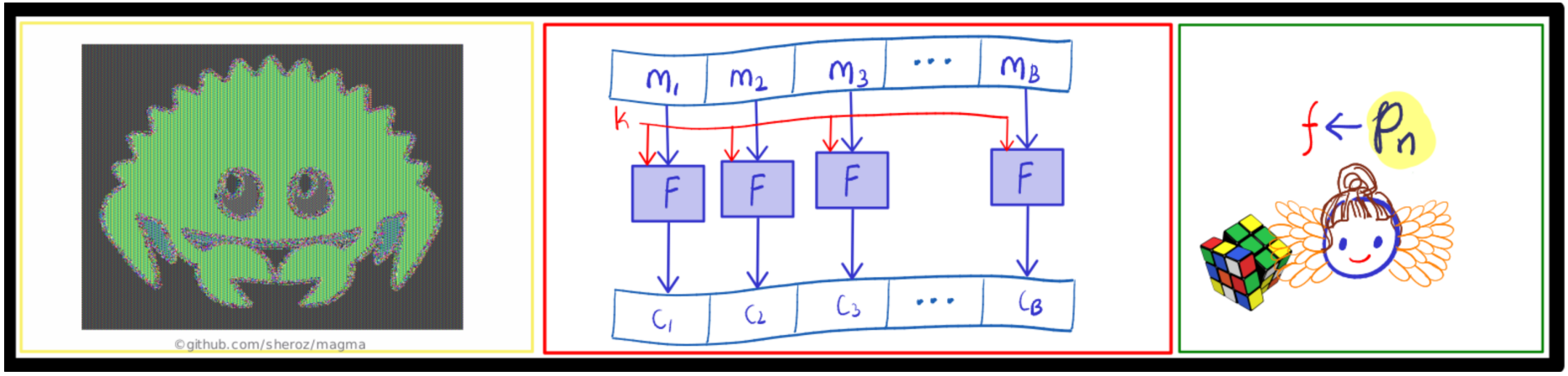


CS409m: Introduction to Cryptography

Lecture 09 (03/Sep/25)

Instructor: Chethan Kamath

Announcements

- Will finish grading Quiz 1 and Lab Exercise 1 this week
- Lab Exercise 2 (graded) will be out today (03/Sep)
  - Deadline to submit flag on CTFd server: 23:59, Sunday (06/Sep)
  - Deadline to submit report on Moodle: 23:59, Tuesday (09/Sep)
- Assignment 3 (ungraded) will be uploaded on Friday (05/Sep)

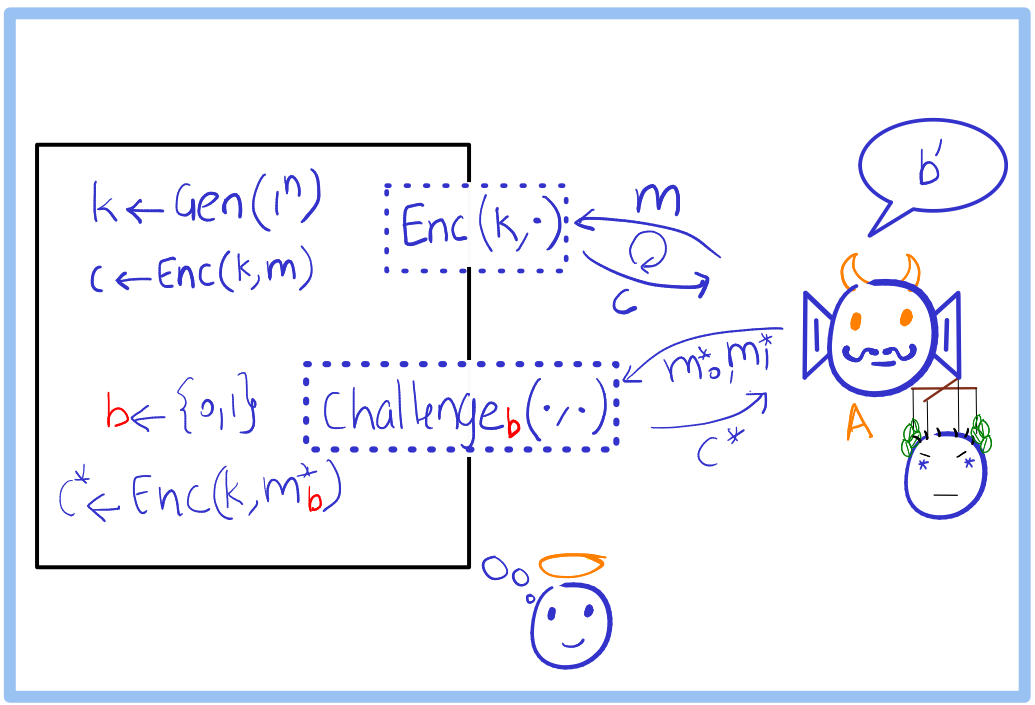
Recall from Previous Lecture...

- Task: secure communication of *multiple messages* with shared keys
- Threat model: ind. against chosen-plaintext attack (IND-CPA)

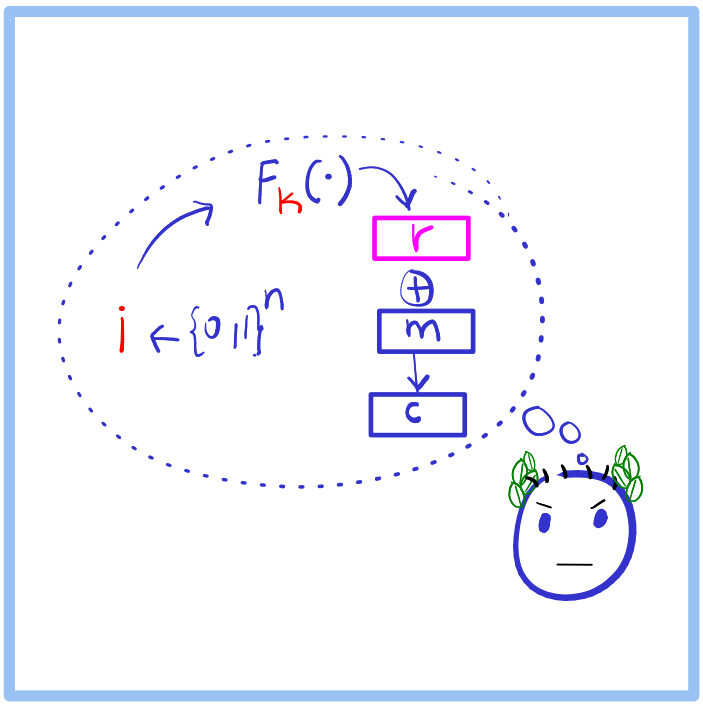
Recall from Previous Lecture...

- Task: secure communication of *multiple messages* with shared keys
- Threat model: ind. against chosen-plaintext attack (IND-CPA)

IND-CPA



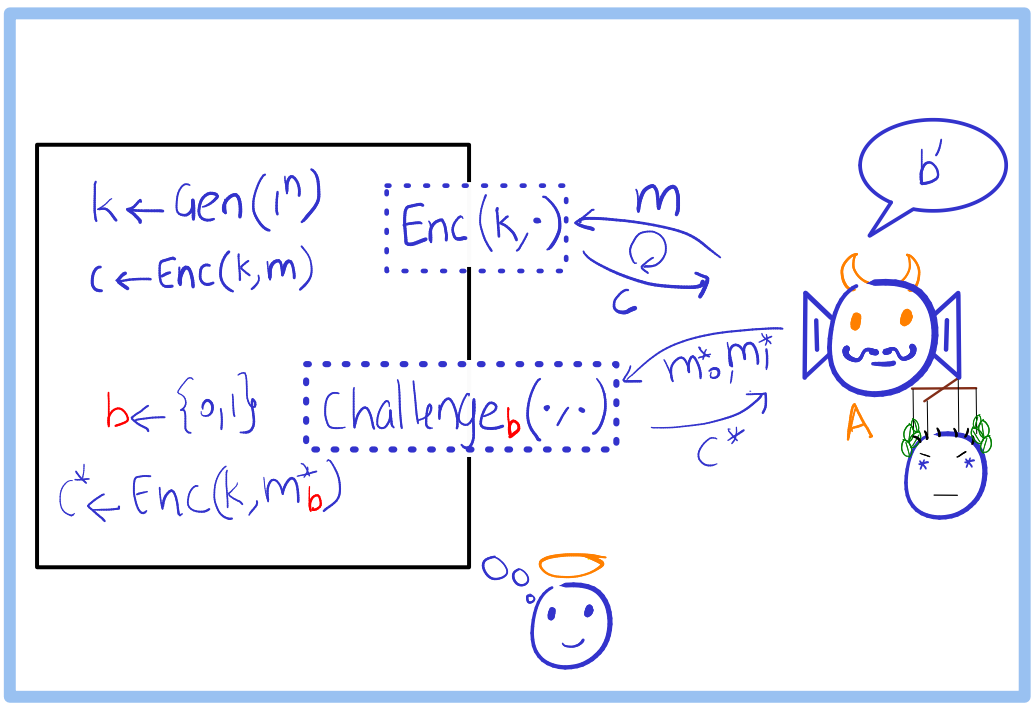
PRF $\Longrightarrow$ CPA-SKE



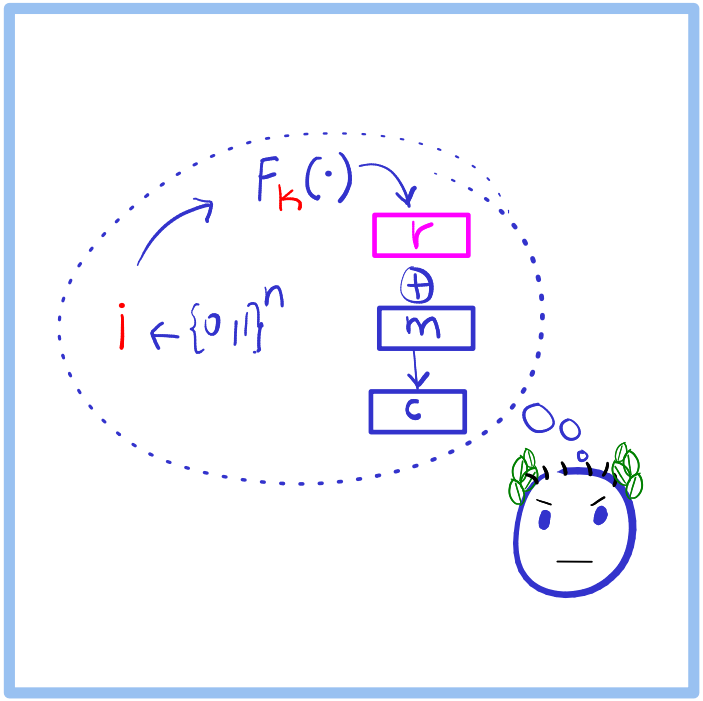
Recall from Previous Lecture...

- Task: secure communication of *multiple messages* with shared keys
- Threat model: ind. against chosen-plaintext attack (IND-CPA)

IND-CPA



PRF $\Longrightarrow$ CPA-SKE



Takeaway: IND-CPA-secure SKE *must* have randomised Enc!

Recall from Previous Lecture...

Theorem 3 (Lecture 08)

If F is a PRF, then Construction 1 (Lecture 07/08) is IND-CPA-secure

Proof by reduction.

- $\exists$ distinguisher D for F / $\Leftarrow$ $\exists$ CPA adversary A
- Main ideas:
  - Whenever A makes a query to $\mathrm{Enc}(k, \cdot)$ oracle, D queries its own oracle $O : \{0,1\}^n \to \{0,1\}^n$ to generate ciphertext
    - r chosen by D
  - When $O(\cdot) = \mathrm{F}_k(\cdot)$ D simulates Π; when $O(\cdot) = f(\cdot)$, D simulates an information-theoretically secure scheme $\tilde{\Pi}$
  - A's advantage in breaking IND-CPA translated into D's advantage in breaking F

□

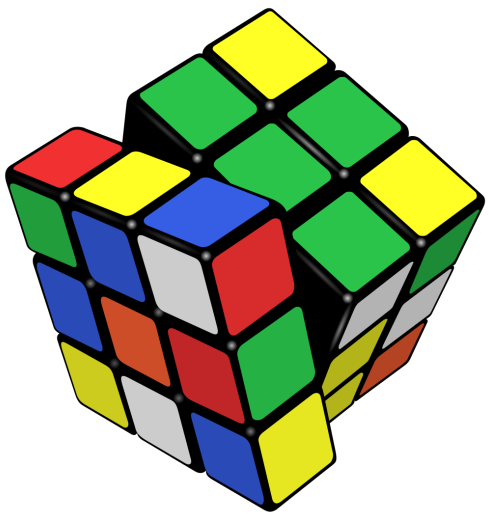
Plan for Today's Lecture

- Task: secure comm. of *multiple long* messages with shared keys
- Threat model: ind. against chosen-plaintext attack (IND-CPA)

Plan for Today's Lecture

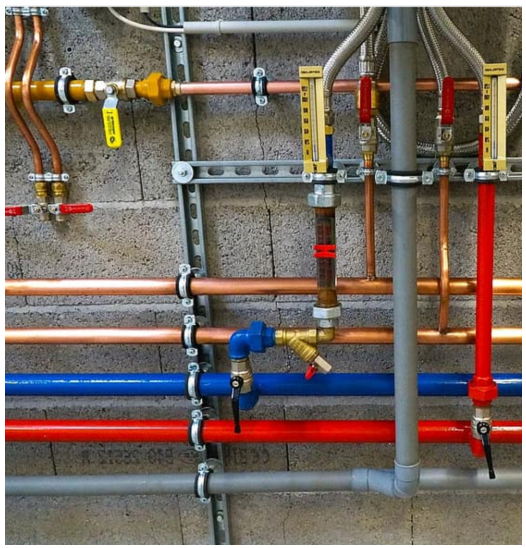
- Task: secure comm. of *multiple long* messages with shared keys
- Threat model: ind. against chosen-plaintext attack (IND-CPA)

PRP a/k/a Block Cipher



© Booyabazooka-Wikipedia

Modes of Operation

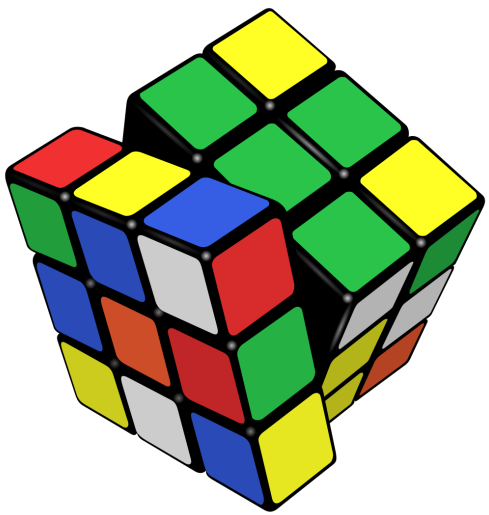


© pikist.com

Plan for Today's Lecture

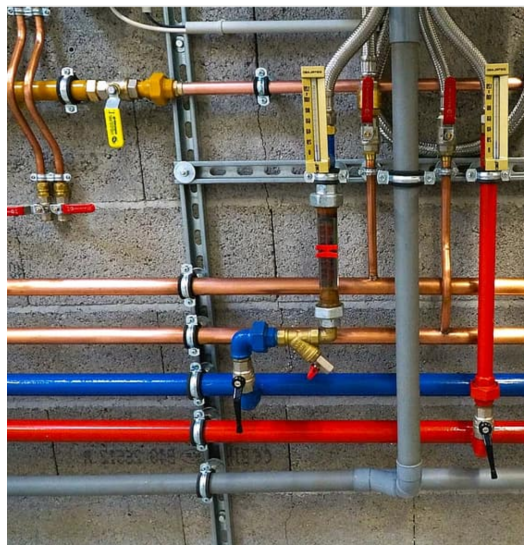
- Task: secure comm. of *multiple long* messages with shared keys
- Threat model: ind. against chosen-plaintext attack (IND-CPA)

PRP a/k/a Block Cipher



© Booyabazooka-Wikipedia

Modes of Operation



© pikist.com

Focus on efficiency: short ciphertexts, frugal use of random coins...

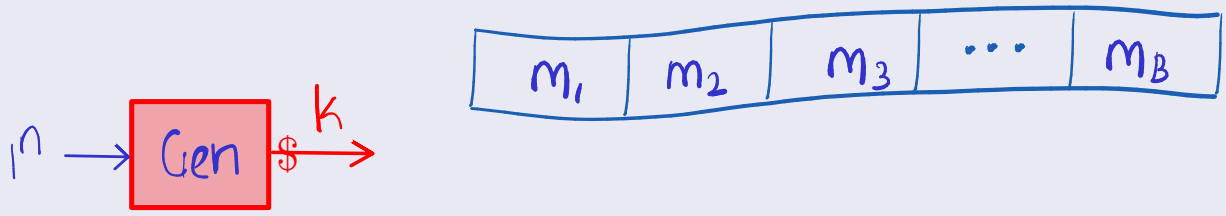
Baseline Scheme for Long Messages...

- IND-CPA for fixed-length $\Longrightarrow$ IND-CPA for arbitrary length
  - IND-CPA $\Longrightarrow$ can reuse the key!

Baseline Scheme for Long Messages...

- IND-CPA for fixed-length $\Longrightarrow$ IND-CPA for arbitrary length
  - IND-CPA $\Longrightarrow$ can reuse the key!

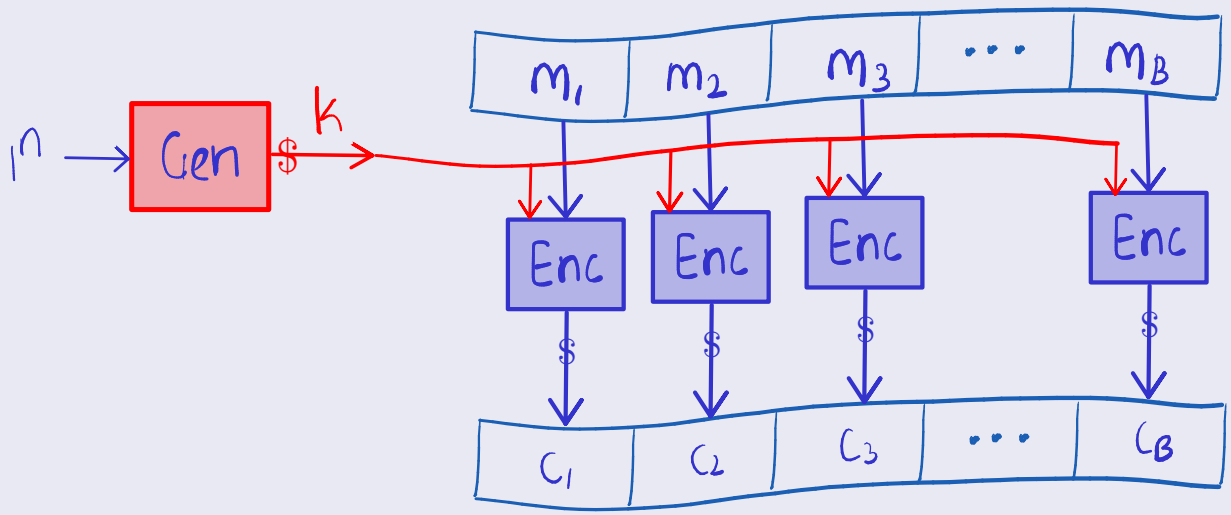
Construction 1 (Π for $\mathcal{M} := \{0,1\}^n \Longrightarrow \Pi'$ for $\mathcal{M}^B := \{0,1\}^{Bn}$)



Baseline Scheme for Long Messages...

- IND-CPA for fixed-length $\Longrightarrow$ IND-CPA for arbitrary length
  - IND-CPA $\Longrightarrow$ can reuse the key!

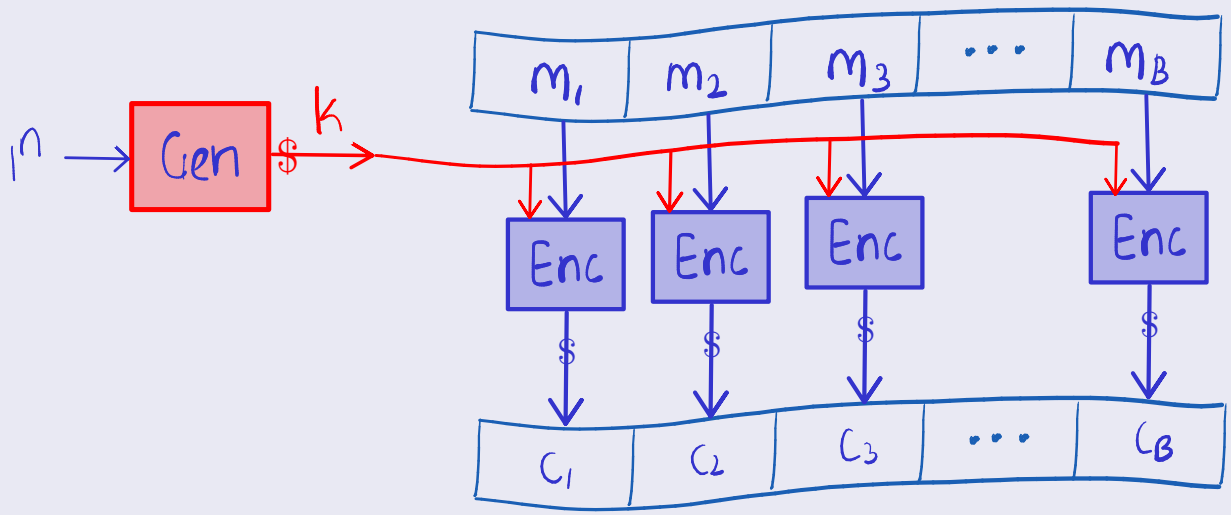
Construction 1 (Π for $\mathcal{M} := \{0,1\}^n \Longrightarrow \Pi'$ for $\mathcal{M}^B := \{0,1\}^{Bn}$)



Baseline Scheme for Long Messages...

- IND-CPA for fixed-length $\Longrightarrow$ IND-CPA for arbitrary length
  - IND-CPA $\Longrightarrow$ can reuse the key!

Construction 1 (Π for $\mathcal{M} := \{0,1\}^n \Longrightarrow \Pi'$ for $\mathcal{M}^B := \{0,1\}^{Bn}$)

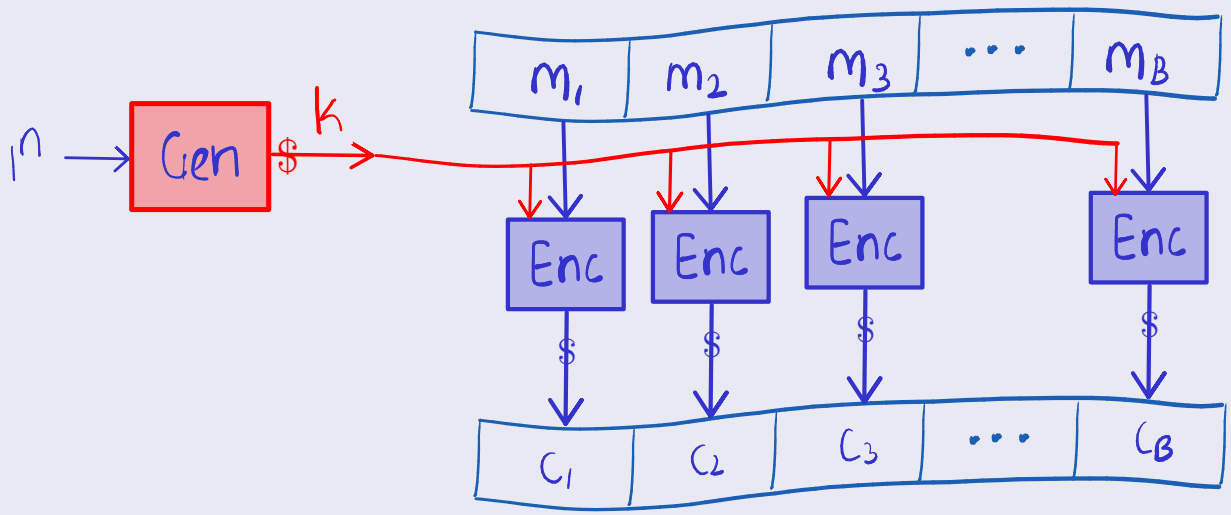


- $\forall i \in [1, B] : c_i \leftarrow \mathsf{Enc}(k, m_i)$

Baseline Scheme for Long Messages...

- IND-CPA for fixed-length $\Longrightarrow$ IND-CPA for arbitrary length
  - IND-CPA $\Longrightarrow$ can reuse the key!

Construction 1 (Π for $\mathcal{M} := \{0,1\}^n \Longrightarrow \Pi'$ for $\mathcal{M}^B := \{0,1\}^{Bn}$)



- $\forall i \in [1, B] : c_i \leftarrow \mathsf{Enc}(k, m_i)$

Exercise 1

Show that if Π is IND-CPA-secure then Π' is also IND-CPA-secure.

Baseline Scheme for Long Messages...

	Baseline
$\lvert\text{Ciphertext}\rvert$	$2nB$
#Random coins	nB
Paralellisable?	✓
IND-CPA-secure?	✓
Assumption on F	PRF

$\lvert\text{key}\rvert = \lvert\text{Message block}\rvert := n \quad \#\text{Message blocks} := B$

Baseline Scheme for Long Messages...

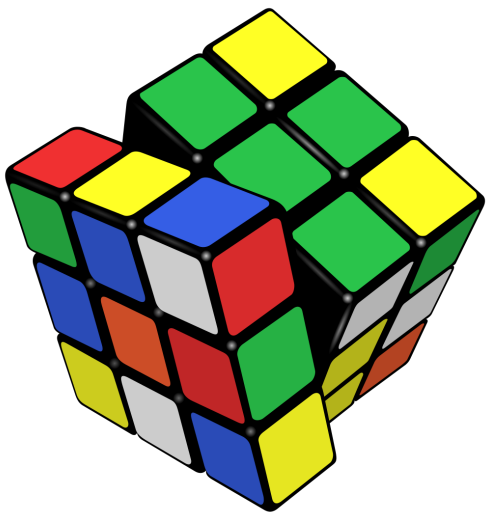
	Baseline	ECB	CBC	OFB	CTR	Ideal
|Ciphertext|	$2nB$	nB	$nB + n$	$nB + n$	$nB + n$	$nB + n$
#Random coins	nB					n
Paralellisable?	✓					✓
IND-CPA-secure?	✓					✓
Assumption on F	PRF					PRF

$|\text{key}| = |\text{Message block}| := n \quad \#\text{Message blocks} := B$

Plan for Today's Lecture

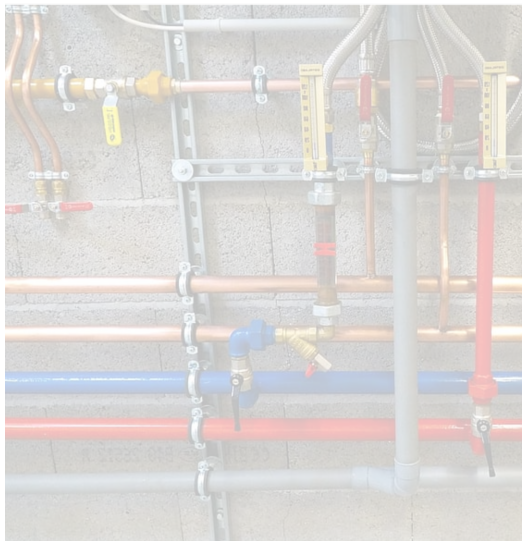
- Task: secure comm. of *multiple long* messages with shared keys
- Threat model: ind. against chosen-plaintext attack (IND-CPA)

Block Cipher a/k/a PRP



© Booyabazooka-Wikipedia

Modes of Operation



© pikist.com

Focus on efficiency: short ciphertexts, frugal use of random coins...

Recall Pseudo-Random Function (PRF)

- Indistinguishable from random function to PPT distinguishers 

Recall Pseudo-Random Function (PRF)

- Indistinguishable from random function to PPT distinguishers 

Definition 1 (Lecture 07)

A family of functions $\{F_k : \{0,1\}^n \to \{0,1\}^n\}_{k \in \{0,1\}^n}$ is a PRF if for every PPT *oracle distinguisher* D

$$\delta(n) := \left| \Pr_{k \leftarrow \{0,1\}^n}[D^{F_k(\cdot)}(1^n) = 0] - \Pr_{f \leftarrow \mathcal{F}_n}[D^{f(\cdot)}(1^n) = 0] \right|$$

is negligible.

Recall Pseudo-Random Function (PRF)

- Indistinguishable from random function to PPT distinguishers

Definition 1 (Lecture 07)

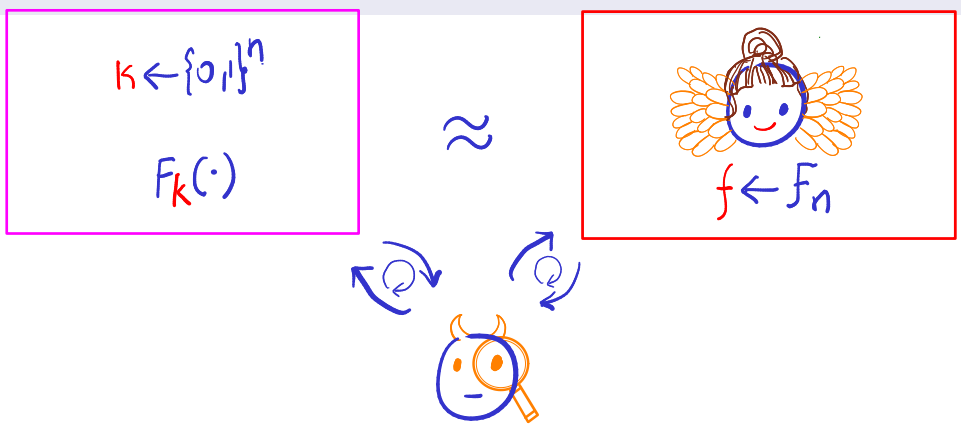
A family of functions $\{F_k : \{0,1\}^n \to \{0,1\}^n\}_{k \in \{0,1\}^n}$ is a PRF if for every PPT *oracle distinguisher* D

$$\delta(n) := \left| \Pr_{k \leftarrow \{0,1\}^n}[D^{F_k(\cdot)}(1^n) = 0] - \Pr_{f \leftarrow \mathcal{F}_n}[D^{f(\cdot)}(1^n) = 0] \right|$$

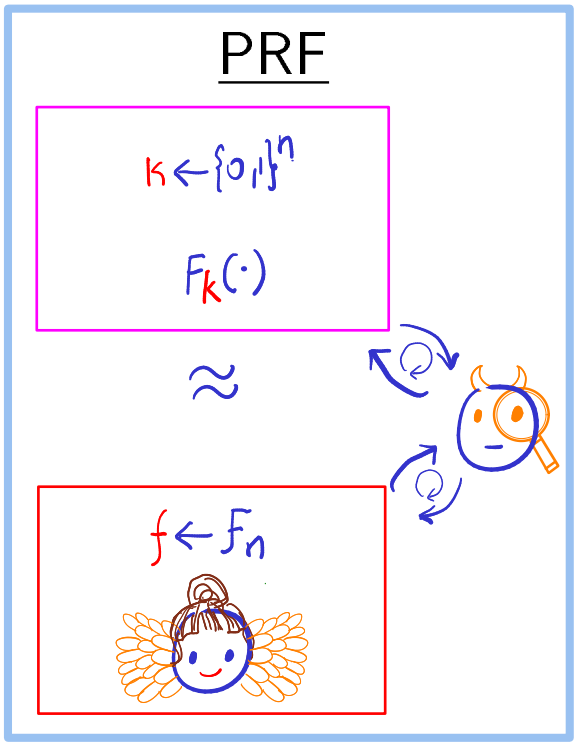
is negligible.

pseudorandom world

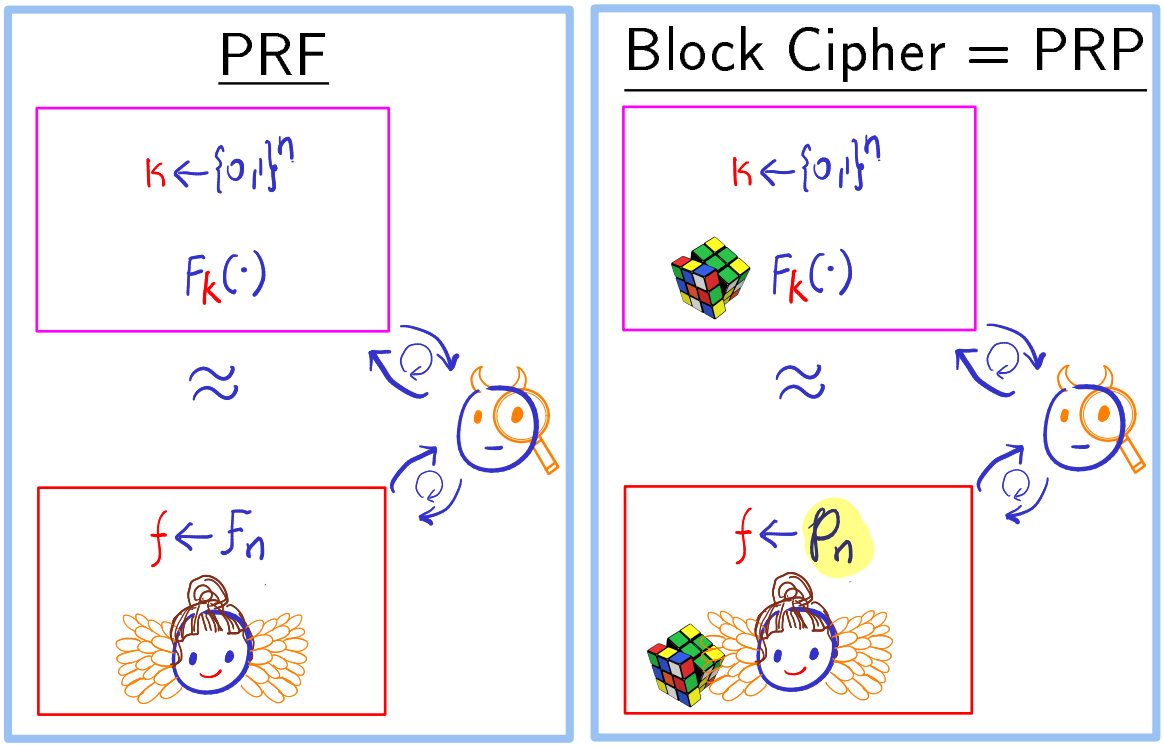
random world



Block Cipher = Pseudo-Random *Permutation* (PRP)

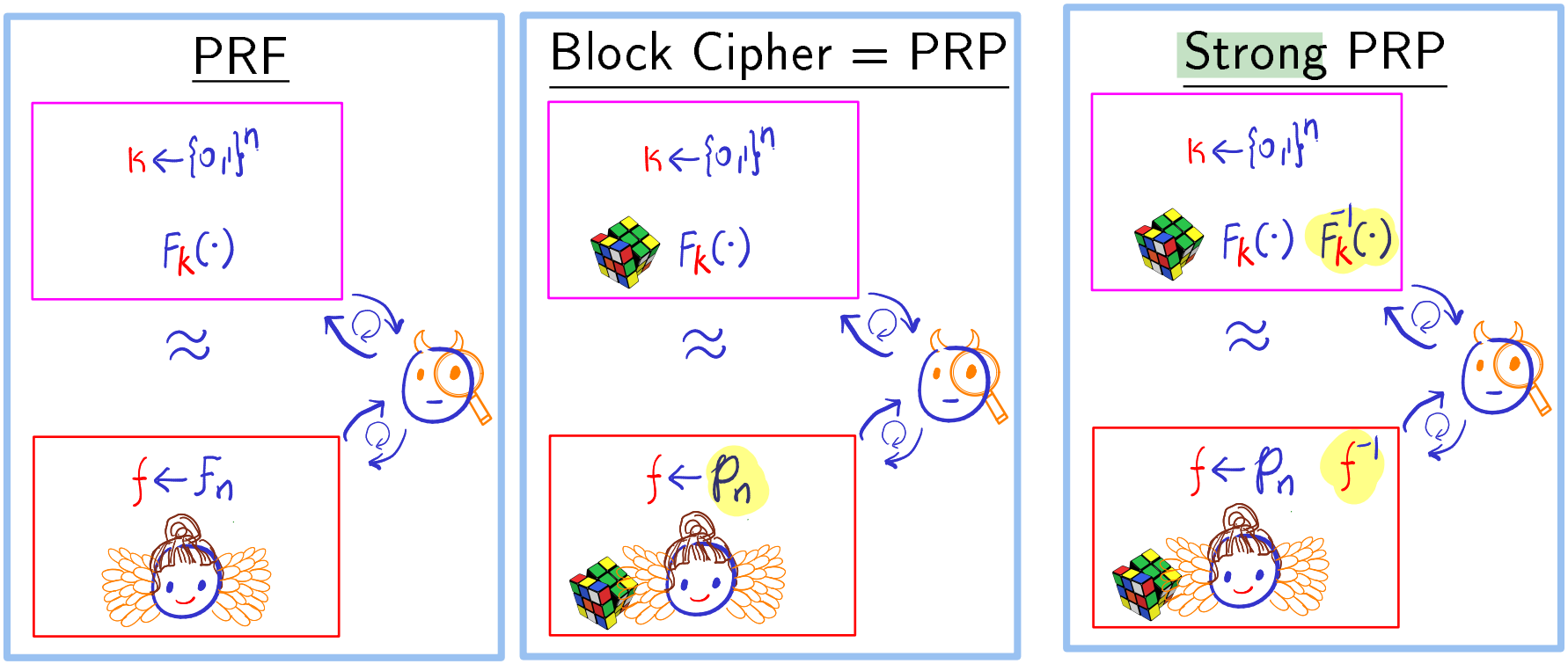


Block Cipher = Pseudo-Random *Permutation* (PRP)



- PRP: each F_k is a *permutation*
  - How many permutations are there in the PRP family?
- Ind. from random *permutation* from $\mathcal{P}_n$ (set of all perms.)
  - How many permutations are there from $\{0,1\}^n \to \{0,1\}^n$?

Block Cipher = Pseudo-Random *Permutation* (PRP)

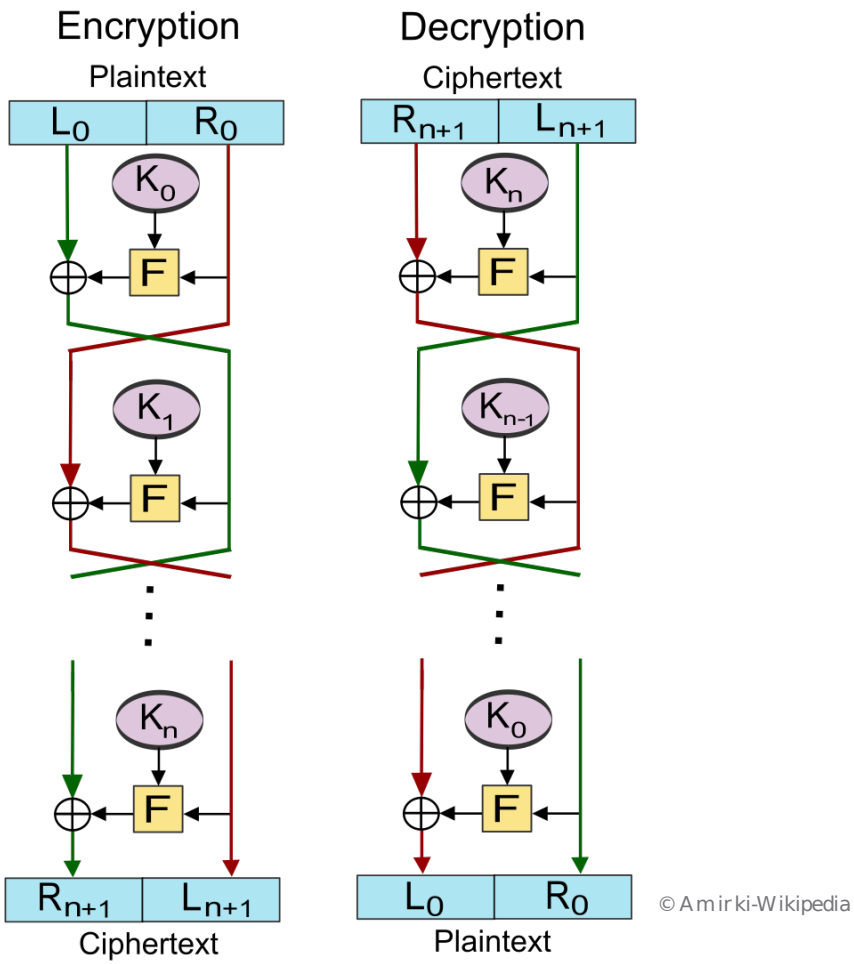


- PRP: each F_k is a *permutation*
  - How many permutations are there in the PRP family?
- Ind. from random *permutation* from $\mathcal{P}_n$ (set of all perms.)
  - How many permutations are there from $\{0,1\}^n \to \{0,1\}^n$?
- Strong PRP: indistinguishability holds even given "inverse oracle"

PRF $\Leftrightarrow$ PRP

Theorem 1 (Feistel cipher)

If PRFs exist, then so do (strong) PRPs.

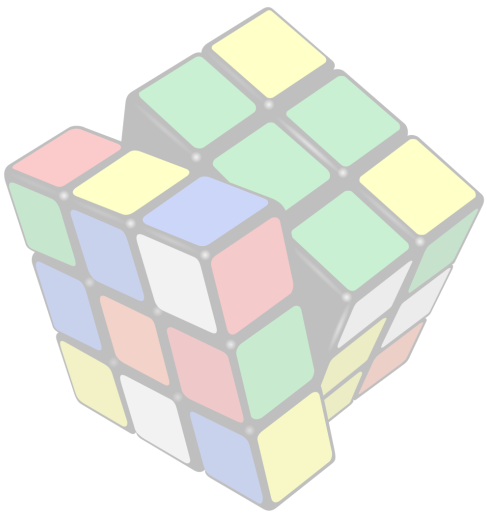


© Amirki-Wikipedia

Plan for Today's Lecture

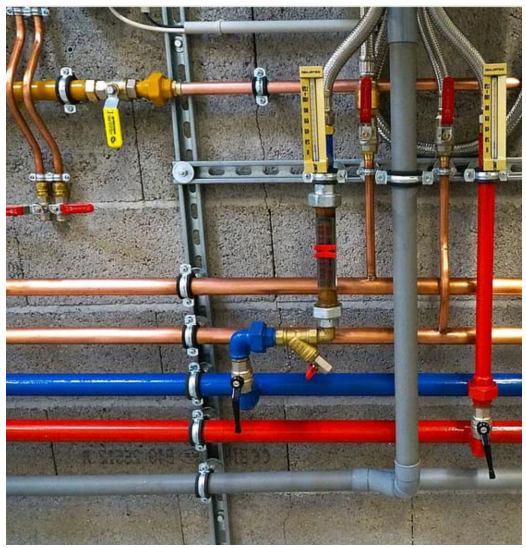
- Task: secure comm. of *multiple long* messages with shared keys
- Threat model: ind. against chosen-plaintext attack (IND-CPA)

Block Cipher a/k/a PRP



© Booyabazooka-Wikipedia

Modes of Operation



© pikist.com

Focus on efficiency: short ciphertexts, frugal use of random coins...

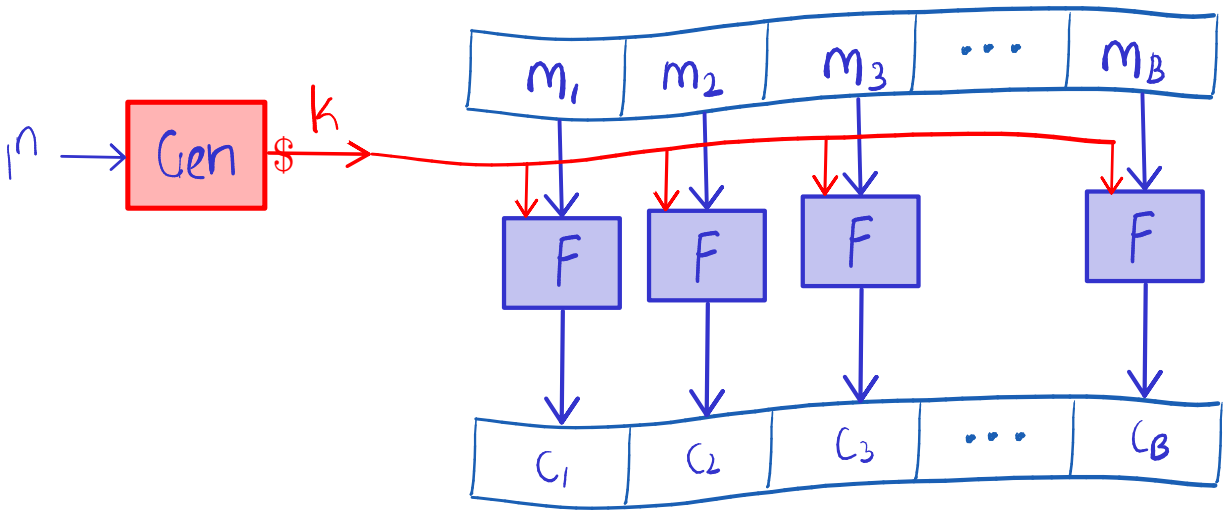
Modes of Operation: Motivation

- Given: $\{F_k : \{0,1\}^n \to \{0,1\}^n\}_{k \in \{0,1\}^n}$ that is PRF, PRP or SPRP

Modes of Operation: Motivation

- Given: $\{F_k : \{0,1\}^n \to \{0,1\}^n\}_{k \in \{0,1\}^n}$ that is PRF, PRP or SPRP

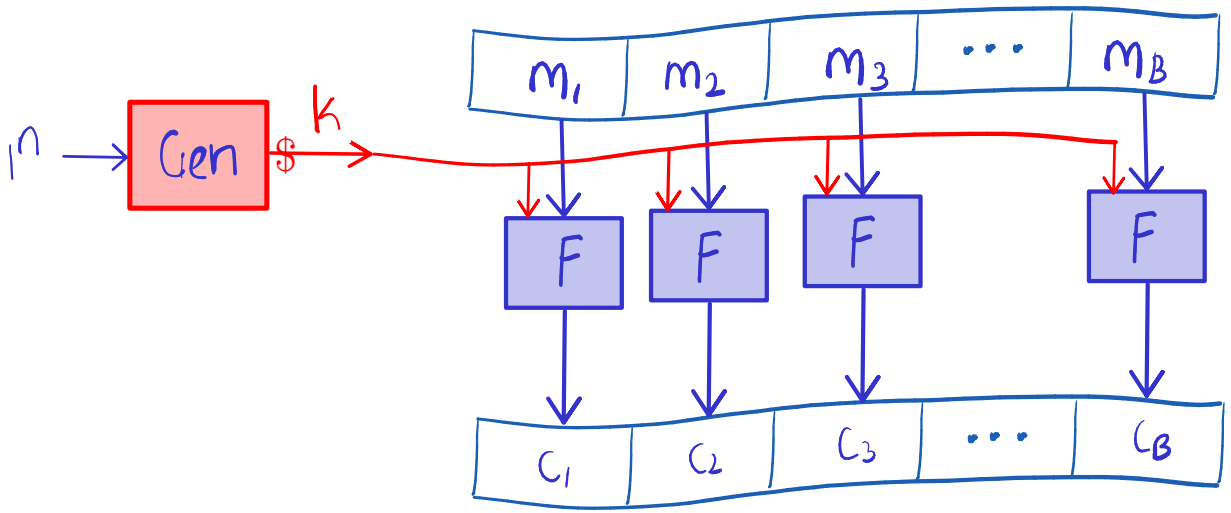
Goal: encrypt $m := m_1 \| \cdots \| m_B$, where $m_i \in \{0,1\}^n$



Modes of Operation: Motivation

- Given: $\{F_k : \{0,1\}^n \to \{0,1\}^n\}_{k \in \{0,1\}^n}$ that is PRF, PRP or SPRP

Goal: encrypt $m := m_1 \| \cdots \| m_B$, where $m_i \in \{0,1\}^n$



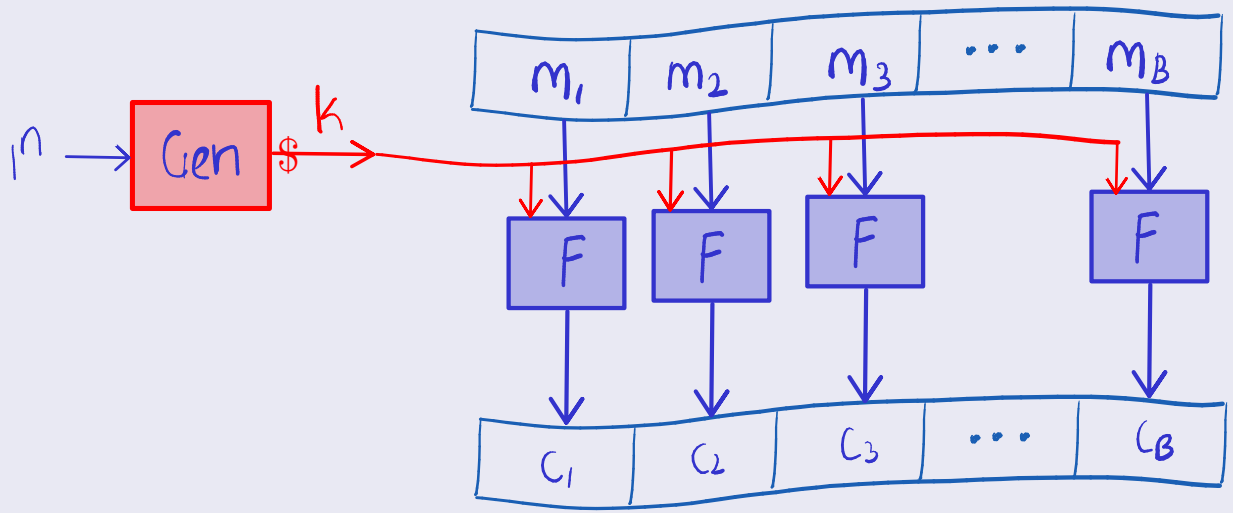
Optimise: ciphertext size, number of random coins...

Exercise 2 (Coming up in Lecture 10!)

What could we do if $|m|$ is not a multiple of n?

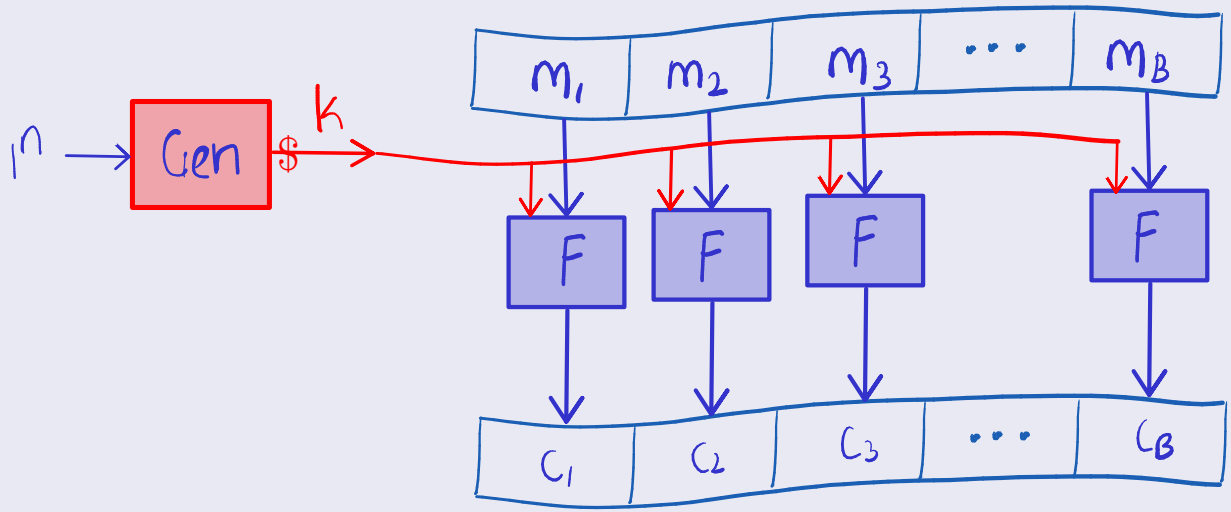
Electronic Codebook (ECB) Mode...

Construction 2



Electronic Codebook (ECB) Mode...

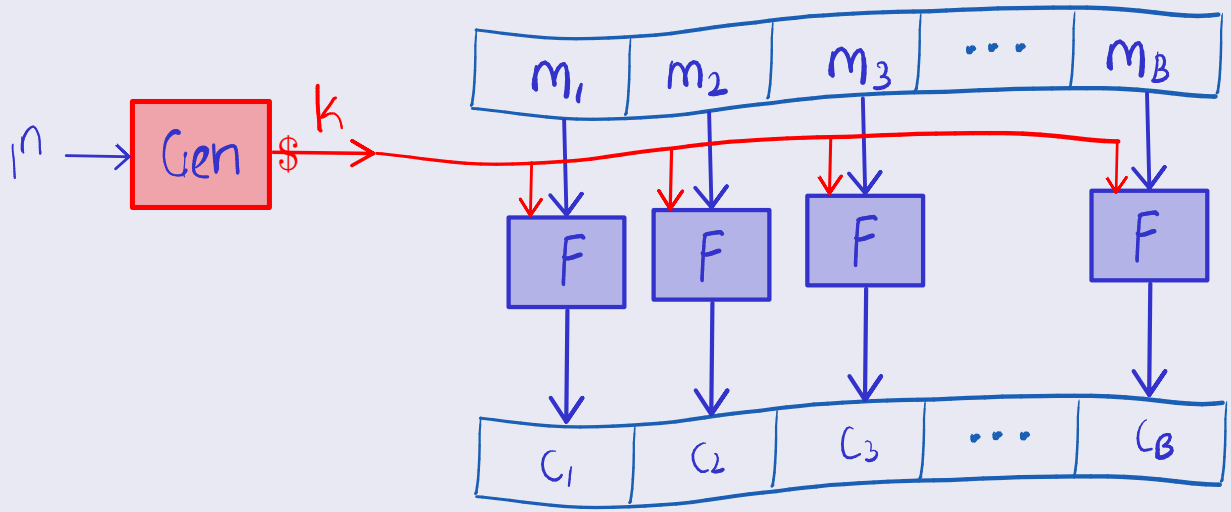
Construction 2



- $\forall i \in [1, B] : c_i := F(k, m_i)$

Electronic Codebook (ECB) Mode...

Construction 2

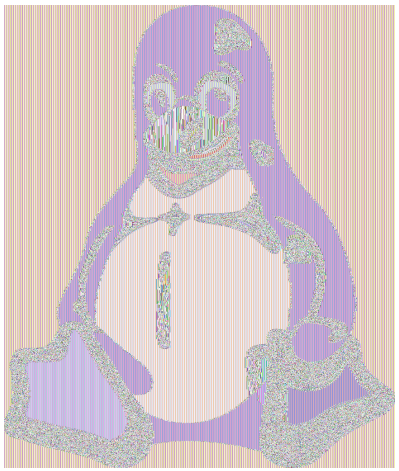


- $\forall i \in [1, B] : c_i := F(k, m_i)$

- |Ciphertext|: $|c| = |m|$
- #Random coins: No randomness!
- Paralellisable? Yes
- IND-CPA-secure? No, not even EAV*-secure!
- Assumption on F: N.A.

Electronic Codebook (ECB) Mode...

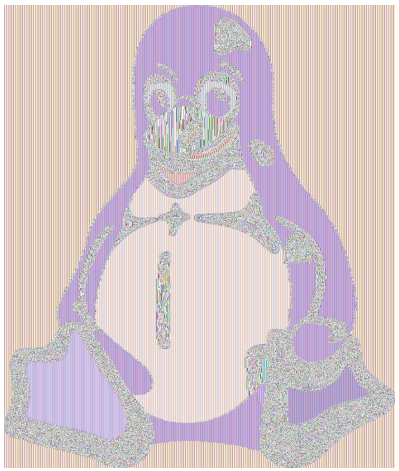
Guess the plaintext!



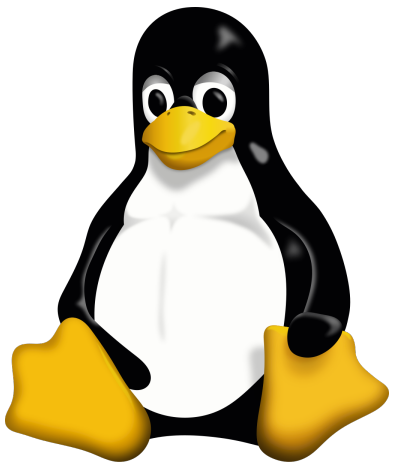
© RFL890-Wikipedia

Electronic Codebook (ECB) Mode...

Guess the plaintext!



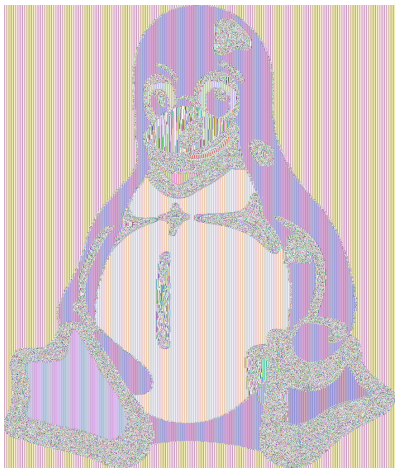
© RFL890-Wikipedia



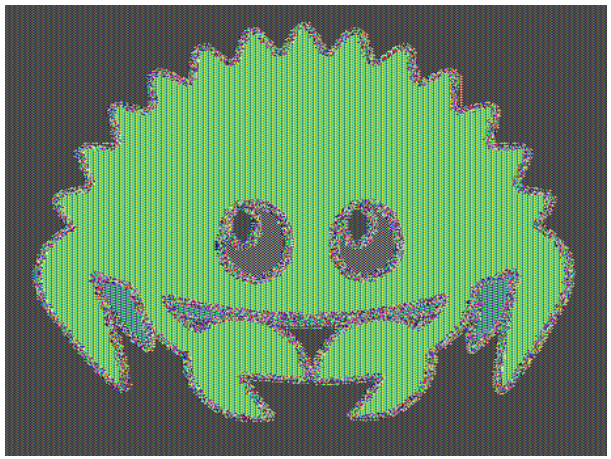
© Larry Ewing/GIMP-Wikipedia

Electronic Codebook (ECB) Mode...

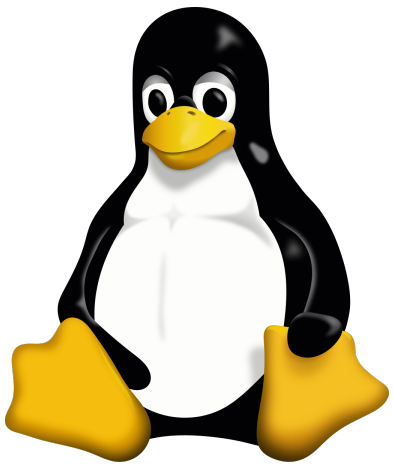
Guess the plaintext!



© RFL890-Wikipedia



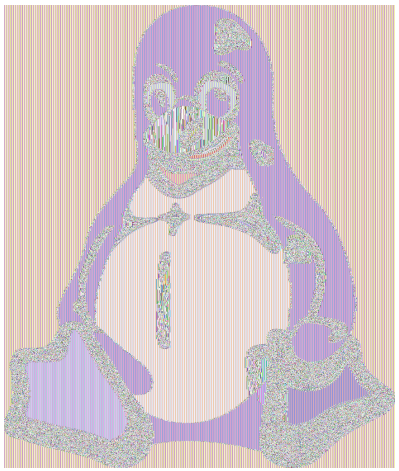
© github.com/sheroz/magma



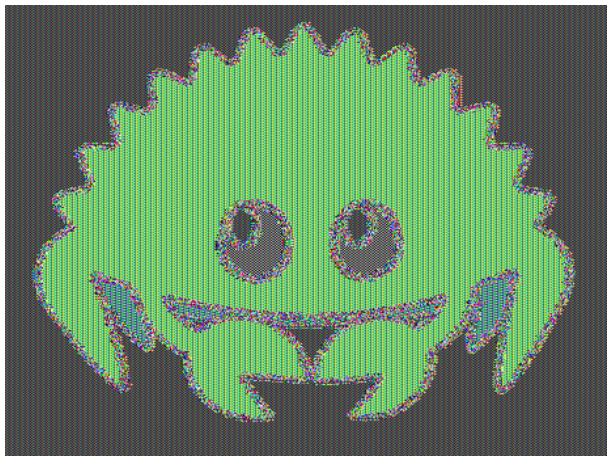
© Larry Ewing/GIMP-Wikipedia

Electronic Codebook (ECB) Mode...

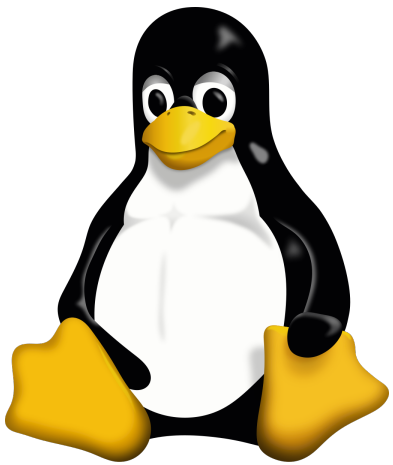
Guess the plaintext!



© RFL890-Wikipedia



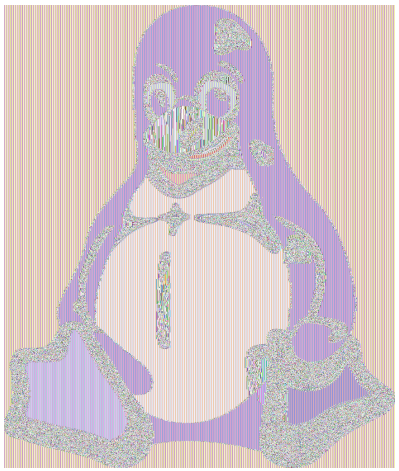
© github.com/sheroz/magma



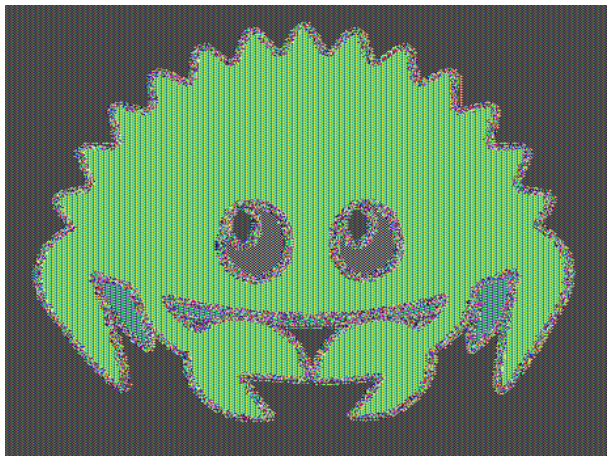
© Larry Ewing/GIMP-Wikipedia

Electronic Codebook (ECB) Mode...

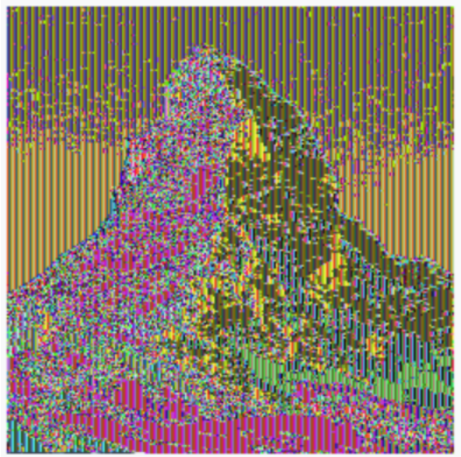
Guess the plaintext!



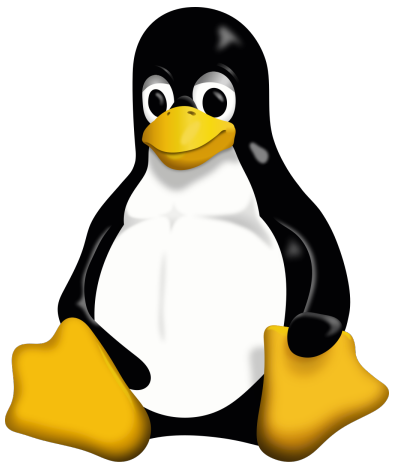
© RFL890-Wikipedia



© github.com/sheroz/magma



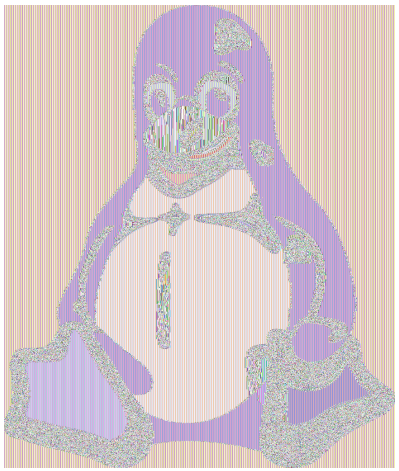
© blog.thomasdurand.fr



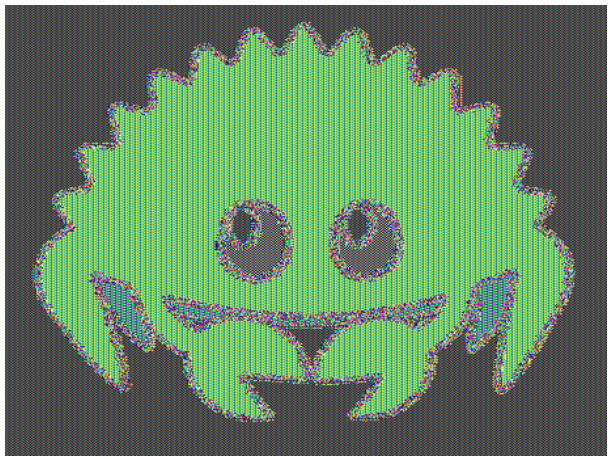
© Larry Ewing/GIMP-Wikipedia

Electronic Codebook (ECB) Mode...

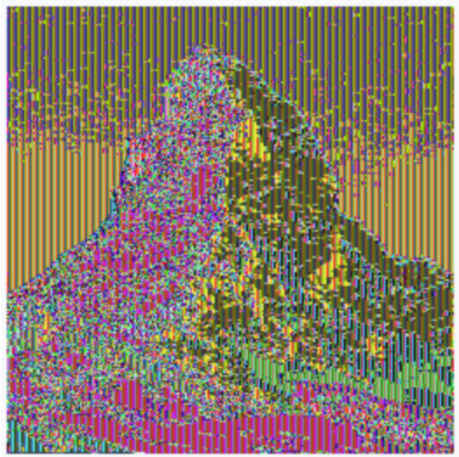
Guess the plaintext!



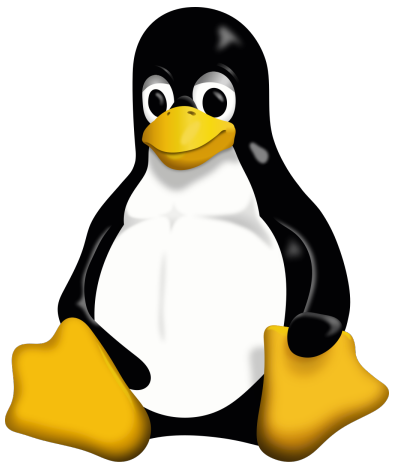
© RFL890-Wikipedia



© github.com/sheroz/magma



© blog.thomasdurand.fr



© Larry Ewing/GIMP-Wikipedia

Electronic Codebook (ECB) Mode...

	Baseline	Ideal
|Ciphertext|	$2nB$	$nB + n$
#Random coins	nB	n
Paralellisable?	✓	✓
IND-CPA-secure?	✓	✓
Assumption on F	PRF	PRF

$|\text{key}| = |\text{Message block}| := n \quad \#\text{Message blocks} := B$

Electronic Codebook (ECB) Mode...

	Baseline	ECB	CBC	OFB	CTR	Ideal
|Ciphertext|	$2nB$	nB	$nB + n$	$nB + n$	$nB + n$	$nB + n$
#Random coins	nB	0				n
Paralellisable?	✓	✓				✓
IND-CPA-secure?	✓	×				✓
Assumption on F	PRF	N.A.				PRF

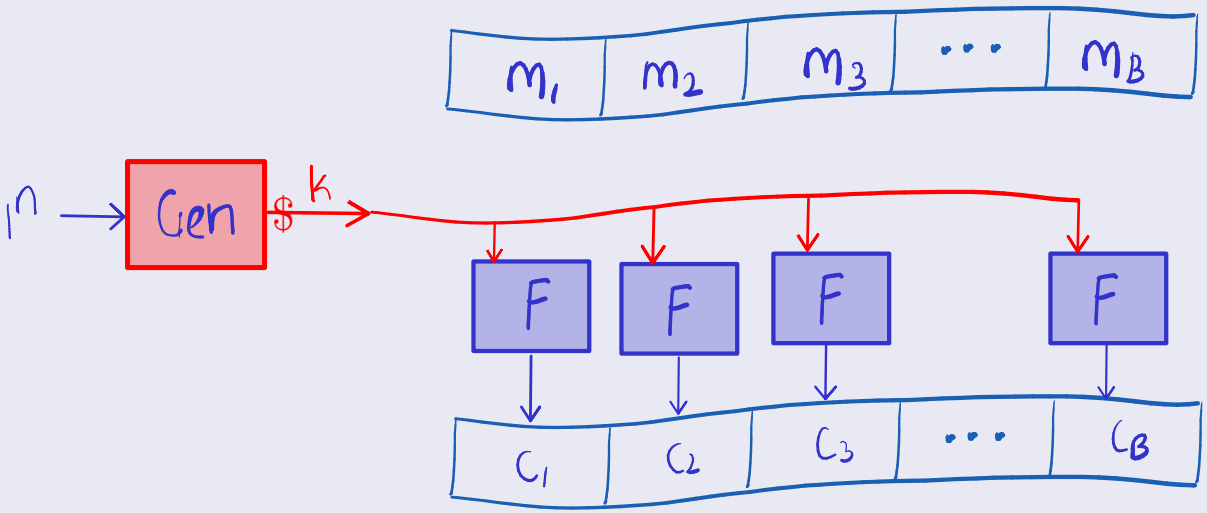
$|\text{key}| = |\text{Message block}| := n \quad \#\text{Message blocks} := B$

Exercise 3

Write down pseudocode for ECB mode

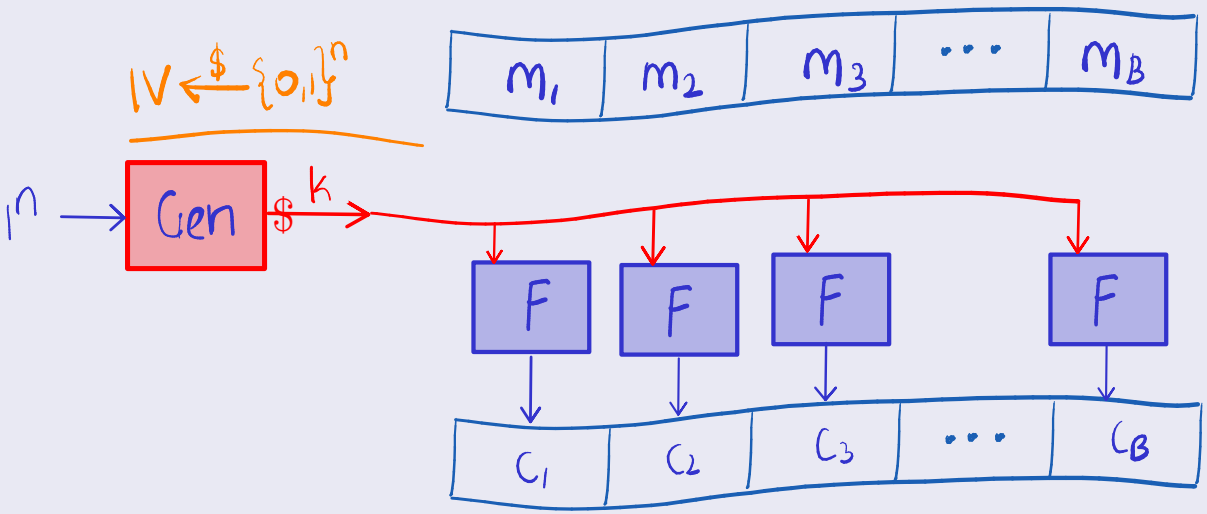
Cipher-Block Chaining (CBC) Mode...

Construction 3 ?



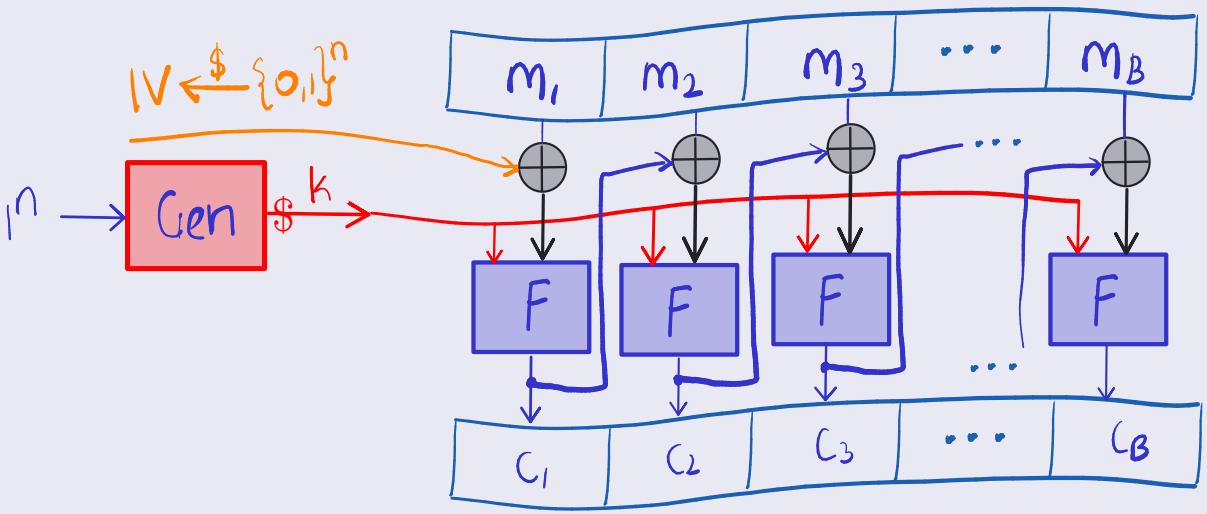
Cipher-Block Chaining (CBC) Mode...

Construction 3 ?



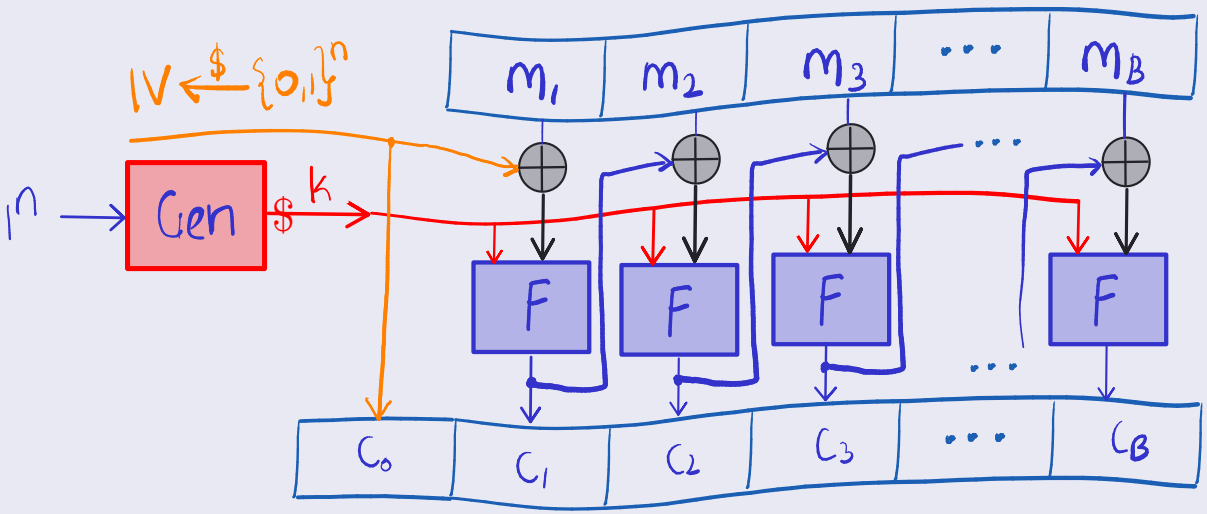
Cipher-Block Chaining (CBC) Mode...

Construction 3 (?)



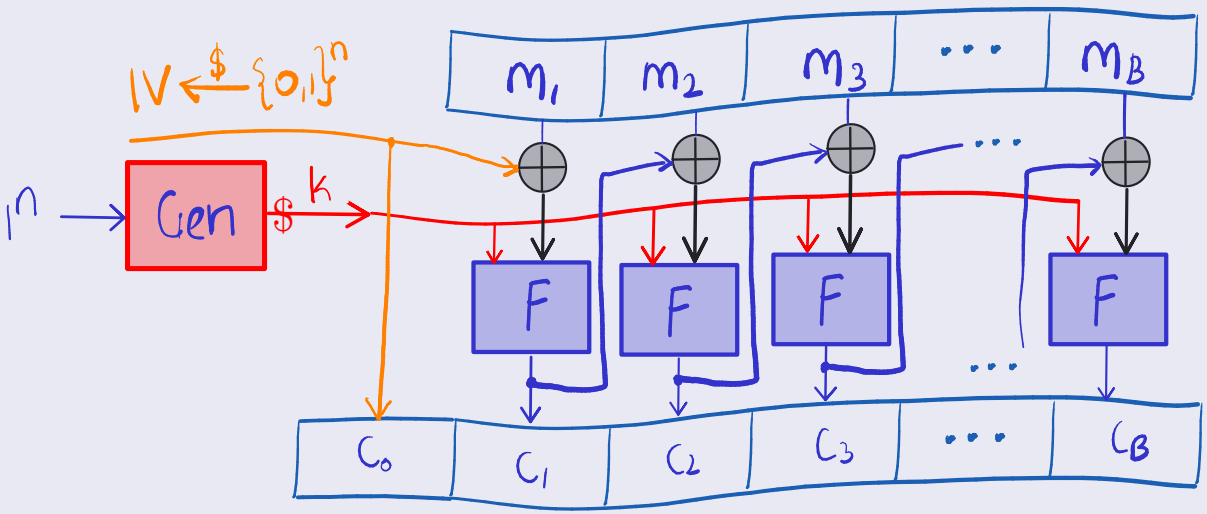
Cipher-Block Chaining (CBC) Mode...

Construction 3 (?)



Cipher-Block Chaining (CBC) Mode...

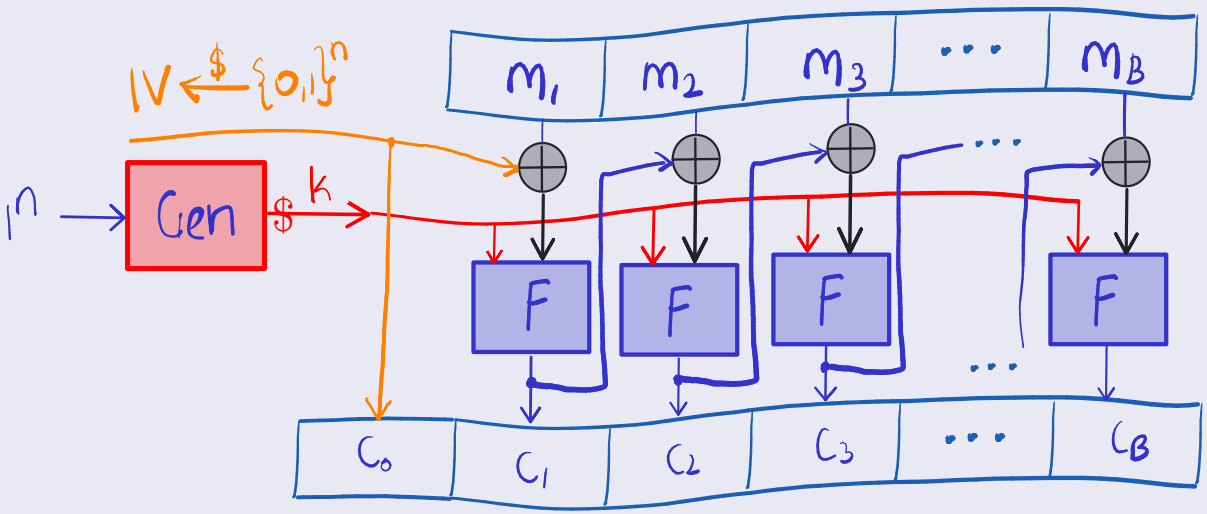
Construction 3



- $c_0 := IV$, $\forall i \in [1, B] : c_i := F(k, c_{i-1} \oplus m_i)$

Cipher-Block Chaining (CBC) Mode...

Construction 3 (?)



- $c_0 := IV$, $\forall i \in [1, B] : c_i := F(k, c_{i-1} \oplus m_i)$

- |Ciphertext|: $|m| + n = nB + n$
- #Random coins: n
- Paralellisable? No, inherently sequential
- IND-CPA-secure? Yes!
- Assumption on F: F must be a PRP (for perfect correctness)

Cipher-Block Chaining (CBC) Mode...

	Baseline	ECB	Ideal
|Ciphertext|	$2nB$	nB	$nB + n$
#Random coins	nB	0	n
Paralellisable?	✓	✓	✓
IND-CPA-secure?	✓	×	✓
Assumption on F	PRF	N.A.	PRF

$|\text{key}| = |\text{Message block}| := n \quad \#\text{Message blocks} := B$

Cipher-Block Chaining (CBC) Mode...

	Baseline	ECB	CBC	OFB	CTR	Ideal
|Ciphertext|	$2nB$	nB	$nB + n$	$nB + n$	$nB + n$	$nB + n$
#Random coins	nB	0	n			n
Paralellisable?	✓	✓	×			✓
IND-CPA-secure?	✓	×	✓			✓
Assumption on F	PRF	N.A.	PRP			PRF

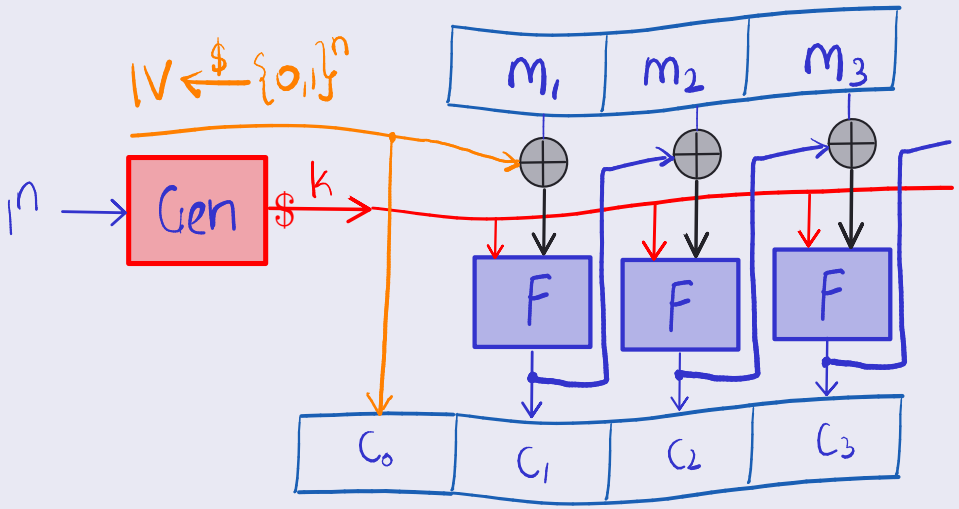
$|\text{key}| = |\text{Message block}| := n \quad \#\text{Message blocks} := B$

Exercise 4

1. Write down pseudocode for CBC mode
2. Prove that if F is a SPRP then CBC mode is CPA secure

Chained CBC Mode: IV Misuse

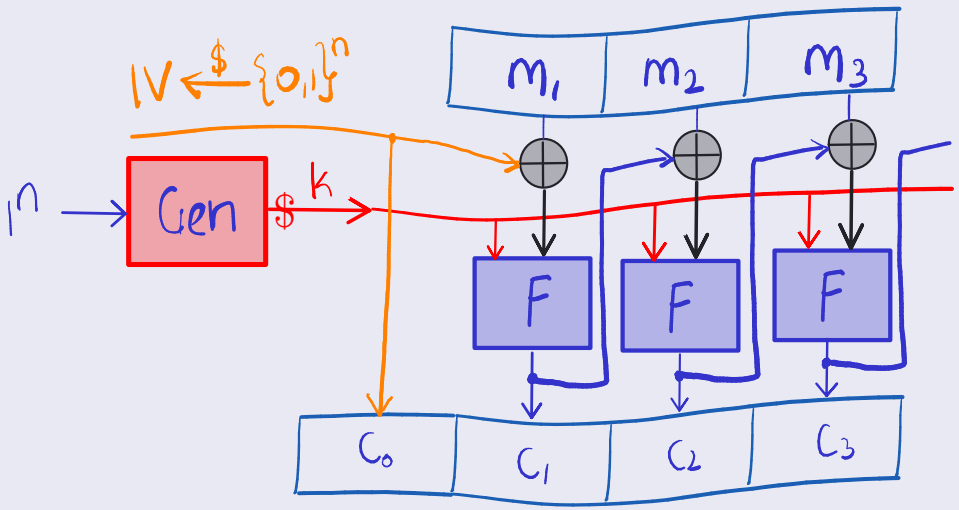
Construction 3



- $c_0 := IV, \forall i \in [1, B] : c_i := F(k, c_{i-1} \oplus m_i)$

Chained CBC Mode: IV Misuse

Construction 3



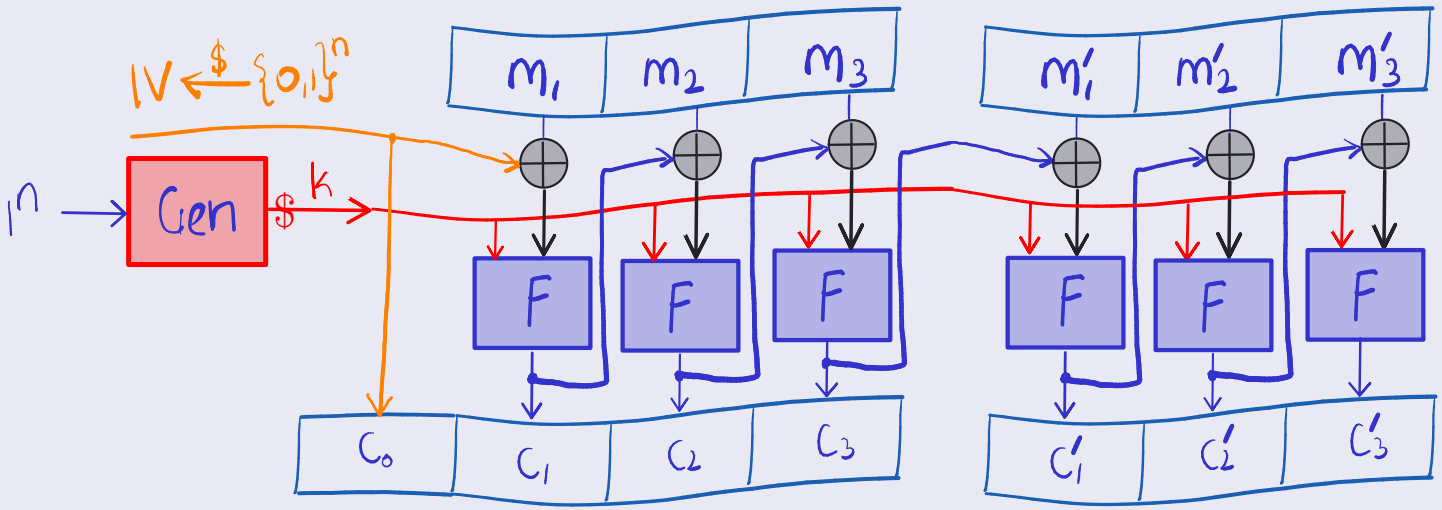
- $c_0 := IV, \forall i \in [1, B] : c_i := F(k, c_{i-1} \oplus m_i)$

? In random IV necessary? Is choosing distinct IVs enough?

- Stateful mode: c_B from previous round used as IV for current round

Chained CBC Mode: IV Misuse

Construction 3



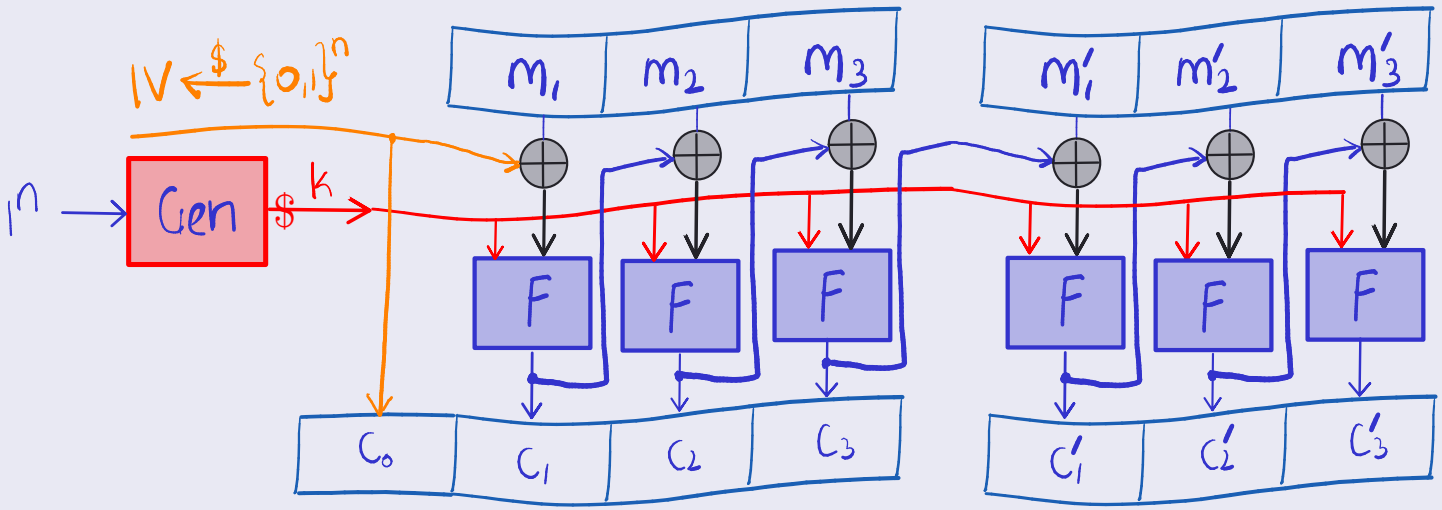
- $c_0 := IV$, $\forall i \in [1, B] : c_i := F(k, c_{i-1} \oplus m_i)$

? In random IV necessary? Is choosing distinct IVs enough?

- Stateful mode: c_B from previous round used as IV for current round

Chained CBC Mode: IV Misuse

Construction 3



- $c_0 := IV, \forall i \in [1, B] : c_i := F(k, c_{i-1} \oplus m_i)$

(?) In random IV necessary? Is choosing distinct IVs enough?

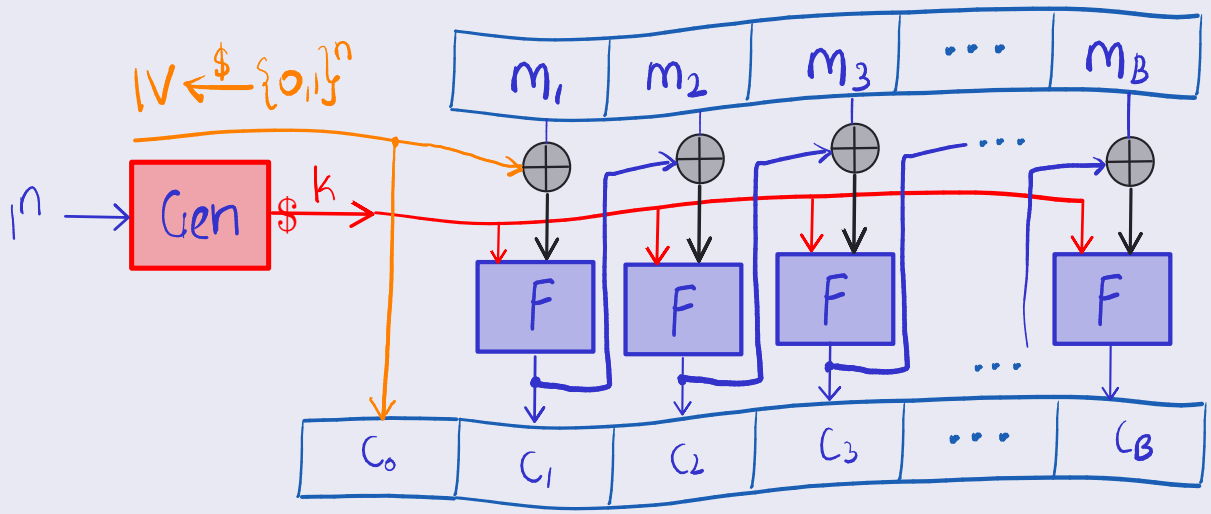
- Stateful mode: c_B from previous round used as IV for current round

Exercise 5 ⚠

Show that chained CBC mode is *not* IND-CPA secure!

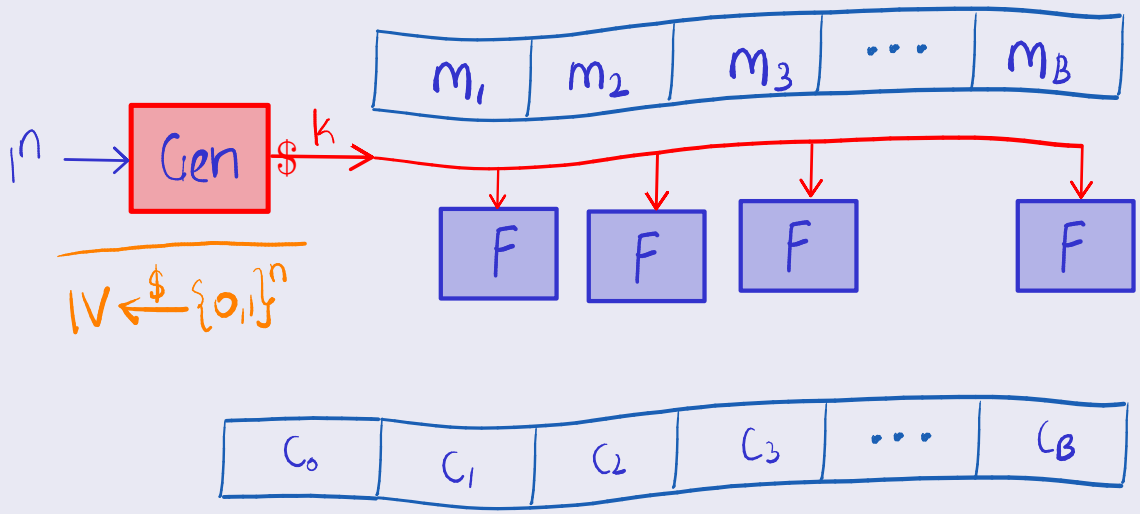
Output Feedback (OFB) Mode...

Construction 4



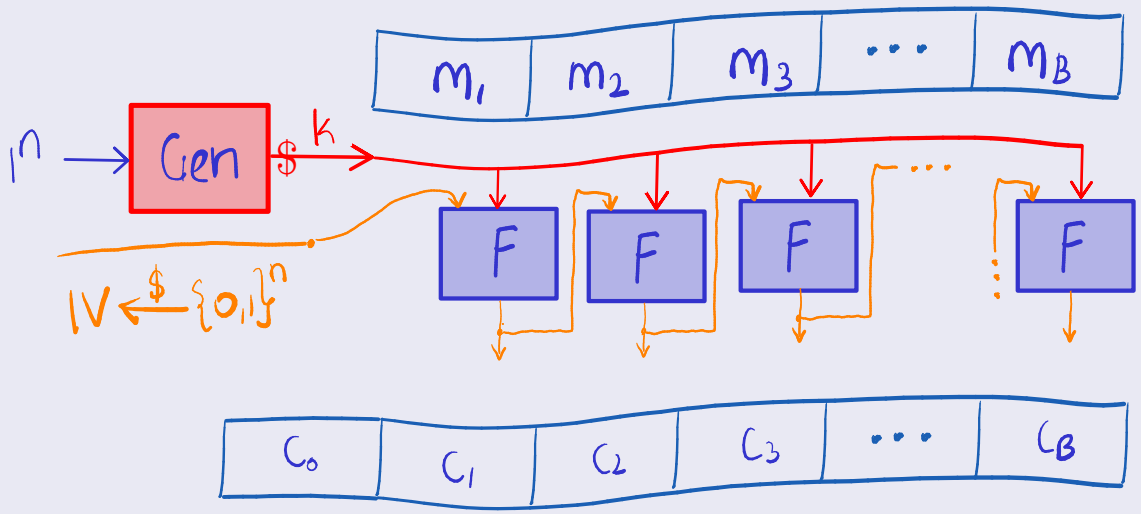
Output Feedback (OFB) Mode...

Construction 4



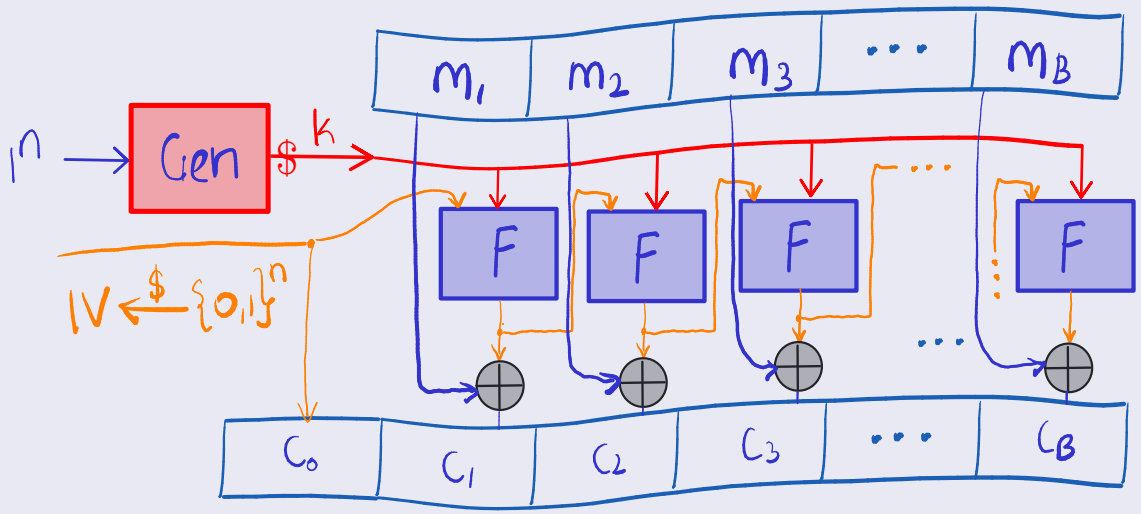
Output Feedback (OFB) Mode...

Construction 4



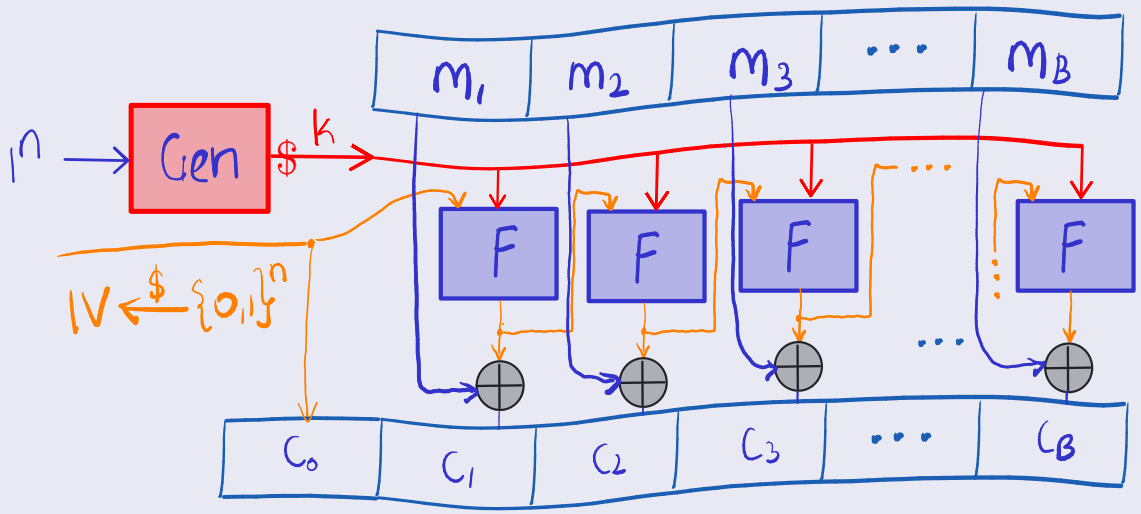
Output Feedback (OFB) Mode...

Construction 4



Output Feedback (OFB) Mode...

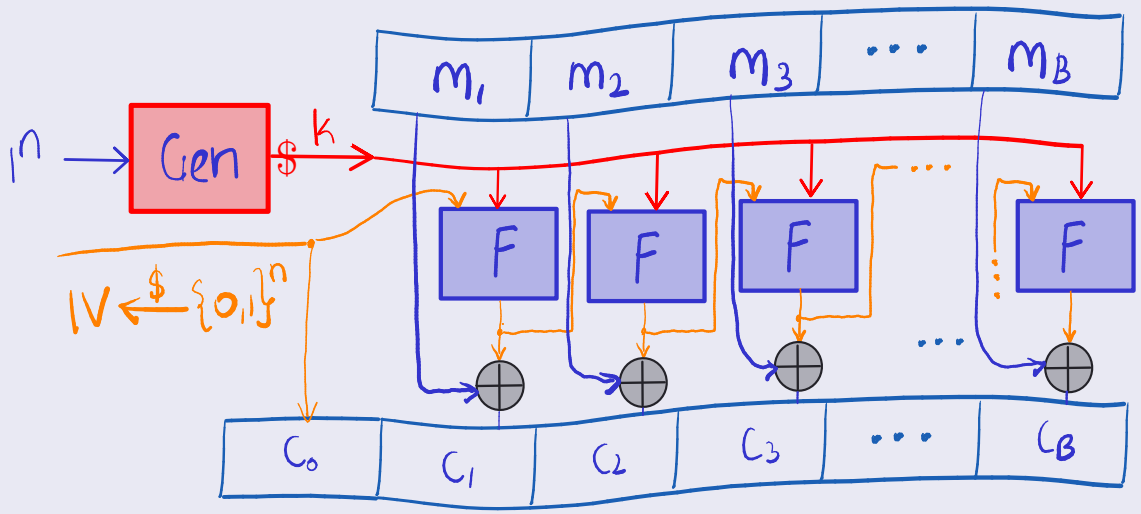
Construction 4



- $c_0 = y_0 := IV$, $\forall i \in [1, B] : c_i := y_i \oplus m_i$, where $y_i := F(k, y_{i-1})$

Output Feedback (OFB) Mode...

Construction 4



- $c_0 = y_0 := IV$, $\forall i \in [1, B] : c_i := y_i \oplus m_i$, where $y_i := F(k, y_{i-1})$

- |Ciphertext|: $|m| + n = nB + n$
- #Random coins: n
- Paralellisable? No, but precomputable
- IND-CPA-secure? Yes! So is the stateful chained variant
- Assumption on F: PRF

Output Feedback (OFB) Mode...

	Baseline	ECB	CBC	Ideal
|Ciphertext|	$2nB$	nB	$nB + n$	$nB + n$
#Random coins	nB	0	n	n
Paralellisable?	✓	✓	×	✓
IND-CPA-secure?	✓	×	✓	✓
Assumption on F	PRF	N.A.	PRP	PRF

$|\text{key}| = |\text{Message block}| := n \quad \#\text{Message blocks} := B$

Output Feedback (OFB) Mode...

	Baseline	ECB	CBC	OFB	CTR	Ideal
|Ciphertext|	$2nB$	nB	$nB + n$	$nB + n$	$nB + n$	$nB + n$
#Random coins	nB	0	n	n		n
Paralellisable?	✓	✓	×	×		✓
IND-CPA-secure?	✓	×	✓	✓		✓
Assumption on F	PRF	N.A.	PRP	PRF		PRF

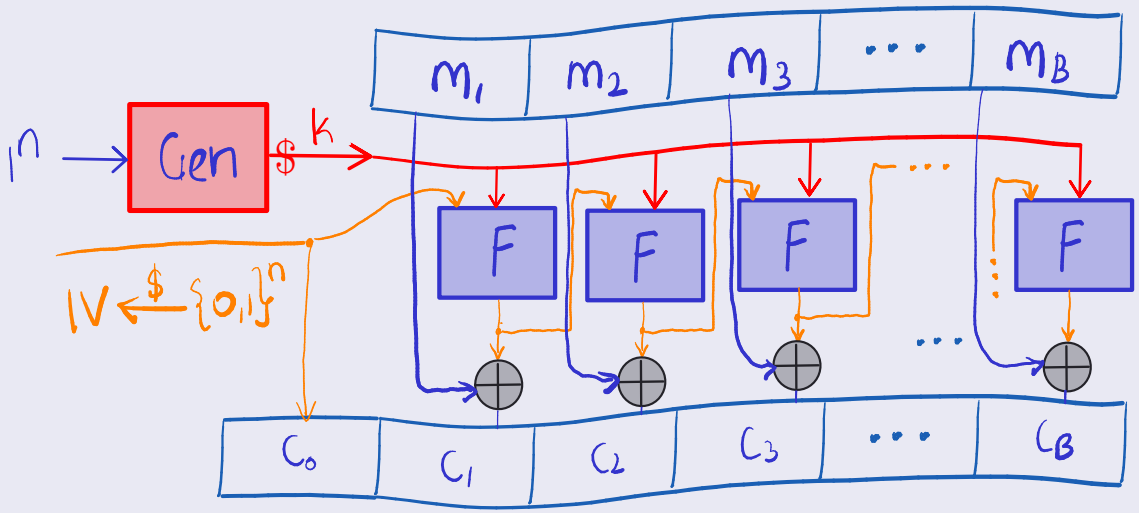
$|\text{key}| = |\text{Message block}| := n \quad \#\text{Message blocks} := B$

Exercise 6

Write down pseudocode for OFB mode

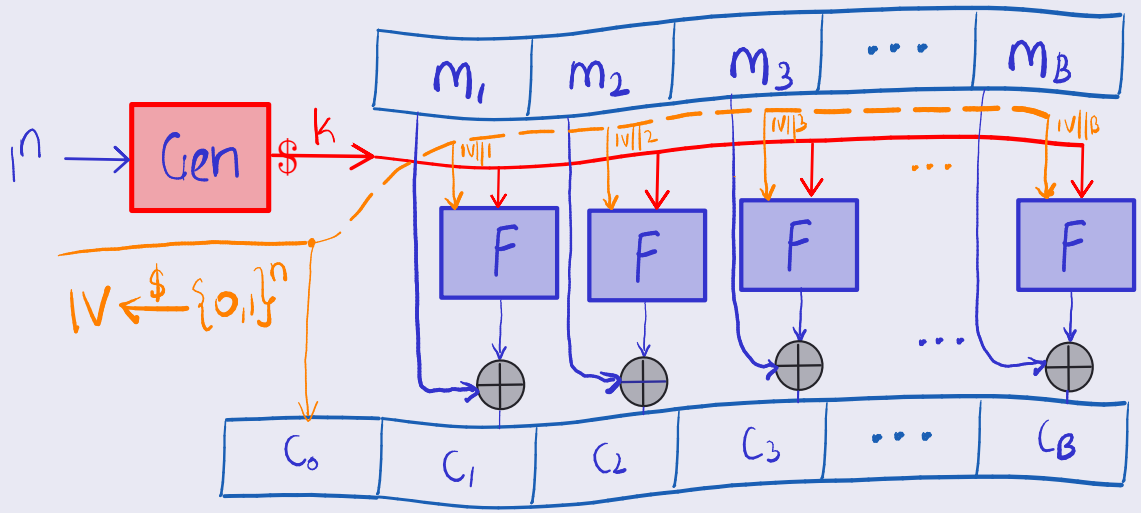
Counter (CTR) Mode...

Construction 5



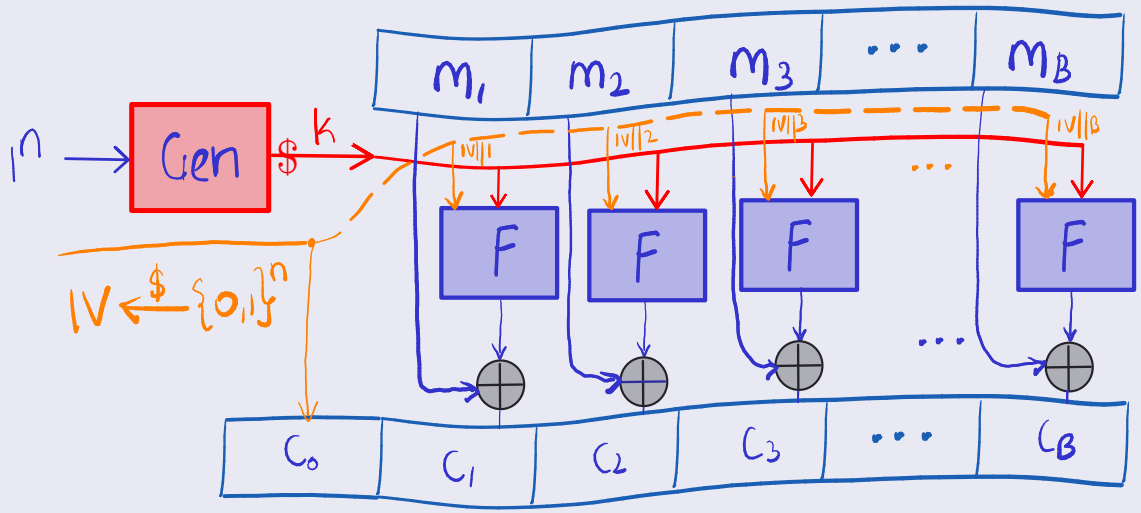
Counter (CTR) Mode...

Construction 5



Counter (CTR) Mode...

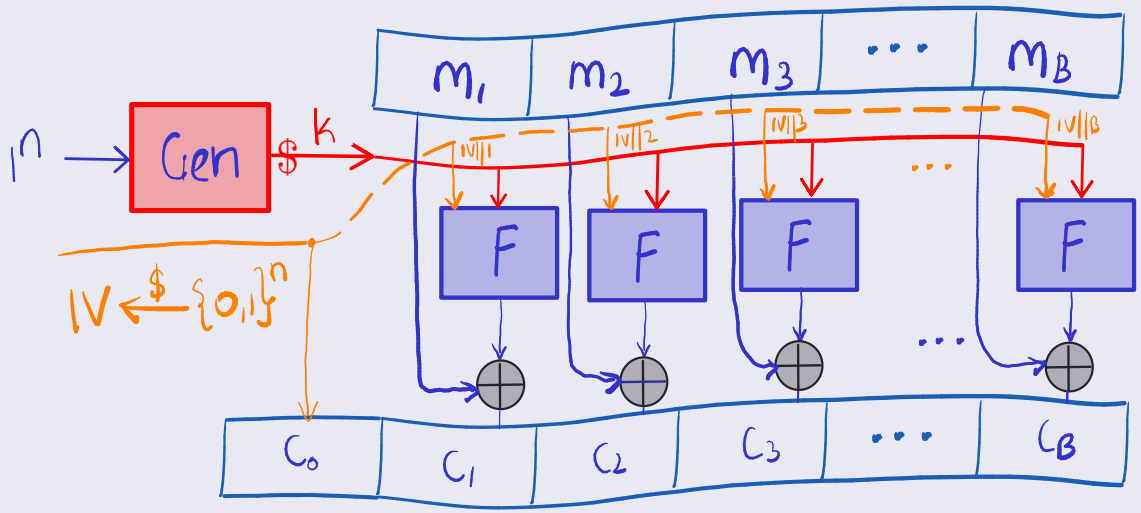
Construction 5



- $c_0 := IV$, $\forall i \in [1, B] : c_i := F(k, IV \| i) \oplus m_i$

Counter (CTR) Mode...

Construction 5



- $c_0 := IV$, $\forall i \in [1, B] : c_i := F(k, IV \| i) \oplus m_i$

- |Ciphertext|: $|m| + n = nB + n$
- #Random coins: n
- Paralellisable? Yes, fully!
- IND-CPA-secure? Yes! So is the stateful chained variant
- Assumption on F: PRF

Counter (CTR) Mode...

	Baseline	ECB	CBC	OFB	Ideal
|Ciphertext|	$2nB$	nB	$nB + n$	$nB + n$	$nB + n$
#Random coins	nB	0	n	n	n
Paralellisable?	✓	✓	×	×	✓
IND-CPA-secure?	✓	×	✓	✓	✓
Assumption on F	PRF	N.A.	SPRP	PRF	PRF

$|\text{key}| = |\text{Message block}| := n \quad \#\text{Message blocks} := B$

Counter (CTR) Mode...

	Baseline	ECB	CBC	OFB	CTR	Ideal
|Ciphertext|	$2nB$	nB	$nB + n$	$nB + n$	$nB + n$	$nB + n$
#Random coins	nB	0	n	n	n	n
Paralellisable?	✓	✓	×	×	✓	✓
IND-CPA-secure?	✓	×	✓	✓	✓	✓
Assumption on F	PRF	N.A.	SPRP	PRF	PRF	PRF

$|\text{key}| = |\text{Message block}| := n \quad \#\text{Message blocks} := B$

Exercise 7

Write down pseudocode for CTR mode

Some Practical Considerations

- How many messages can be sent?
  - Recall: $|\text{IV}|=|\text{Block}|=n$ and $IV \leftarrow \{0,1\}^n$
  - After $\approx 2^{n/2}$ encryptions, IV will repeat with constant probability
  - Breakable if n is too short (e.g., 64)

Some Practical Considerations

- How many messages can be sent?
  - Recall: $|\text{IV}|=|\text{Block}|=n$ and $IV \leftarrow \{0,1\}^n$
  - After $\approx 2^{n/2}$ encryptions, IV will repeat with constant probability
  - Breakable if n is too short (e.g., 64)

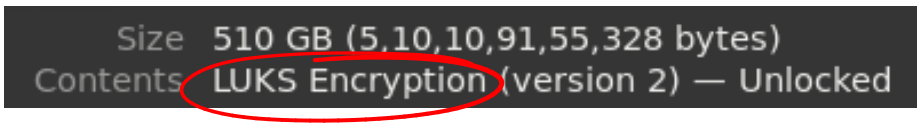
- IV misuse: if IV repeated then
  - In CTR and OFB mode, same pseudorandom mask generated $\Longrightarrow$ security lost
  - CBC mode doesn't seem to be affected. Why?

Recap/Next Lecture

- Block cipher: (strong) pseudo-random permutation
- Modes of operation
  - Discussed: ECB, CBC, OFB and CTR
  - Other modes: Cipher feedback (CFB), XOR-Encrypt-XOR (XEX)...

Recap/Next Lecture

- Block cipher: (strong) pseudo-random permutation
- Modes of operation
  - Discussed: ECB, CBC, OFB and CTR
  - Other modes: Cipher feedback (CFB), XOR-Encrypt-XOR (XEX)...

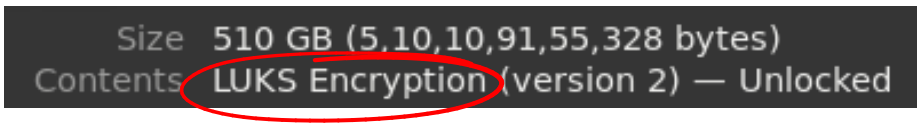


©Wikipedia

  - IRL:
    - ⚠ Chained CBC: SSL 3.0/TLS 1.0
    - Galois/Counter mode (GCM): WPA3 (Wi-Fi protocol)
    - AES-XTS: LUKS disk encryption

Recap/Next Lecture

- Block cipher: (strong) pseudo-random permutation
- Modes of operation
  - Discussed: ECB, CBC, OFB and CTR
  - Other modes: Cipher feedback (CFB), XOR-Encrypt-XOR (XEX)...



  - IRL:
    - ⚠ Chained CBC: SSL 3.0/TLS 1.0
    - Galois/Counter mode (GCM): WPA3 (Wi-Fi protocol)
    - AES-XTS: LUKS disk encryption

- Next lecture
  - Stronger threat model: chosen-ciphertext attack (CCA)
    - If time permits: padding oracle attack
  - Message-*authentication* codes (MACs)

Further Reading

1. More details on modes of operations can be found in [KL14, §3.6.3]
2. You can read more about Feistel cipher and Theorem 1 in [KL14, §7.2.2]


Jonathan Katz and Yehuda Lindell.
Introduction to Modern Cryptography (3rd ed.).
Chapman and Hall/CRC, 2014.