- keeps length (n-bit strings mapped to n-bit strings), **BIJECTION**
- for fixed $k \in \{0,1\}^n$, $F_k(.)$ is a member of the family
- any random element of the family is indistinguishable from a truly random function, knowing the functions and **inverses**.

Block ciphers

Block cipher

Let F be a strong PRP and

Gen $k \in_R \{0,1\}^n$

Enc for key $k \in \{0,1\}^n$, message $m \in \{0,1\}^n$ and random value $r \in_R \{0,1\}^n$, let $c = Enc_k(m) = (r, F_k(r) \oplus m)$.

Dec For $c = (r, s)$, let $Dec_k(r, s) = F_k(r) \oplus s$.

- Remaining challenges: encrypt long messages with block ciphers
- $m = (m_1, \ldots, m_l)$ where $\forall i : |m_i| = n$ (padding if needed)
- Let's encrypt block m_i according to some *mode of operation* one by one

Block ciphers

Block cipher

Let F be a strong PRP and

Gen $k \in_R \{0,1\}^n$

Enc for key $k \in \{0,1\}^n$, message $m \in \{0,1\}^n$ and random value $r \in_R \{0,1\}^n$, let $c = Enc_k(m) = (r, F_k(r) \oplus m)$.

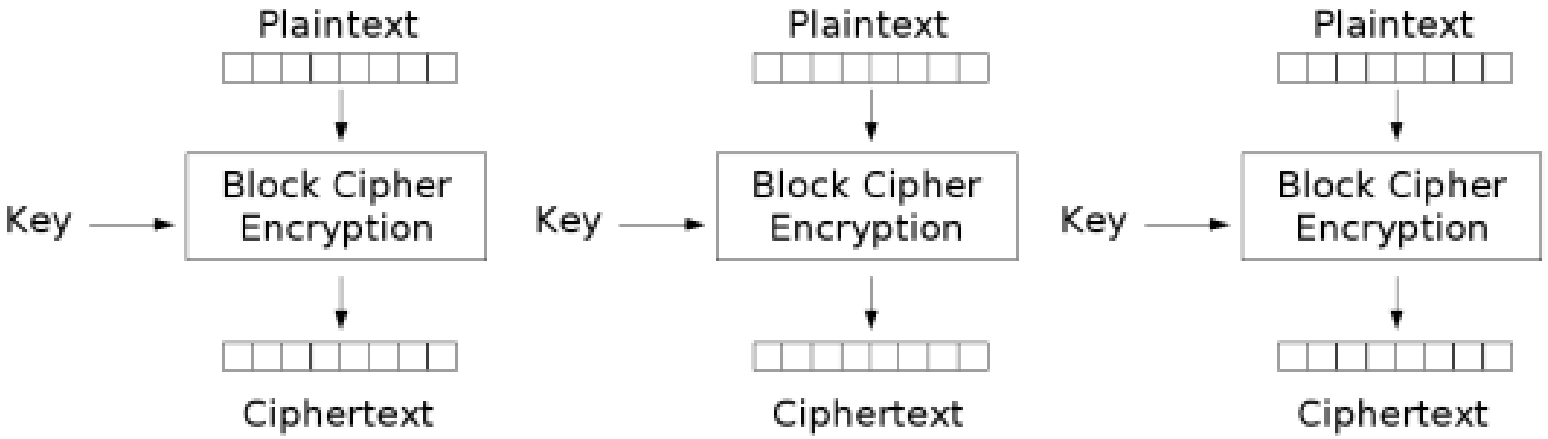
Dec For $c = (r, s)$, let $Dec_k(r, s) = F_k(r) \oplus s$.

- Remaining challenges: encrypt long messages with block ciphers
- $m = (m_1, \ldots, m_l)$ where $\forall i : |m_i| = n$ (padding if needed)
- Let's encrypt block m_i according to some *mode of operation* one by one

Modes of operation: ECB

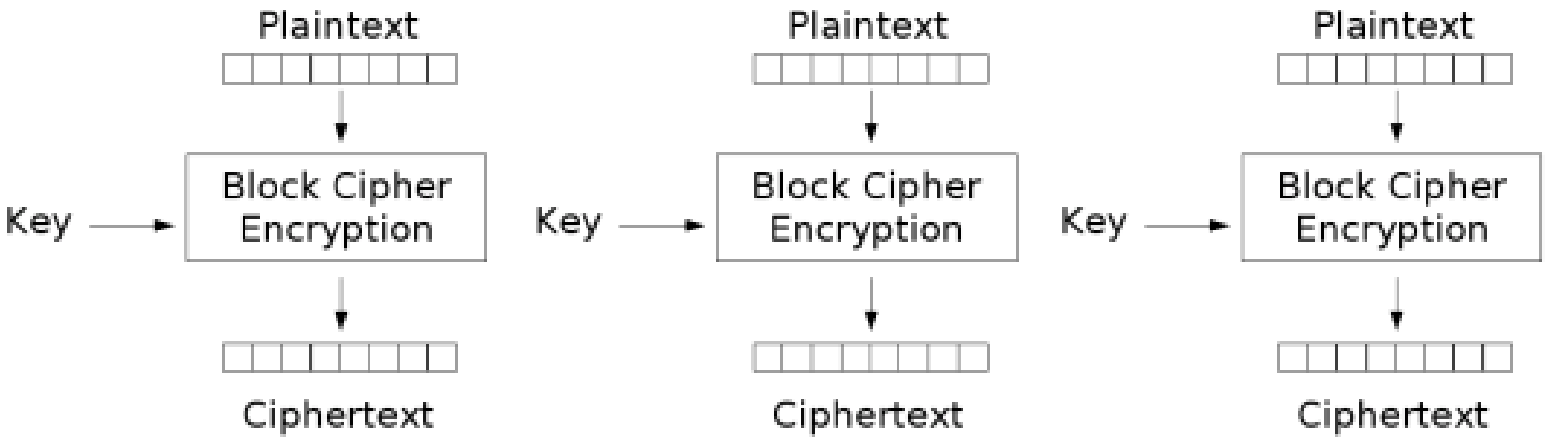
Electronic Code Book mode (ECB)

Let $F_k(.)$ be a strong PRP,
$Enc_k(m) = c = (F_k(m_1), \ldots, F_k(m_l))$.



Electronic Codebook (ECB) mode encryption

Modes of operation: ECB



Electronic Codebook (ECB) mode encryption

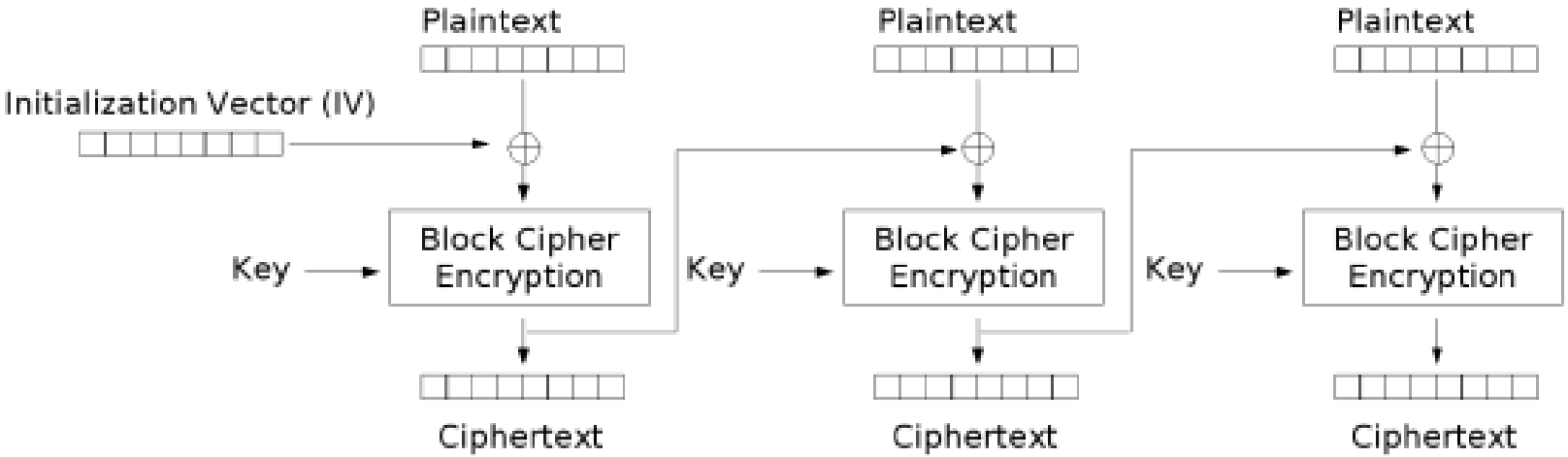
Properties

- Dec: $F_k(.)^{-1}$ should be efficiently computable
- deterministic $\Rightarrow$ no CPA-security
- eavesdropping: no security (repeated blocks)
- DON'T USE

Modes of operation: CBC

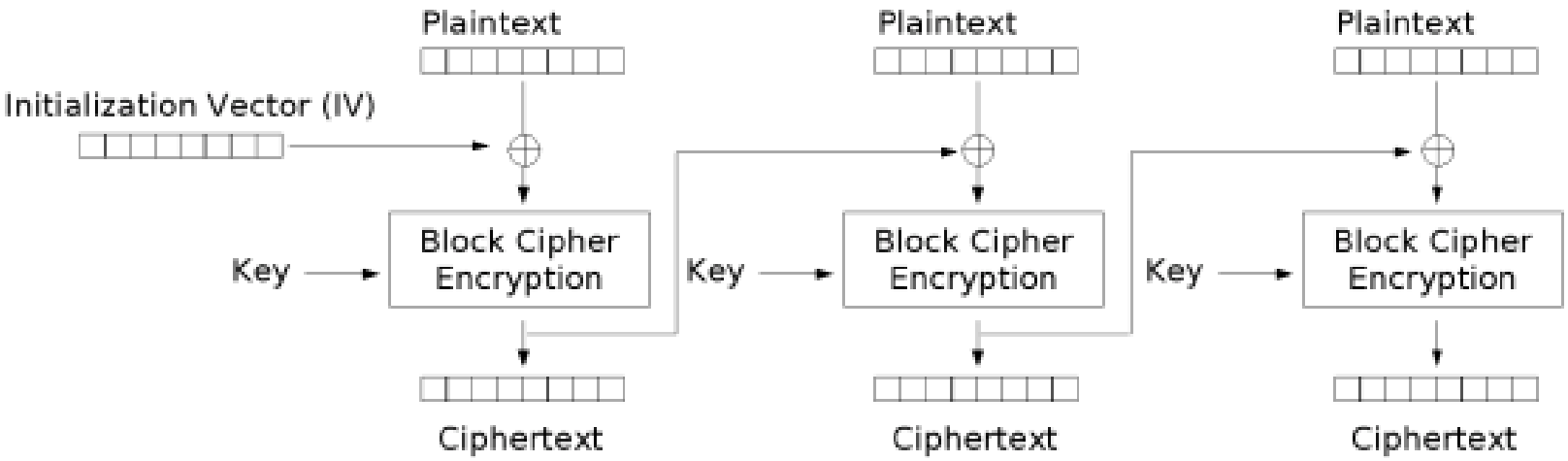
Cipher Block Chaining mode (CBC)

1. $IV \in_R \{0,1\}^n$ initialization vector
2. $c_0 = IV, c_i = F_k(m_i \oplus c_{i-1})$
3. $c = (c_0, c_1, \ldots, c_l)$



Cipher Block Chaining (CBC) mode encryption

CBC



Cipher Block Chaining (CBC) mode encryption

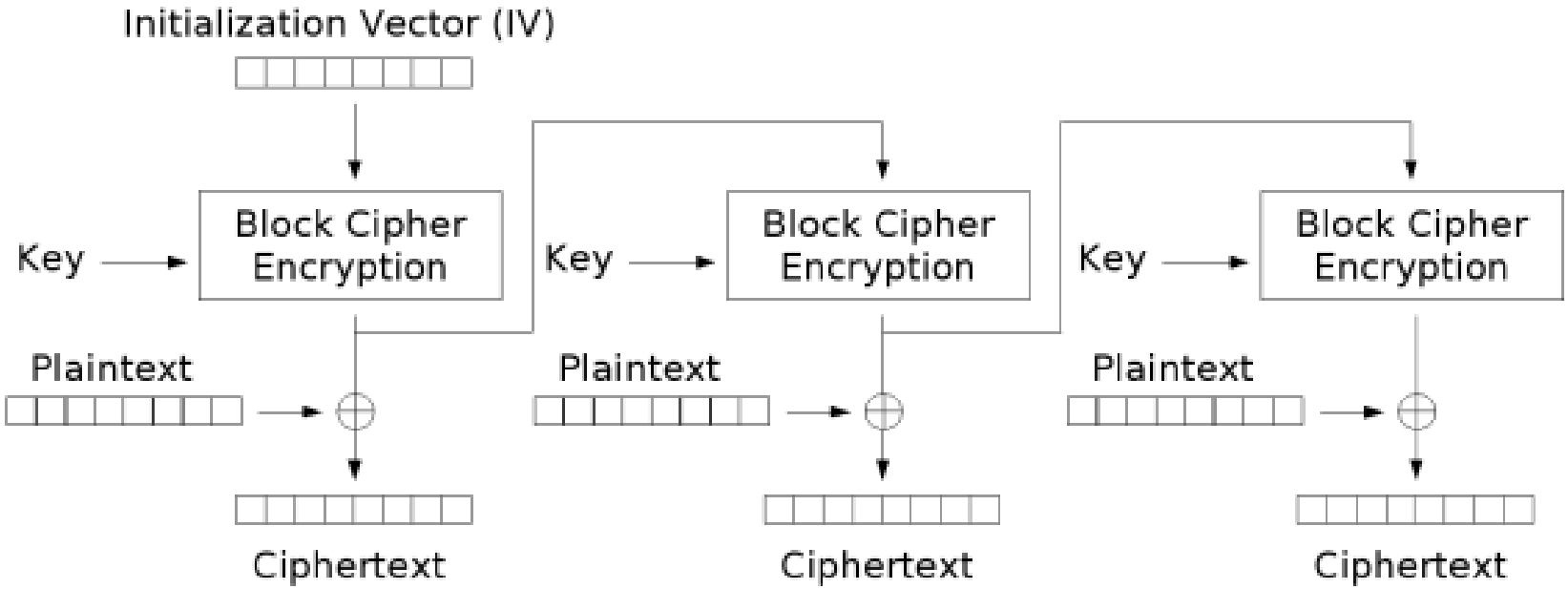
Properties

- probabilistic
- If $F_k(.)$ is strong PRP $\Rightarrow$ CPA-security
- sequential
- IV should be truly random (NO counter to be used here)

Modes of operation: OFB

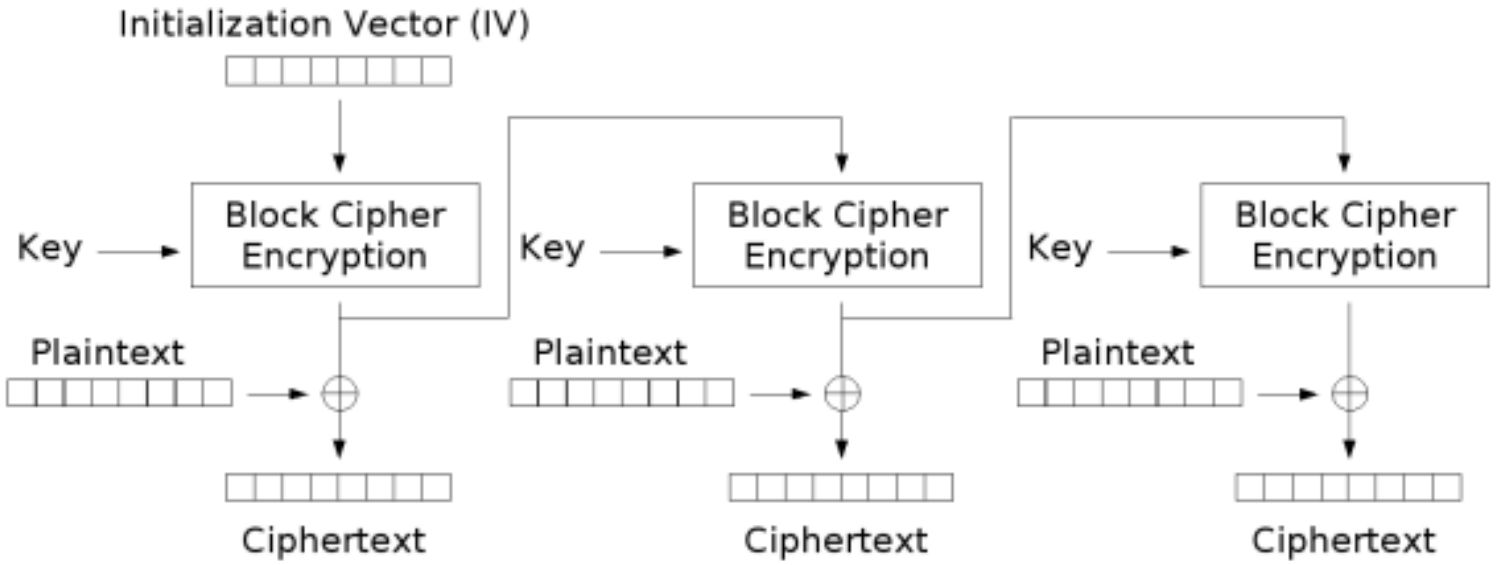
Output Feedback mode (OFB)

1. $IV \in_R \{0,1\}^n$ initialization vector
2. $r_0 = IV, r_i = F_k(r_{i-1}), c_i = m_i \oplus r_i$
3. $c = (c_0, c_1, \ldots, c_l)$



Output Feedback (OFB) mode encryption

OFB



Output Feedback (OFB) mode encryption

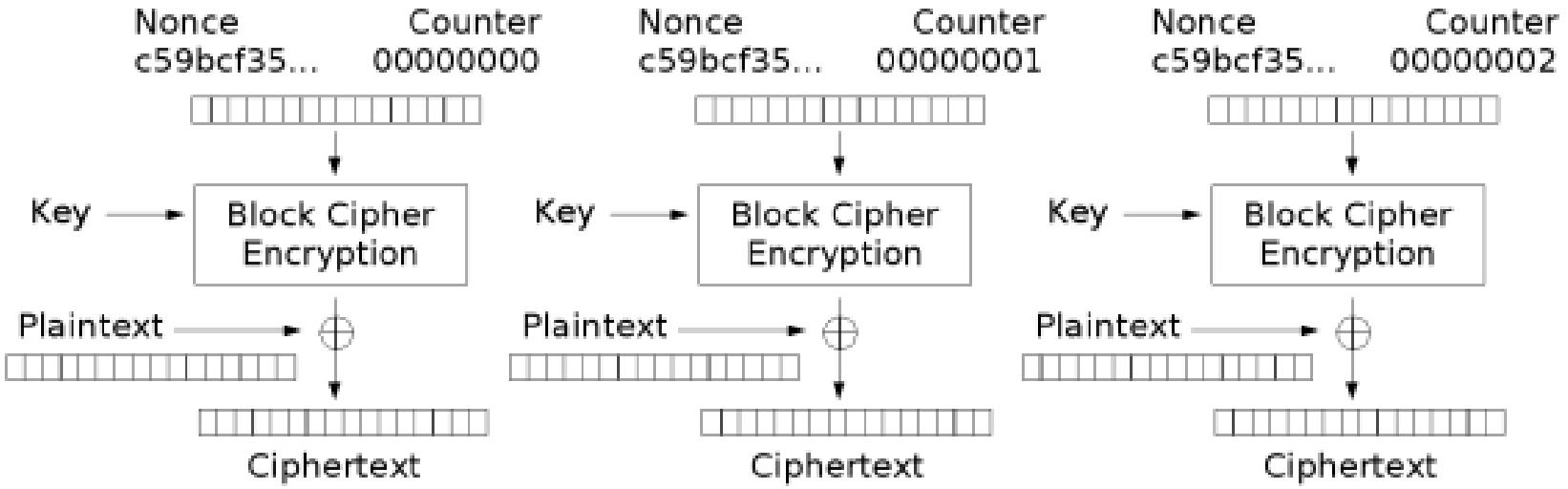
Properties

- probabilistic
- If $F_k(.)$ PRF $\Rightarrow$ CPA-security $\Rightarrow$ $F_k(.)$ has weaker assumption
- sequential
- preprocessing possible

Modes of operation: CTR

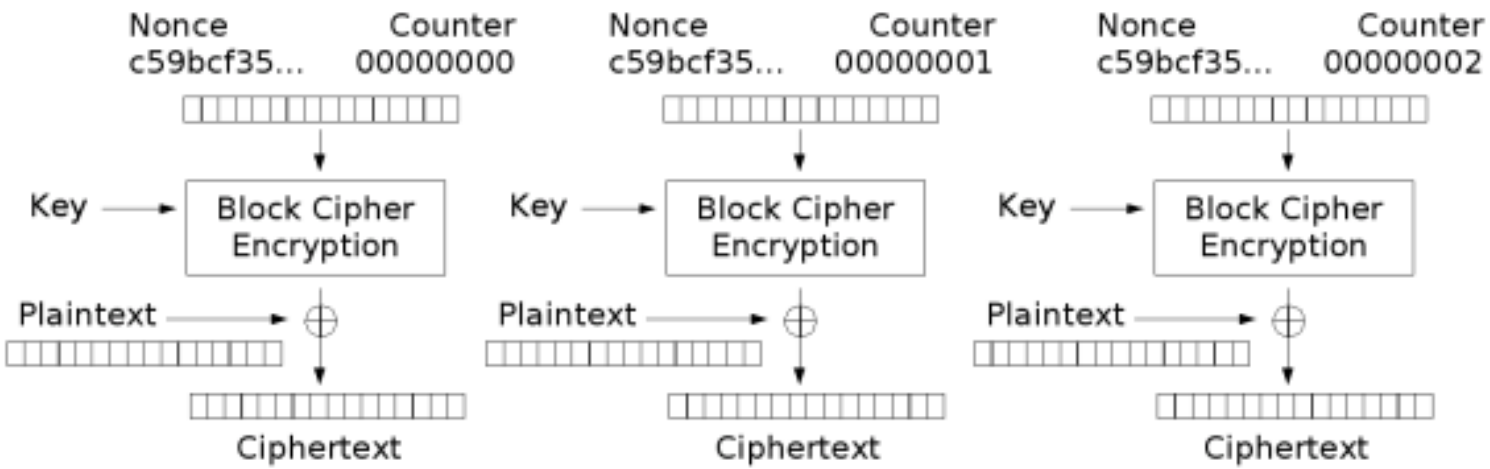
(Randomized) Counter mode (CTR)

1. $ctr = IV \in_R \{0,1\}^n$ initialization vector
2. $r_0 = IV, r_i = F_k(ctr + i), c_i = m_i \oplus r_i$
3. $c = (c_0, c_1, \ldots, c_l)$



Counter (CTR) mode encryption

CTR



Counter (CTR) mode encryption

Properties

- probabilistic
- if $F_k(.)$ is a PRF $\Rightarrow$ CPA-security $\Rightarrow$ $F_k(.)$ has weaker assumption
- parallelization
- preprocessing
- random access (decrypt ith block only)

Block or stream?

- block-size and security
- further modes
- modification of ciphertext: possible attacks

Block vs stream

- OFB and CTR mode makes stream cipher operation possible
- generates PR sequences
- better understood, more attack attempts, well-established
- stream cipher: can be faster

Block or stream?

- block-size and security
- further modes
- modification of ciphertext: possible attacks

Block vs stream

- OFB and CTR mode makes stream cipher operation possible
- generates PR sequences
- better understood, more attack attempts, well-established
- stream cipher: can be faster