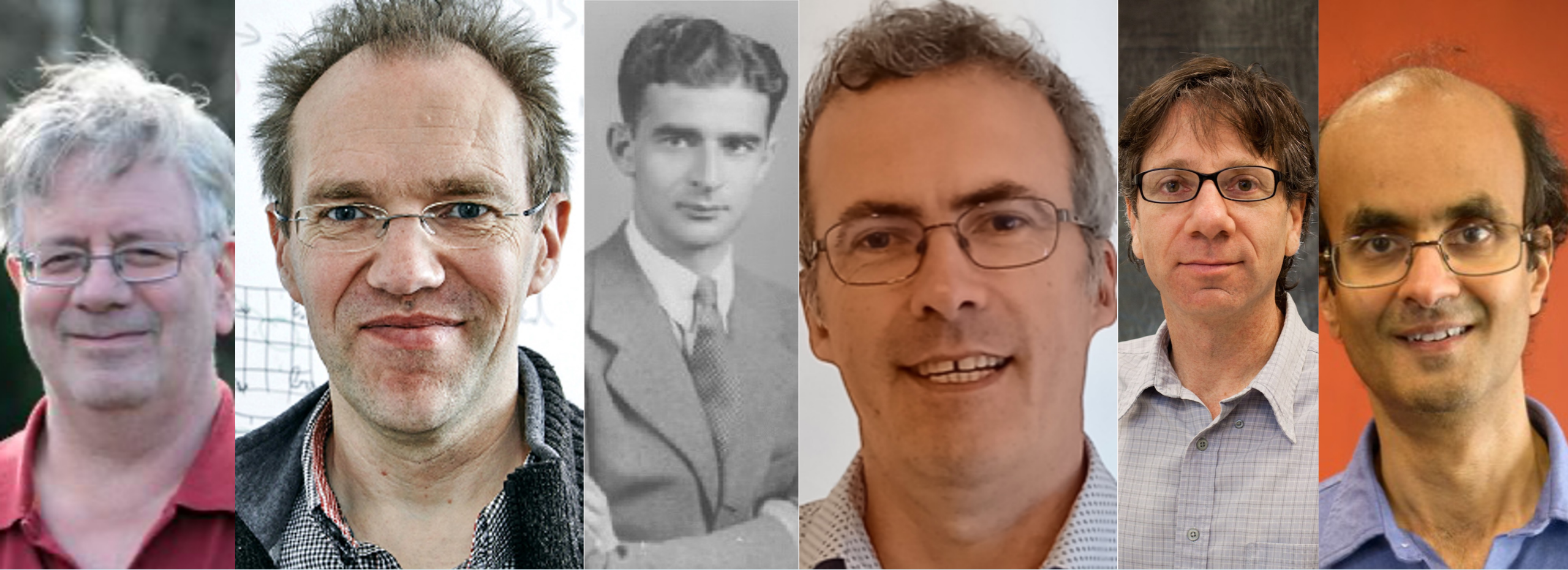


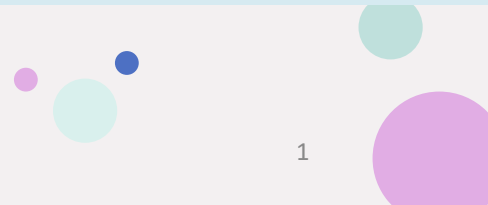


Lecture 8

CPA security, Modes of Operation

CS409/6011: Introduction to Cryptography

Instructor: Sruthi Sekar



Recap

- How to encrypt multiple messages using the same key in the eavesdropper Eve world?
 - **Stateful Setting:** can be done using PRGs (not desired)
 - **Stateless:** Repeating a deterministic encryption using the same key for multiple messages is not secure.
- **Stateless Symmetric Encryption Scheme for multiple messages:** using a random function oracle (gives you exponential one time pads that are efficiently accessible)
- **Pseudorandom Functions:** computational analogue of a random oracle.

Today

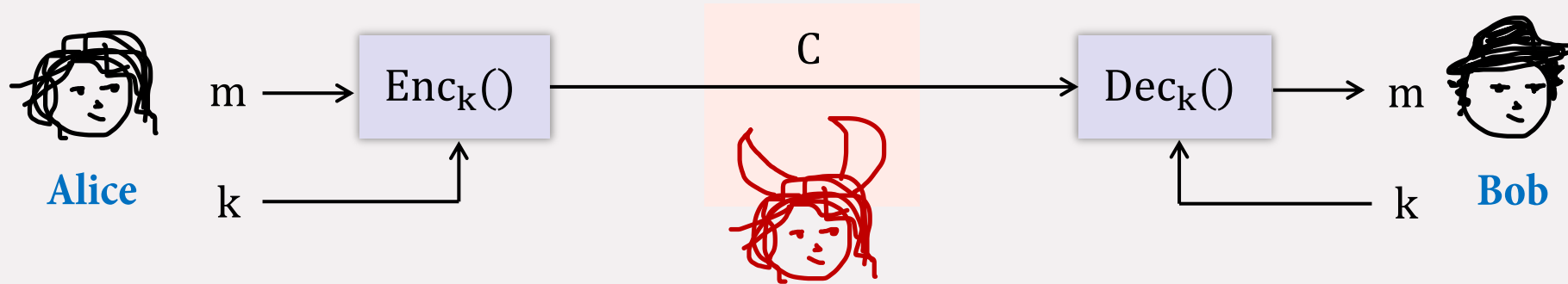


Chosen Plaintext Attacks (CPA)



Modes of Operation

Chosen Plaintext Attack (CPA)



RECALL Eve

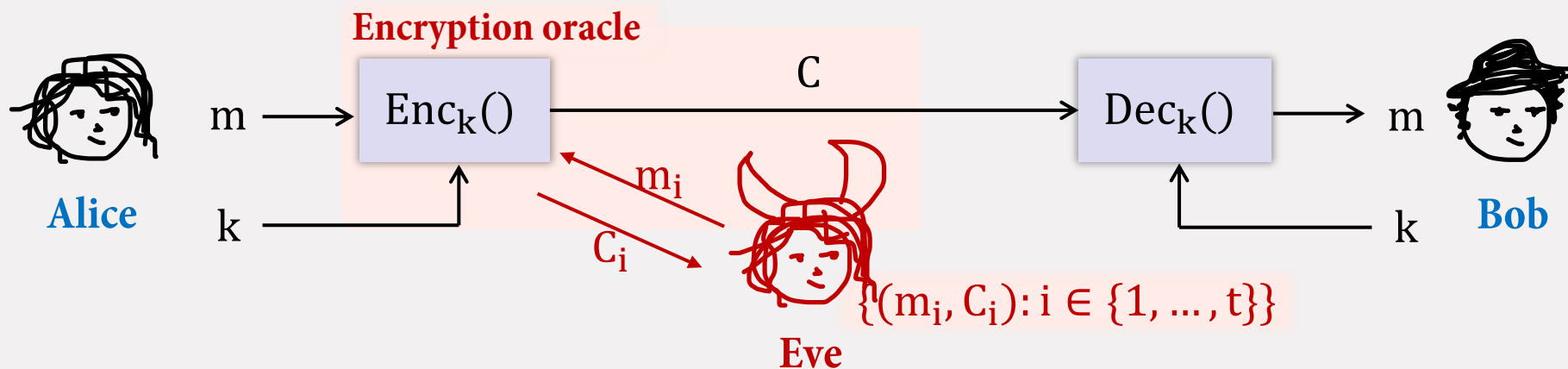
Ciphertext Only Attack (COA):

Eavesdropper

PPT

Will refer to the computational indistinguishability definition we saw in [[Lec 3, Def 7](#)] as security against Ciphertext Only Attack (COA)

Chosen Plaintext Attack (CPA)

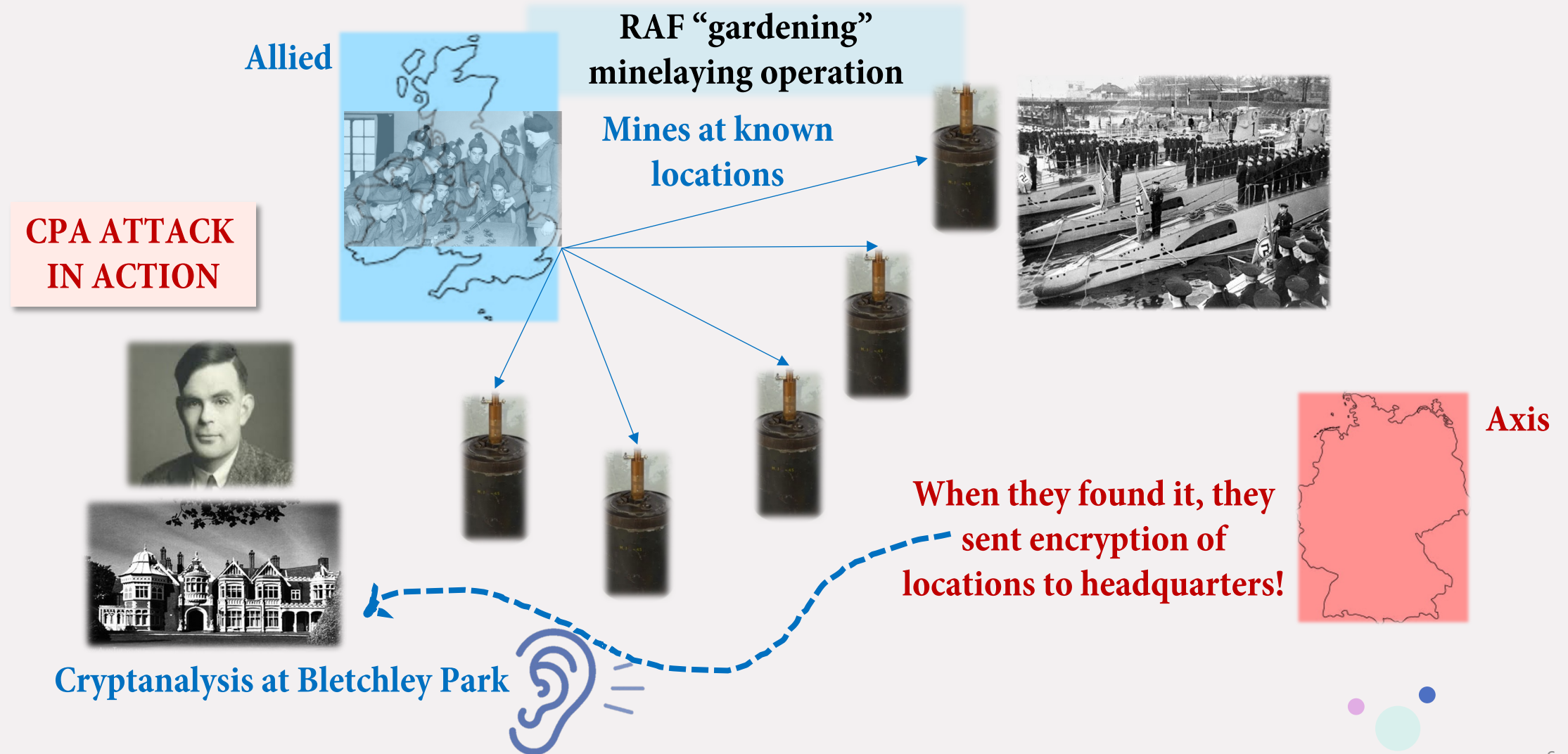


Chosen Plaintext Attack (CPA):

~~Eavesdropper~~ **Eavesdropper with encryption oracle**
PPT

- Eve influences Alice to encrypt messages of her choice (on the same key).
- Eve's goal is then to gain more information about message under a new ciphertext!

CPA shortened WWII by 2-3 years!



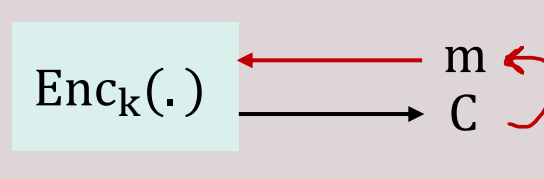
Security against CPA



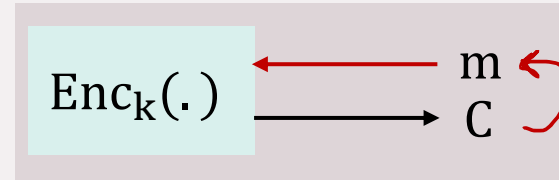
$k \leftarrow \text{Gen}(1^n)$

 $b \in_R \{0,1\}$

$\Pi = (\text{Gen}, \text{Enc}, \text{Dec}), \mathcal{M}$



$m_0 \neq m_1 \in \mathcal{M}$
 $|m_0| = |m_1|$
 $c_b \leftarrow \text{Enc}_k(m_b)$



$b' \in \{0,1\}$
Guess which one encrypted



**Can include
 queried messages!**

Eve wins if output is 1

$\text{PrivK}_{\text{Eve}, \Pi}^{\text{cpa}}$ outputs 1, if $b' = b$
 and 0, o.w.

Definition 3

Π is **CPA secure** if, for all **PPT** adversary **Eve**, there exists a negligible function **negl** such that, $\forall n$

$$\Pr[\text{PrivK}_{\text{Eve}, \Pi}^{\text{cpa}}(n) = 1] \leq 1/2 + \text{negl}(n)$$

Security against CPA



Challenger

$k \leftarrow \text{Gen}(1^n)$

 $b \in_R \{0,1\}$

$\Pi = (\text{Gen}, \text{Enc}, \text{Dec}), \mathcal{M}$

$\text{Enc}_k(\cdot)$ $\xleftarrow{\quad} m$
 $\xrightarrow{\quad} c$

$m_0 \neq m_1 \in \mathcal{M}$
 $|m_0| = |m_1|$

$c_b \leftarrow \text{Enc}_k(m_b)$

$\text{Enc}_k(\cdot)$ $\xleftarrow{\quad} m$
 $\xrightarrow{\quad} c$

$b' \in \{0,1\}$

Guess which one encrypted



PPT

Eve

**Can include
queried messages!**

Eve wins if output is 1

$\text{PrivK}_{\text{Eve}, \Pi}^{\text{cpa}}$ outputs 1, if $b' = b$
and 0, o.w.



Can we have a CPA secure encryption scheme with deterministic encryption?

Can we have indistinguishability for multiple messages (what we were trying to build last class) for a (stateless) encryption scheme with deterministic encryption?

Security against CPA



Challenger

$k \leftarrow \text{Gen}(1^n)$

 $b \in_R \{0,1\}$

$\Pi = (\text{Gen}, \text{Enc}, \text{Dec}), \mathcal{M}$

$\text{Enc}_k(\cdot)$ $\xleftarrow{\text{red}} m$ $\xrightarrow{\text{black}} c$

$m_0 \neq m_1 \in \mathcal{M}$
 $|m_0| = |m_1|$

$c_b \leftarrow \text{Enc}_k(m_b)$

$\text{Enc}_k(\cdot)$ $\xleftarrow{\text{red}} m$ $\xrightarrow{\text{black}} c$

$b' \in \{0,1\}$

Guess which one encrypted



PPT

Eve

**Can include
queried messages!**

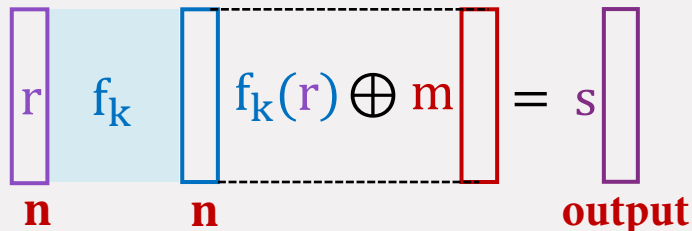
Eve wins if output is 1

$\text{PrivK}_{\text{Eve}, \Pi}^{\text{cpa}}$ outputs 1, if $b' = b$
and 0, o.w.

Takeaway: For the reasonable stronger notions of encryption security allowing reuse of keys for multiple messages, randomized encryption is necessary!

A CPA Secure Scheme (from last class)

$\mathcal{K} = \{0,1\}^n, \mathcal{M} = \{0,1\}^n, \mathcal{C} = \{0,1\}^n$

Building Block	Let $\mathcal{F} = \{f_k: \{0,1\}^n \rightarrow \{0,1\}^n\}_{k \in \{0,1\}^n}$ be a PRF.	
Gen(1^n): - Pick $k \in_R \{0,1\}^n$ Output k	Enc(k, m): - Pick $r \in_R \{0,1\}^n$  Output $c = (r, s)$	Dec($k, c = (r, s)$): Output $m = f_k(r) \oplus s$

Theorem 1

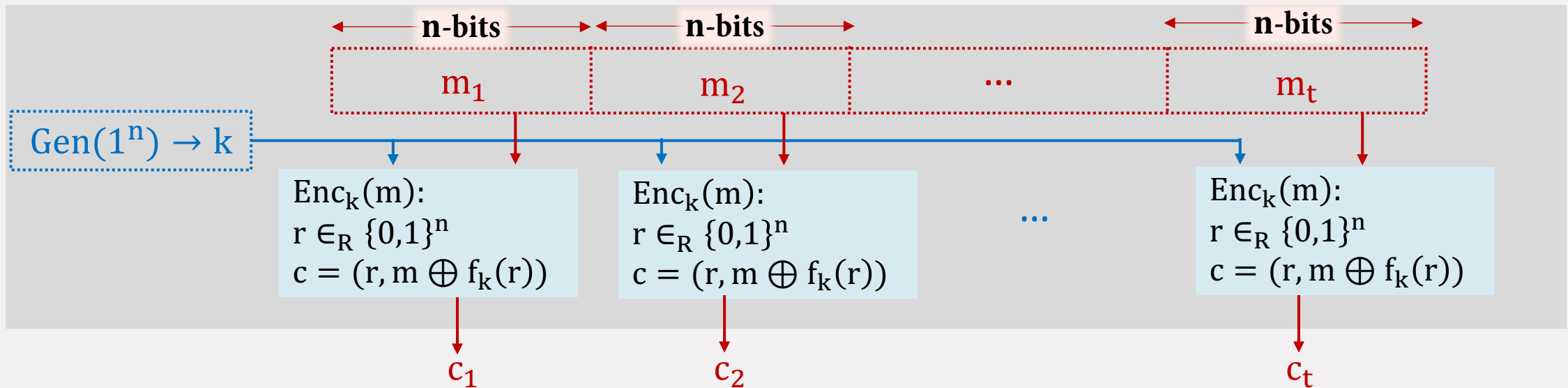
Construction 1

If $\mathcal{F}$ is a pseudorandom function, then **Construction 1** is a CPA secure symmetric key encryption for n -bit messages.

HW 2: Prove this via a security reduction!
[Katz and Lindell third edition, Theorem 3.29]

CPA for Arbitrary Length Messages (Theoretical Construction)

$\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$, $\mathcal{M} = \{0, 1\}^n$ be a CPA-secure encryption for n -bit messages.



Construction 2

HW 3: If Π is CPA secure for n -bit messages then **Construction 2** is CPA secure for tn -bit messages.

[Katz and Lindell third edition, Theorem 3.23]

How good is this?

Message blocks: **t**; Size of each message: **n-bits**

	<u>Theoretical Construction</u>				
Randomness used					
Ciphertext size					
Ciphertext computation parallelizable?					
Randomness reusable?					
Minimal Assumption need					
CPA secure?					

How good is this?

Message blocks: **t**; Size of each message: **n-bits**

	<u>Theoretical Construction</u>				
Randomness used	tn-bits				
Ciphertext size	2tn-bits				
Ciphertext computation parallelizable?	Yes				
Randomness reusable?	No				
Minimal Assumption need	PRF				
CPA secure?	Yes				

How good is this?

Message blocks: **t**; Size of each message: **n-bits**

	<u>Theoretical Construction</u>				Ideal Goal
Randomness used	tn-bits				n-bits
Ciphertext size	2tn-bits				tn + n-bits
Ciphertext computation parallelizable?	Yes				Yes
Randomness reusable?	No				Yes
Minimal Assumption need	PRF				PRF
CPA secure?	Yes				Yes

Today



Chosen Plaintext Attacks (CPA)



Modes of Operation

Block-cipher Modes of Operations

- **Given:** A length preserving block cipher F (a PRF (or “**PRP**”)) with block length n



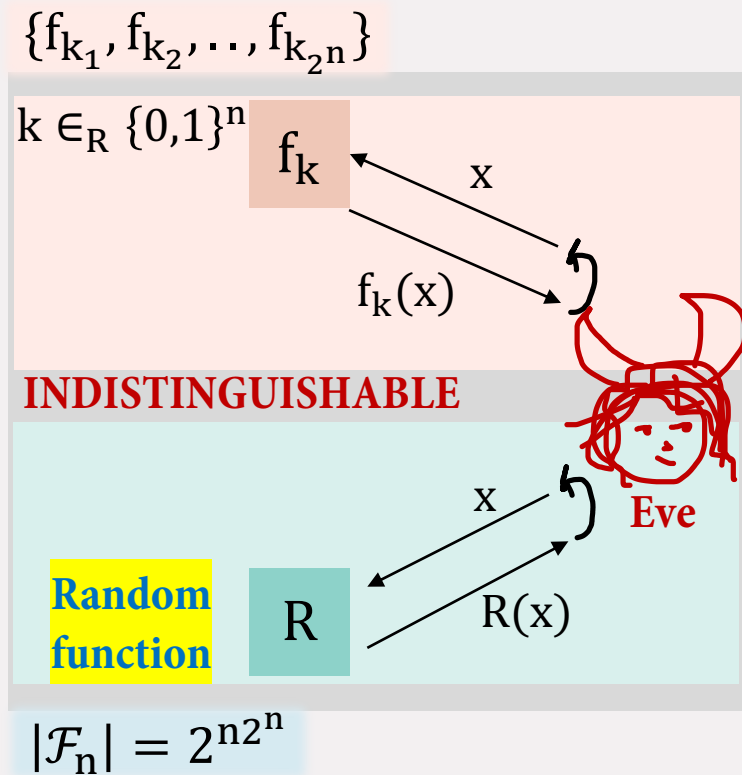
Stronger
variants of PRF

- **Goal:** To encrypt $m = m_1 m_2 \dots m_t$ using F with ciphertext length as small as possible and with randomness as less as possible.

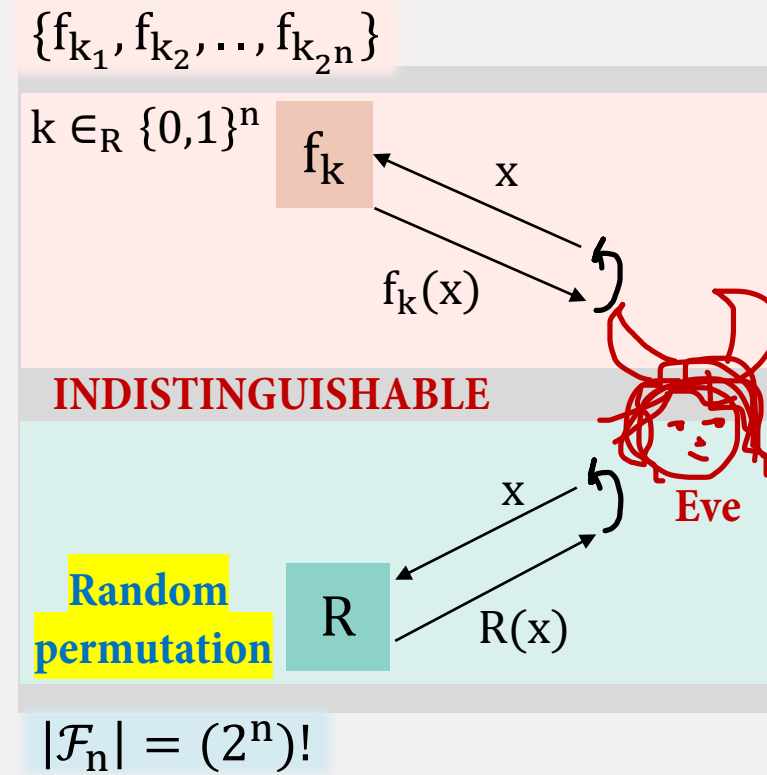


What will you do if messages are not multiple of n -bits long?

PRF vs PRP

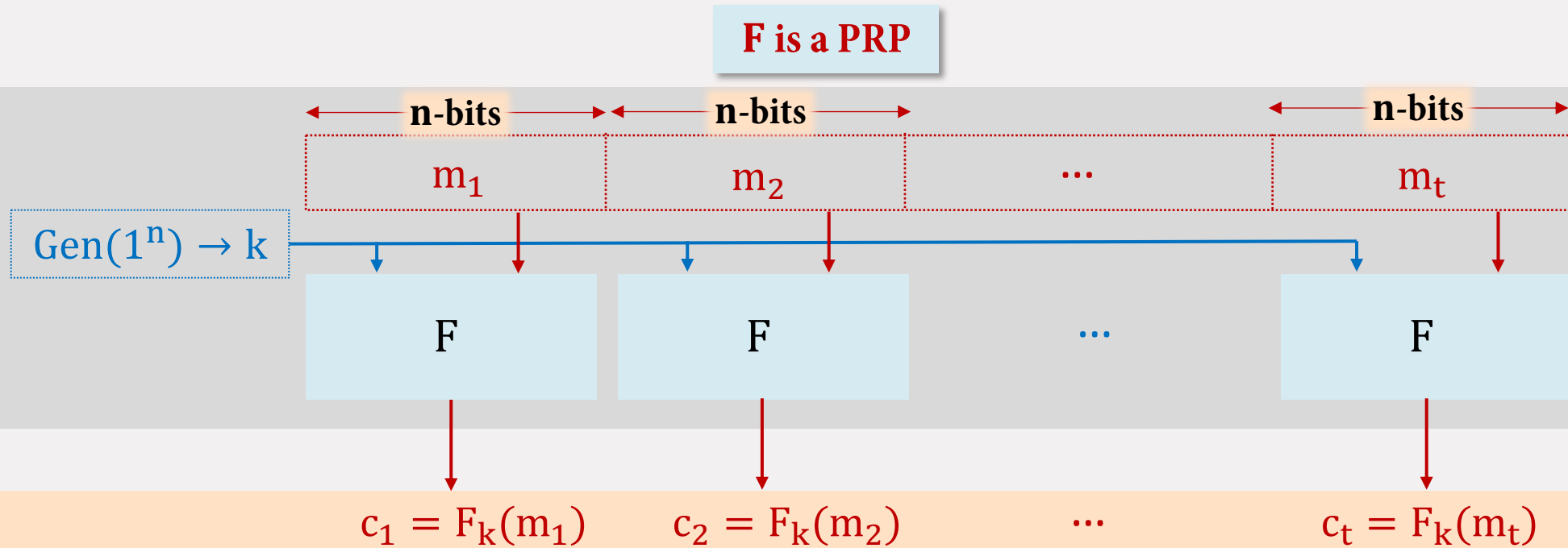


Pseudorandom Function
PRF



Pseudorandom Permutation
PRP

Electronic Code Book (ECB) Mode



- No randomness used!
- $|c| = |m|$
- **Decryption:** compute $F_k^{-1}(c_i) = m_i \forall i$
- It assumes that **F is a PRP**
- Parallelizable? Yes!

CPA SECURITY?



NOT EVEN COA SECURE!

Visible Insecurity of ECB

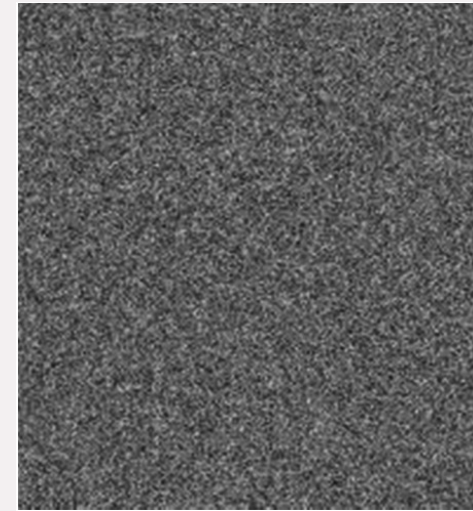
Encrypting an image using ECB, you see the insecurity clearly!



Plain Tux



ECB-encrypted Tux



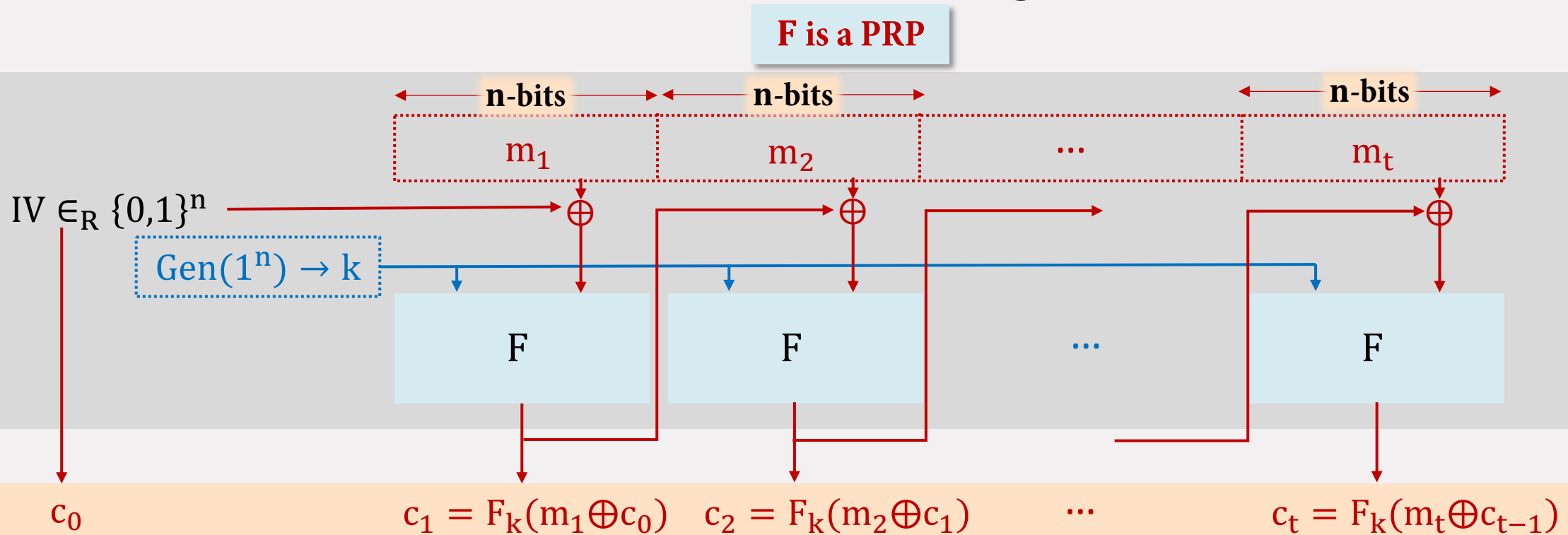
Securely encrypted

Comparison

Message blocks: **t**; Size of each message: **n-bits**

	<u>Theoretical Construction</u>	<u>ECB</u>			Ideal Goal
Randomness used	tn-bits	0-bits			n-bits
Ciphertext size	2tn-bits	tn-bits			tn + n-bits
Ciphertext computation parallelizable?	Yes	Yes			Yes
Randomness reusable?	No	-			Yes
Minimal Assumption need	PRF	PRP			PRF
CPA secure?	Yes	No			Yes

Cipher Block Chaining (CBC) Mode



- $|c| = |m| + n$
- **Decryption:** $m_i = F_k^{-1}(c_i) \oplus c_{i-1} \forall i$
- It assumes that **F is an PRP**
- Parallelizable? NO!

CPA SECURITY?

HW 4 (optional):

Prove it is CPA secure if F is a PRP!

ECB vs CBC Tux

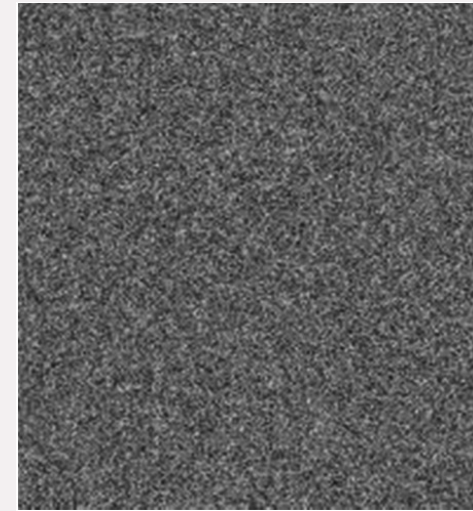
Encrypting an image using ECB, you see the insecurity clearly!



Plain Tux



ECB-encrypted Tux



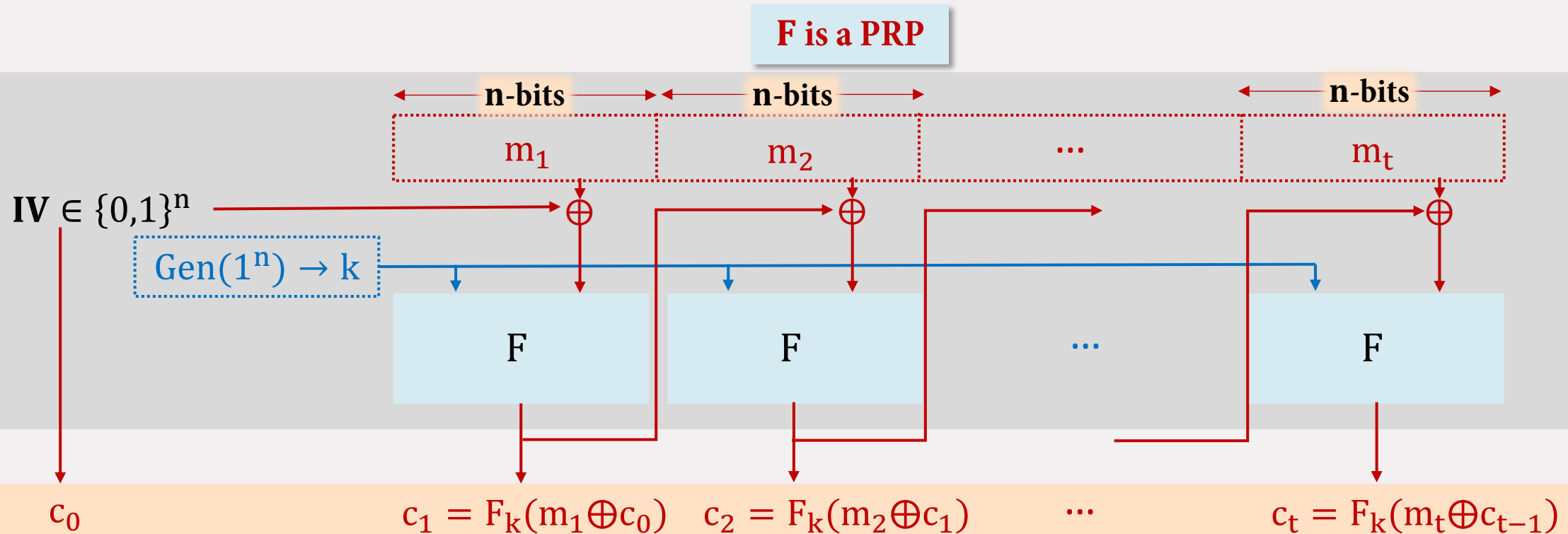
CBC-encrypted Tux

Comparison

Message blocks: **t**; Size of each message: **n-bits**

	<u>Theoretical Construction</u>	<u>ECB</u>	<u>CBC</u>		Ideal Goal
Randomness used	tn-bits	0-bits	n-bits		n-bits
Ciphertext size	2tn-bits	tn-bits	tn + n-bits		tn + n-bits
Ciphertext computation parallelizable?	Yes	Yes	No		Yes
Randomness reusable?	No	-	-		Yes
Minimal Assumption need	PRF	PRP	PRP		PRF
CPA secure?	Yes	No	Yes		Yes

IV misuse in CBC

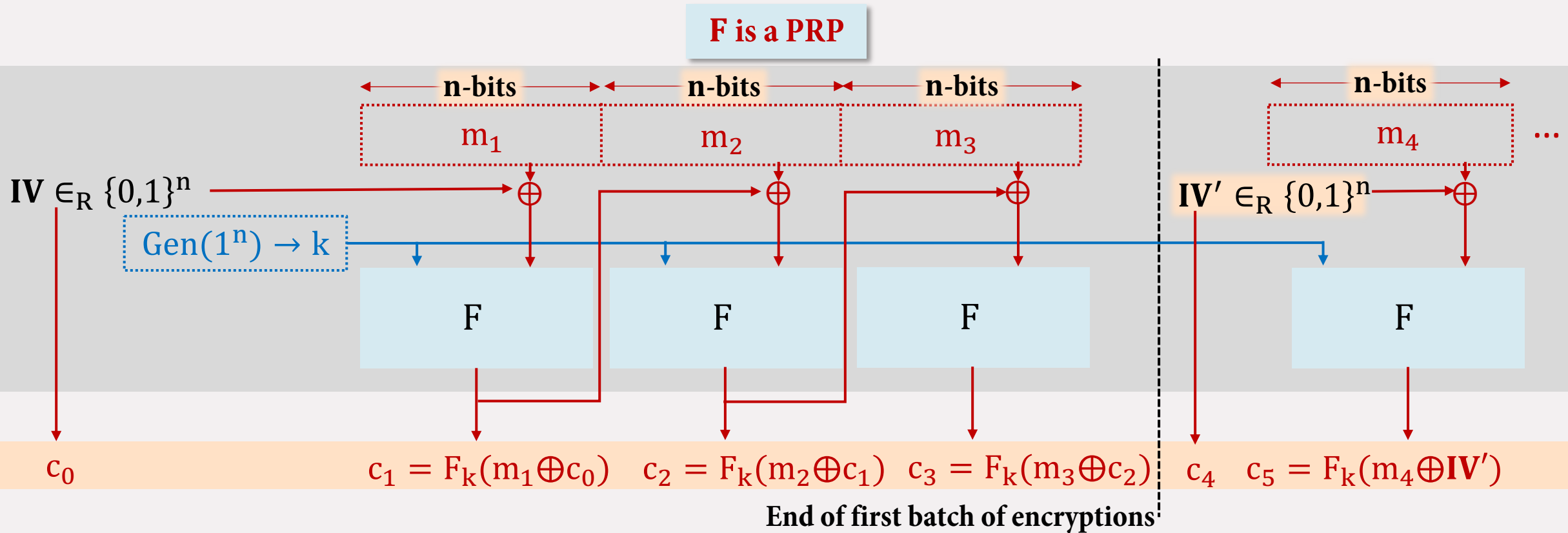


Is choosing a distinct (but not random) **IV** enough (each time a batch of message comes)?

NO!

HW 5: Show that this is insecure!

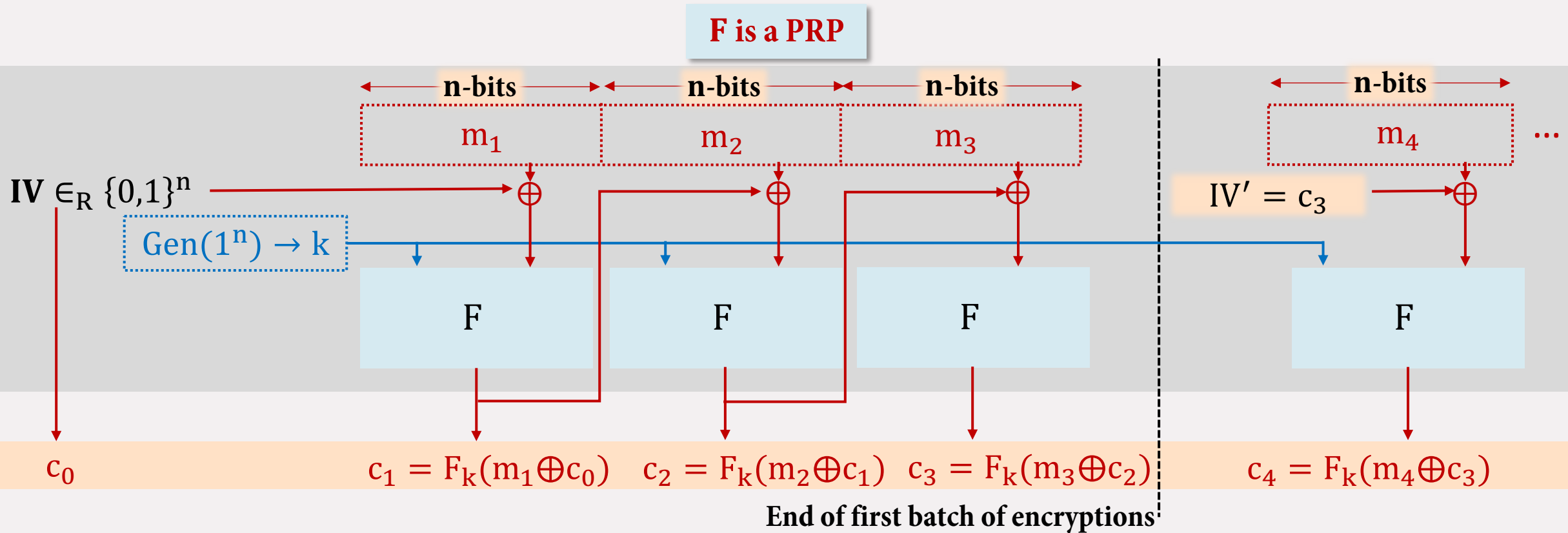
IV misuse in CBC



Stateless CBC Mode

If you had no state information of where you stopped?

IV misuse in CBC

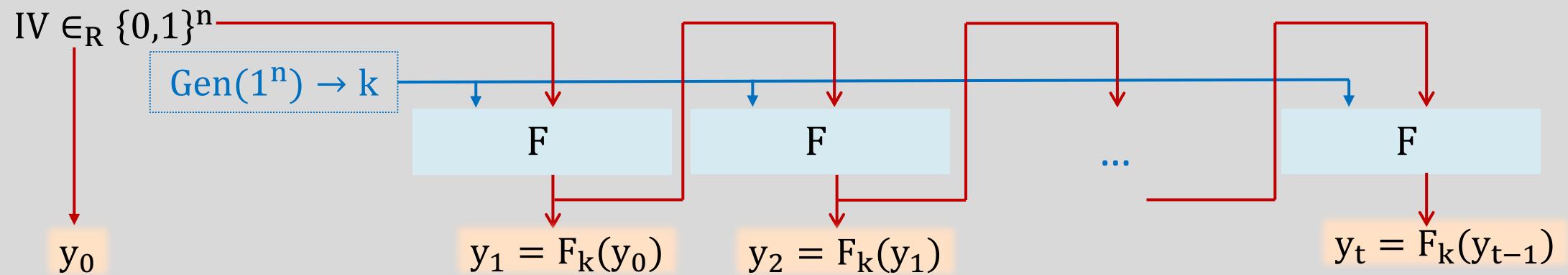


Chained CBC mode –used in SSL 3.0 and TLS 1.0 (stateful variant of CBC)

Can the last ciphertext of previous block be used as IV for the next encryption?
(saves bandwidth and randomness)

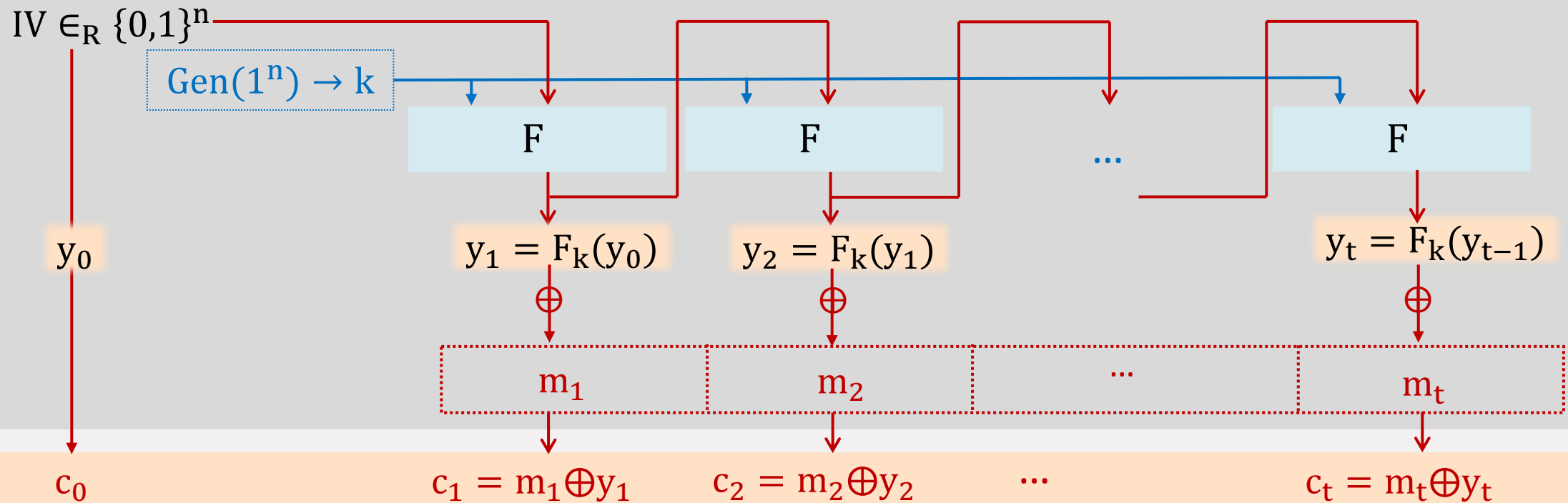
CPA Attack?
No!

Output Feedback (OFB) Mode



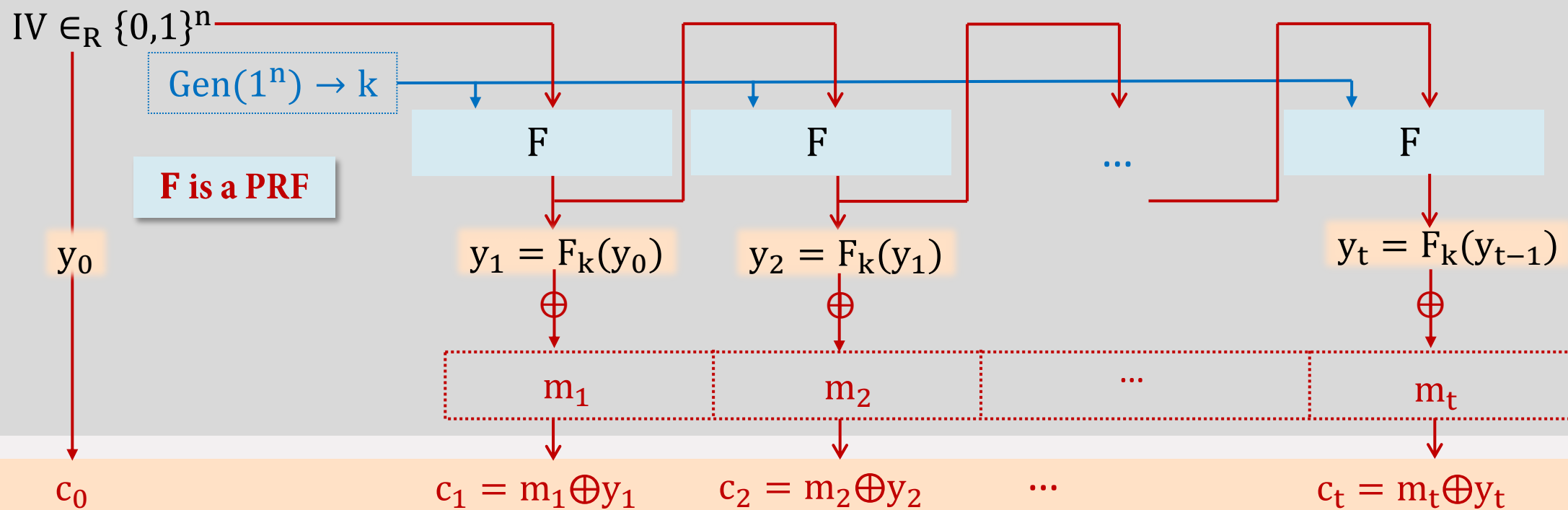
- Generate a pseudorandom stream of pad (independent of message).

Output Feedback (OFB) Mode



- Generate a pseudorandom stream of pads (independent of message).
- Use the pseudorandom stream to mask the message!

Output Feedback (OFB) Mode



- $|c| = |m| + n$
- **Decryption:** $m_i = F_k(y_{i-1}) \oplus c_i \forall i$
- Assuming **F** is a PRF is enough!
- Parallelizable? NO, but is precomputable!

CPA SECURITY?

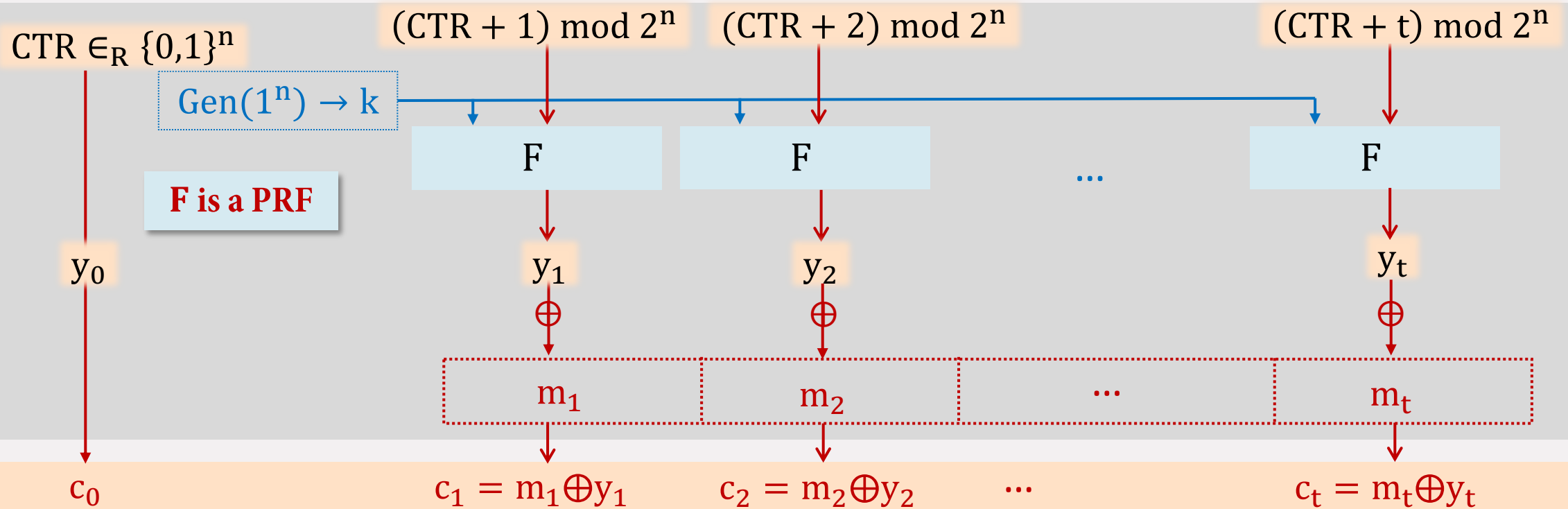
✓ Stateful/chained

Comparison

Message blocks: **t**; Size of each message: **n-bits**

	<u>Theoretical Construction</u>	<u>ECB</u>	<u>CBC</u>	<u>OFB</u>	<u>Ideal Goal</u>
Randomness used	tn-bits	0-bits	n-bits	n-bits	n-bits
Ciphertext size	2tn-bits	tn-bits	tn + n-bits	tn + n-bits	tn + n-bits
Ciphertext computation parallelizable?	Yes	Yes	No	No (but pre-computable)	Yes
Randomness reusable?	No	-	-	Yes	Yes
Minimal Assumption need	PRF	PRP	PRP	PRF	PRF
CPA secure?	Yes	No	Yes	Yes	Yes

Counter (CTR) Mode



- It is the same as OFB in structure: pseudorandom stream first, then mask the message.
- But now, parallelizable!
- **PRF enough again!**
- Can decrypt ciphertext block by just invoking F once!

CPA SECURITY?  **Stateful/chained**

Comparison

Message blocks: **t**; Size of each message: **n-bits**

	<u>Theoretical Construction</u>	<u>ECB</u>	<u>CBC</u>	<u>OFB</u>	<u>CTR</u>
Randomness used	tn-bits	0-bits	n-bits	n-bits	n-bits
Ciphertext size	2tn-bits	tn-bits	tn + n-bits	tn + n-bits	tn + n-bits
Ciphertext computation parallelizable?	Yes	Yes	No	No (but pre-computable)	Yes
Randomness reusable?	No	-	-	Yes	Yes
Minimal Assumption need	PRF	PRP	PRP	PRF	PRF
CPA secure?	Yes	No	Yes	Yes	Yes

Practical Issues

1. Block Length and Concrete Security

- If F supports block length of n -bits, then $IV \in_R \{0,1\}^n$
- **After $2^{n/2}$ encryptions, IV will repeat with constant probability!**
- If n too short, then impractical security!



Example: DES with $n = 64 \Rightarrow$ repetition after $2^{32} \approx 4,300,000,000$ encryptions!
(approx 34 GB of plaintexts —not too large)

What happens when IV is repeated in each mode?

- In **CTR** and **OFB**, same pseudorandom string generated –security lost!
- In **CBC mode**, effect is not that serious –Why?

To avoid this, either use CBC or stateful OFB/CTR (stateful means you don't pick random IV each time as you know where you stopped via the state info, hence you can continue using strings generated via same IV without the risk of reusing a particular output of the PRF!)

Practical Issues

2. Message Transmission Errors (non-adversarial)

- Dropped packets, changed bits, etc.
- Solved by some standard techniques: re-transmission or error correction

3. Adversarial Tampering

- What if Eve now is allowed to modify ciphertexts?
- Issue of message integrity/authentication!

NEXT WEEK



THANK YOU