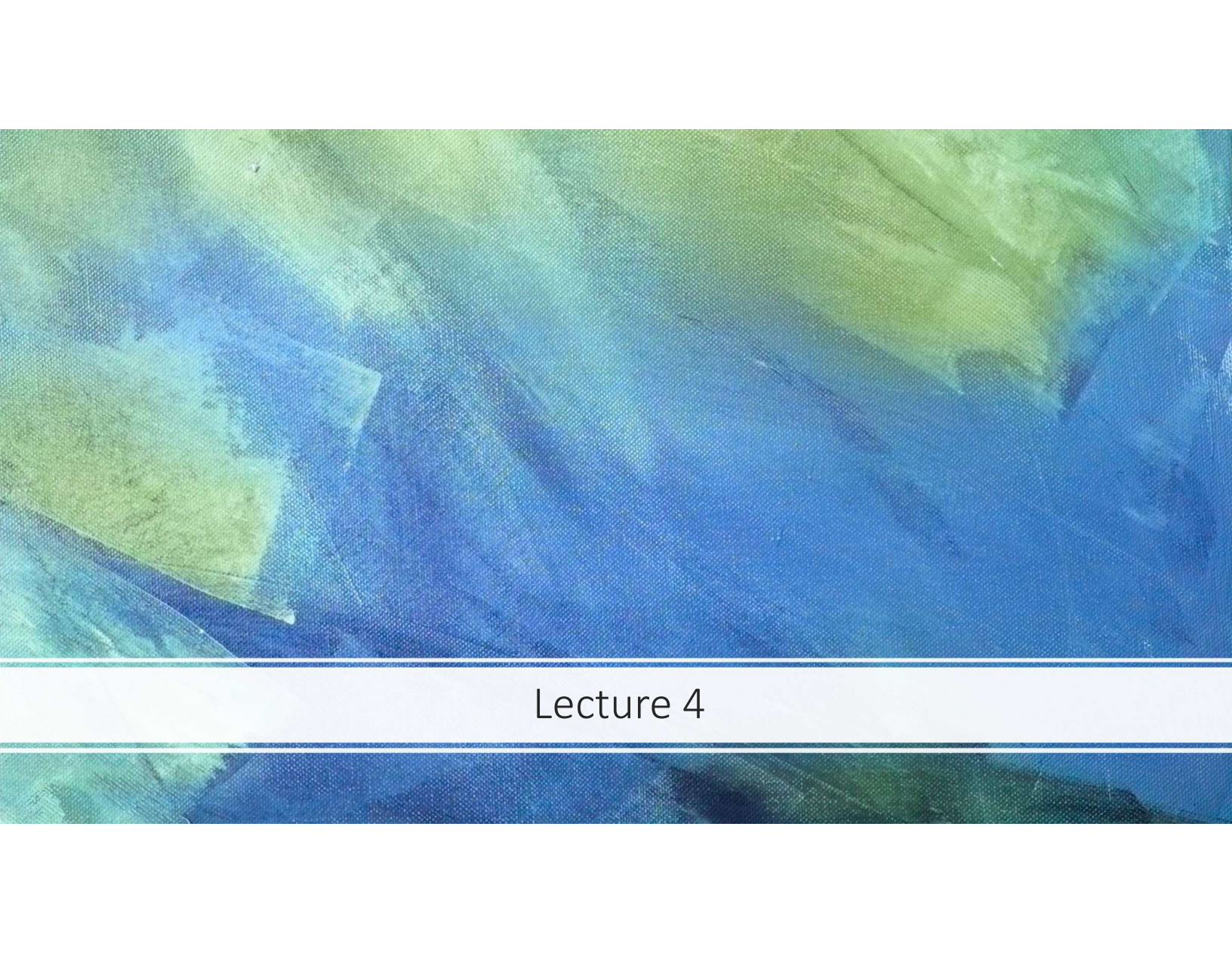


The background of the slide is an abstract composition of broad, textured brushstrokes in various shades of green and blue. The colors are layered and blended, creating a sense of depth and movement. A horizontal white band runs across the middle of the image, containing the text.

Lecture 4



Introduction



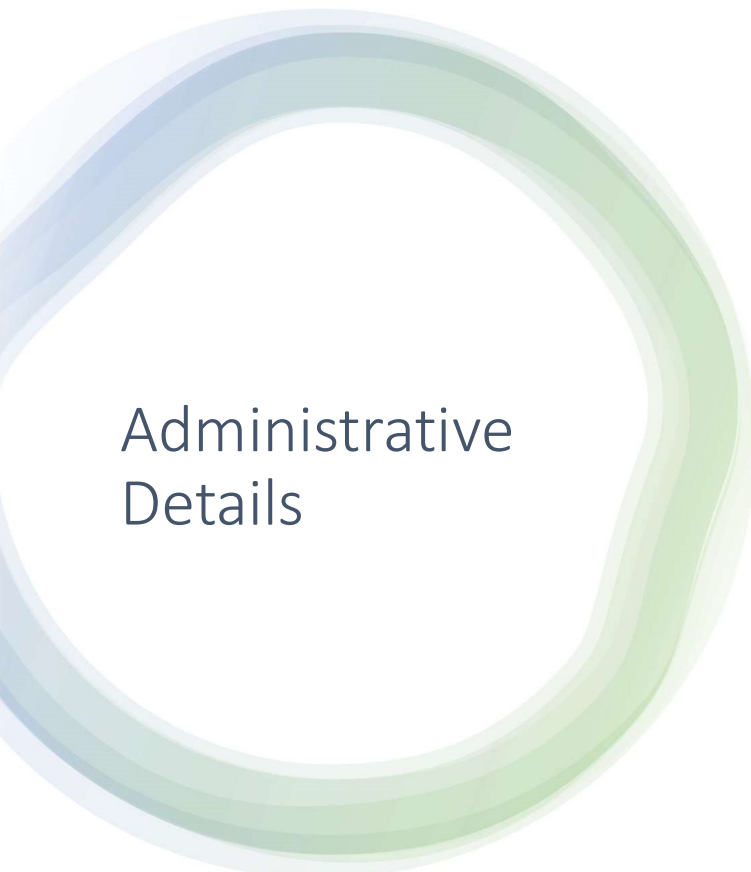
DES: Attacks



AES



Modes of
operation



Administrative Details

- Course website:
<https://courses.grainger.illinois.edu/cs498ac3/fa2020/>
- Has syllabus, instructor and TA info, office hours
- **IMPORTANT: Join Piazza!**
piazza.com/illinois/fall2020/ececs498ac/home

I strongly encourage class participation.
If you don't understand something in class, please interrupt me and ask questions.
Please make abundant use of office hours.

Recall:

- PRG **Pseudo Random Generator**
 $\{0,1\}^k \rightarrow \{0,1\}^{2k}$. $\text{PRG}(K) \stackrel{K \leftarrow \{0,1\}^k}{\sim_c} \text{uniform}_{2k}$
- PRF **PseudoRandom Function** $\rightarrow$ Game₀
 $\{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^m$
 $\begin{array}{c} x_0 \rightarrow \\ \text{PRF}(K, x_0) \\ \leftarrow \end{array}$
 $\begin{array}{c} x_1 \rightarrow \\ \text{PRF}(K, x_1) \\ \leftarrow \end{array}$
 $\vdots$
- PRP **Pseudo Random Permutation** $\rightarrow$ Game₁
 $\text{PRF where } m=n,$
 $+ \text{ invertability (given key)}$
 $\begin{array}{c} x_0 \rightarrow \\ \text{random} \\ \leftarrow \end{array}$
 $\begin{array}{c} x_1 \rightarrow \\ \text{random} \\ \leftarrow \end{array}$
 $\vdots$
 $\begin{array}{c} x_p \rightarrow \\ \text{same random} \\ \leftarrow \text{as above} \end{array}$
 $\left. \begin{array}{l} x_i, x_j \text{ s.t.} \\ x_i = x_j \\ \text{return same} \\ \text{random value} \end{array} \right\}$

Last

Class : Can we build PRG from PRF?

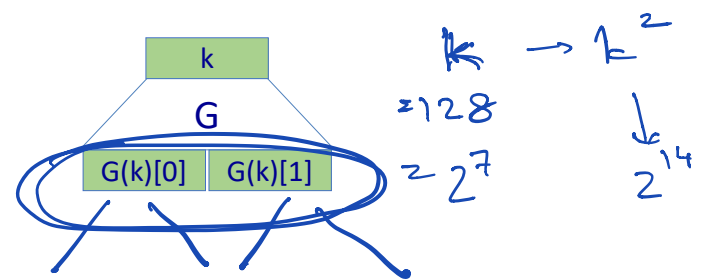
$$\text{PRG}(k) = \text{PRF}(k, 0) \parallel \text{PRF}(k, 1) \dots$$

Can we build a PRF from a PRG?

Let $G: K \rightarrow K^2$ be a secure PRG

Define 1-bit PRF $F: K \times \{0, 1\} \rightarrow K$ as

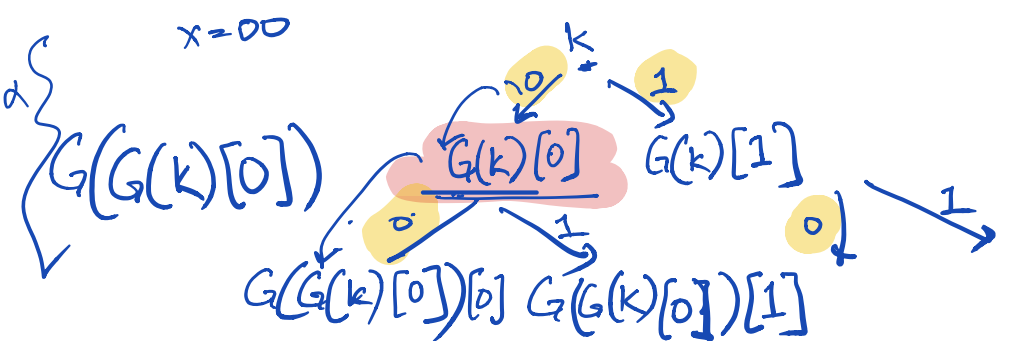
$$F(k, x \in \{0, 1\}) = G(k)[x]$$



Define $\text{PRF}(K, x) \rightarrow ?$

If $x \in \{0, 1\}$.

$\text{PRF}(K, 0) = \text{First half of PRG}(K)$
 $\text{PRF}(K, 1) = \text{Second half of PRG}(K)$



leaves. 2^x .



DES: Attacks

Exhaustive Key Search

$\rightarrow 2^{56}$

k

- For DES: given two pairs $(\underline{m_1}, \underline{c_1}), (\underline{m_2}, \underline{c_2})$ where $c_1 = E(k, m_1), c_2 = E(k, m_2)$
 -- w.h.p. there is at most *one* key k such that $E(k, m_1) = c_1$ and $E(k, m_2) = c_2$
 $\nexists k' \text{ s.t. } E(k', m_1) = c_1 \text{ \& } E(k', m_2) = c_2$
- **DES challenges:** Series of contests to highlight the lack of security of DES.
- $m =$ "The ^{m_1} unknown ^{m_2} message is: XXXX ...".
- CT =

c_1	c_2	c_3	c_4
-------	-------	-------	-------
- Challenge: Given CT, find XXXX
- First goal: Given c_1, c_2 , find common 56-bit key k .
 2^{nd} goal: Given k , Decrypt all other ct's.

Strengthening DES against Exhaustive Search

Method 1: **Triple-DES**

- Let $E : K \times M \rightarrow M$ be a block cipher
- Define $3E : K^3 \times M \rightarrow M$ as

$$3E((k_1, k_2, k_3), m) = E(k_1, D(k_2, E(k_3, m)))$$

For 3DES: key-size = $3 \times 56 = 168$ bits. 3×slower than DES.

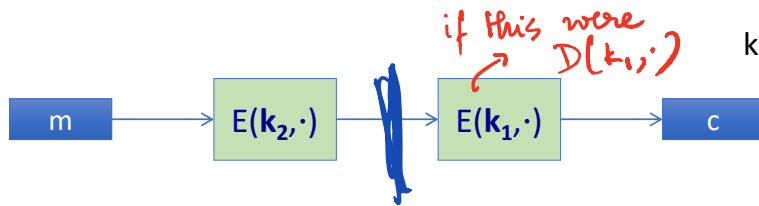
(can actually attack in time $\approx 2^{118}$)

PRG, PRF, PRP can be built from ONE-WAY FUNCTION. $f(x) \xrightarrow{\text{EASY}} y$ $f(y) \xrightarrow{\text{HARD}} x$.

All cryptography ASSUMES one-way FUNCTIONS.
 Prove that $P \neq NP$ $\uparrow$

What about 2DES? Meet-in-the-Middle

• Define $2E((k_1, k_2), m) = E(k_1, E(k_2, m))$



key-len = $56 \times 2 = 112$ bits

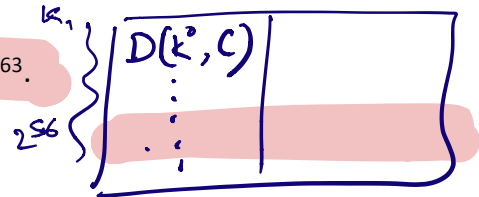
Ideally, ex. search should $\sim 2^{112}$

$2^{56} \log(2^{56})$

SORT
+ BIN. SEARCH

k_2	$k^0 = 00 \dots 00$	$E(k^0, M)$	} 2^{56} entries
	$k^1 = 00 \dots 01$	$E(k^1, M)$	
	$k^2 = 00 \dots 10$	$E(k^2, M)$	
	$\vdots$	$\vdots$	
	$k^N = 11 \dots 11$	$E(k^N, M)$	

Takes time 2^{63} .

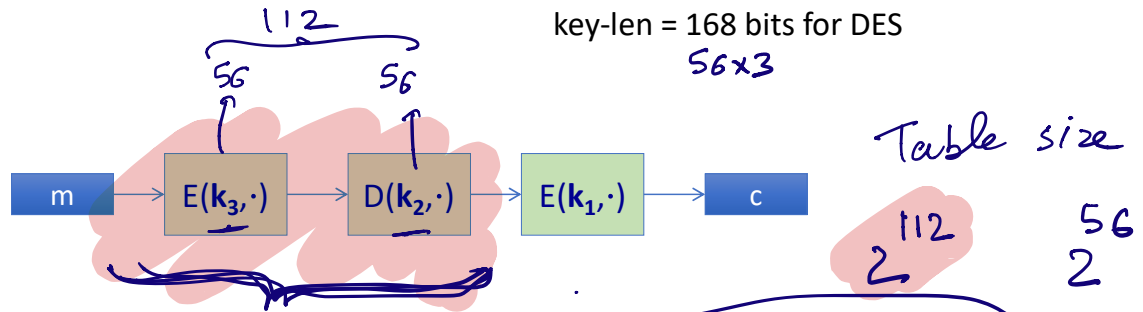


$\exists$ very few k_1, k_2 s.t. $D(k_1, c) = E(k_2, m)$
 This lets you find (k_1, k_2) .

cipher x
3x
4x

What about 3DES?

- Define $3E((k_1, k_2, k_3), m) = E(k_1, D(k_2, E(k_3, m)))$



- Same attack on 3DES in time 2^{118}

2^{63} on 2DES $\rightarrow 2^{56} \log(2^{56})$

Question: Time of attack on 4 DES?

SDDES: 2^{224} 2^{112}
 $2^{112} \log(2^{112})$

Alternative: DESX

$E : K \times \{0,1\}^n \rightarrow \{0,1\}^n$ a block cipher

Define EX as $EX((k_1, k_2, k_3), m) = \underline{k_1 \oplus E(k_2, m \oplus k_3)}$

For DESX: key-length = $64+56+64 = 184$ bits, but attack in time 2^{120}



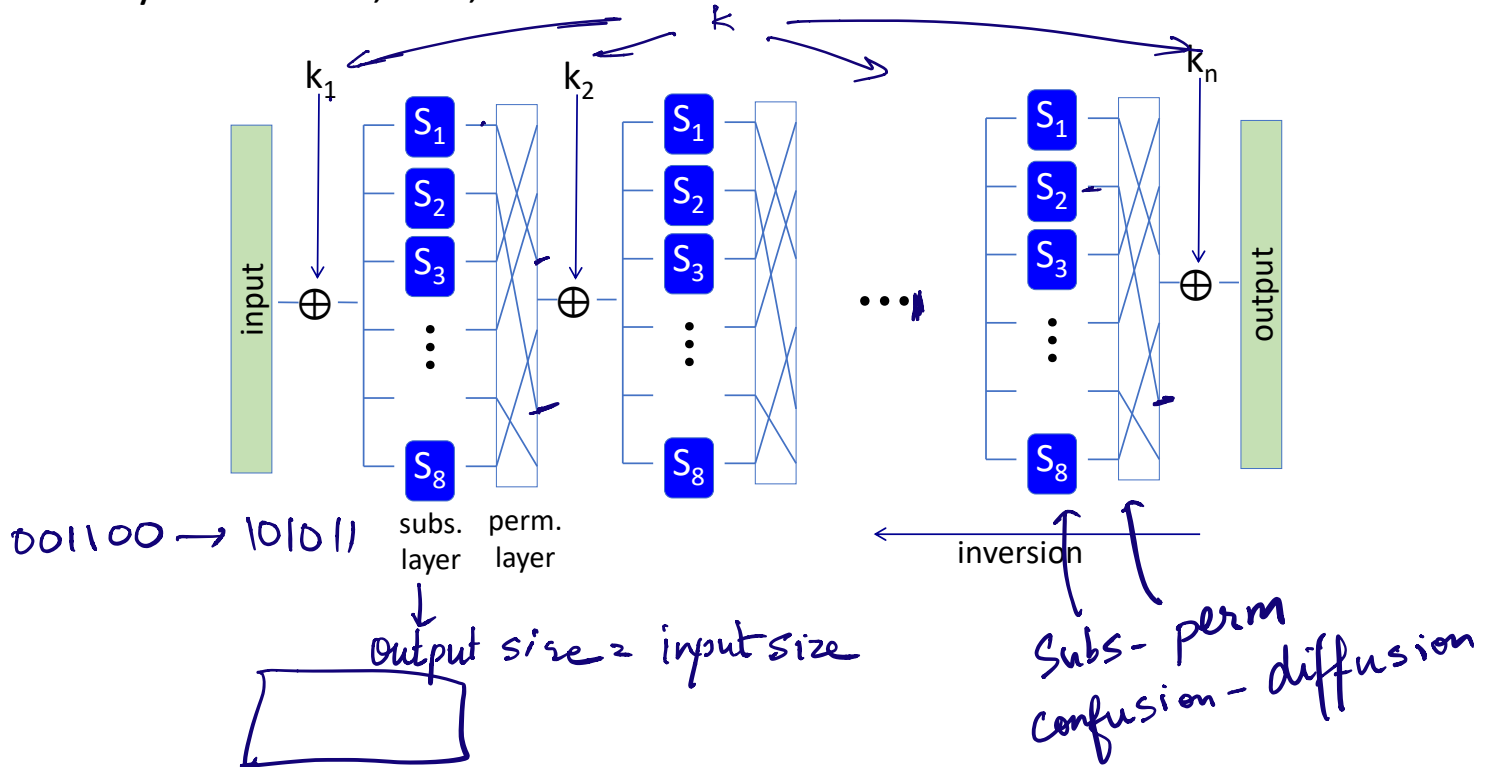
AES (Rjindael)

uninvertible f
↑ converted to
invertible F .

AES is not a Feistel. It is a Subs-Perm network.

Key sizes: 128, 192, 256 bits.

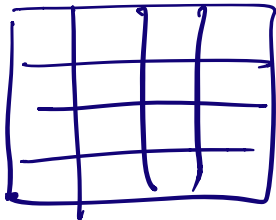
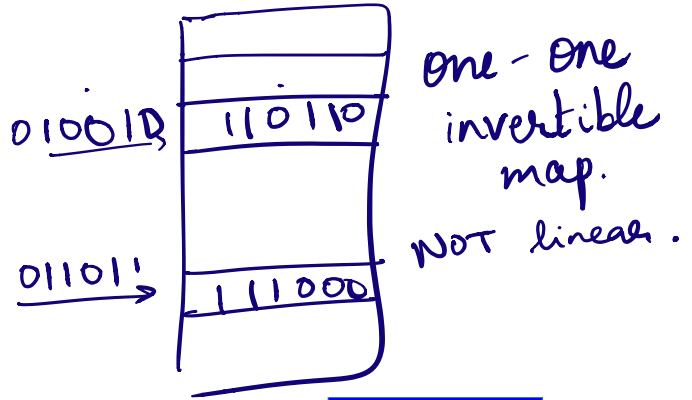
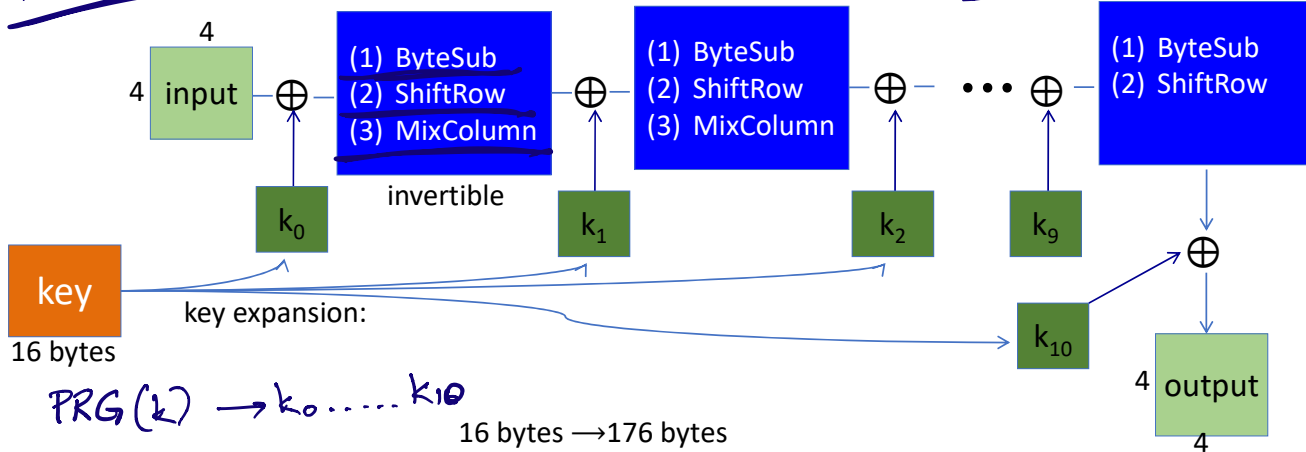
Block size: 128 bits



$$f(k, x) = \alpha k \oplus \beta x.$$

AES Structure

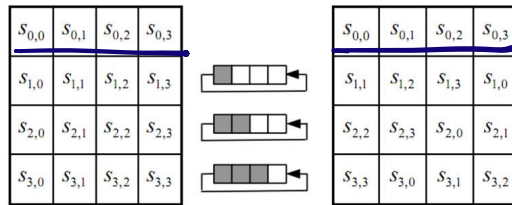
16-byte / 128-bit input



In Each Round

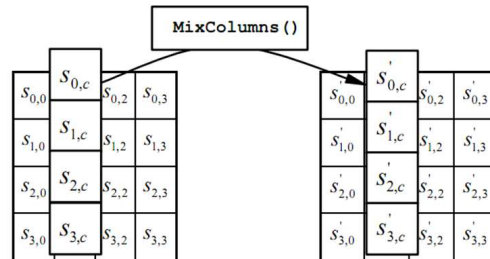
- **ByteSub:** a 1 byte S-box. 256 byte table (computable, so don't need to hardwire)

- **ShiftRows:**



left shift by 1
left shift by 2
" 3.

- **MixColumns:**



$$\begin{bmatrix} 1 & 1 & 2 & 3 \\ 1 & 2 & 3 & 1 \\ 2 & 3 & 1 & 1 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} s_{0c} \\ s_{1c} \\ s_{2c} \\ s_{3c} \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} s'_{0c} = s_{0c} + s_{1c} + 2s_{2c} + 3s_{3c} \\ s'_{1c} \\ s'_{2c} \\ s'_{3c} \end{bmatrix}$$

Block Ciphers are PRPs.

AES has key sizes 128, 192, 256.

↓
fastest,
least secure.

Attacks

Best key recovery attack:

Four times better than ex. search [BKR'11]

$$2^{126}$$

$$\underline{2^{122}}$$

Related key attack on AES-256: [BK'09]

Given 2^{99} input/output pairs from four related keys in AES-256

Can recover keys in time $\approx 2^{99}$

CPA - secure cipher.

$$\forall m_0, m_1, E(k, m_0) \approx E(k, m_1) \\ \in \{0,1\}^{128}$$



Modes of Operation for Block Ciphers

One-time Key

- Goal: build “secure” encryption from a secure PRP (e.g. AES)
- Recall: what is semantic (or CPA/chosen plaintext attack) security

$$\forall m_0, m_1 \in \{0,1\}^{128},$$

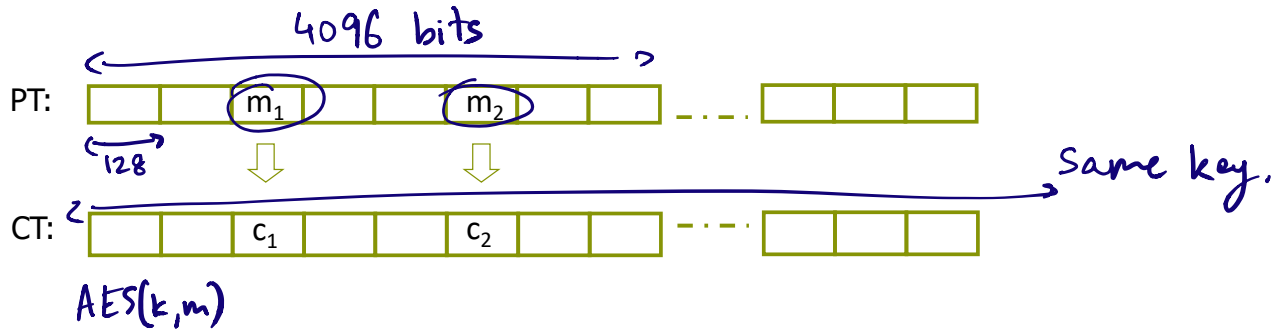
$$E_{k \leftarrow \mathcal{K}}(k, m_0) \approx E_{k \leftarrow \mathcal{K}}(k, m_1)$$

- ECB mode (electronic code book): $E(k, m)$

$$\text{AES}(k, m)$$

Incorrect Use of Block Ciphers

Electronic Code Book (ECB) should not be applied to multiple blocks



Problem:

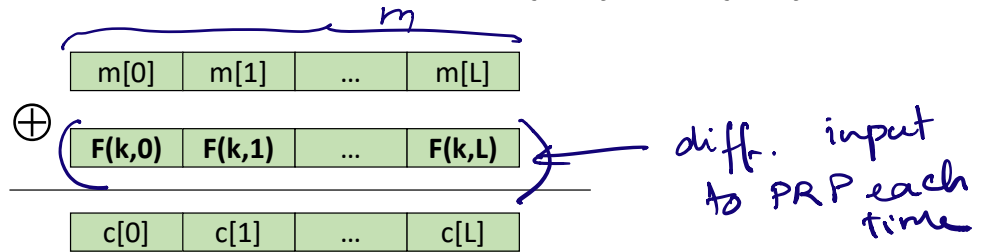
- if $m_1 = m_2$ then $c_1 = c_2$
- not semantically secure for messages that contain two blocks

Semantic = CPA

One-time key, but many blocks

Deterministic counter mode from a PRF $F : \mathcal{K} \times \{0,1\}^n \rightarrow \{0,1\}^n$ ($n = 128$)

• $E_{\text{DETCTR}}(k, m) =$



$\Rightarrow$ Stream cipher built from a PRF (e.g. AES, 3DES)

$$c[0] \oplus c'[0]$$

$$= m[0] \oplus m'[0]$$

$$\begin{array}{cc} m'[0] & m'[1] \\ F(k,0) & F(k,1) \\ \hline c'[0] \end{array}$$

One-time Keys

Theorem: For any $L > 0$,

If F is a secure PRF over $(\mathcal{K}, \mathcal{X}, \mathcal{X})$ then

E_{DECTR} is semantically secure cipher over $(\mathcal{K}, \mathcal{X}^L, \mathcal{X}^L)$

Single message

- example: encrypted email, new key for every message.

Many-time Keys

Example applications:

- 1. File systems: Same AES key used to encrypt many files.
- 2. Ipsec (used in VPN): Same AES key used to encrypt many packets.

Defining Security:

Many-time Keys

If secret key is to be used multiple times $\Rightarrow$
given the same plaintext message twice, encryption must produce different outputs.

Solutions?

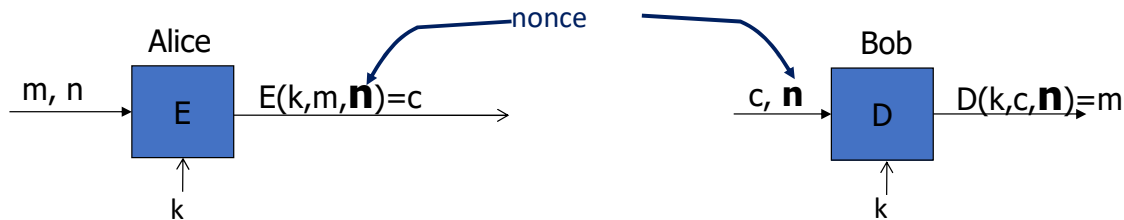
Many-time Keys

Let $F: K \times R \rightarrow M$ be a secure PRF.

For $m \in M$ define $E(k, m) = [r \leftarrow R, \text{ output } (r, F(k, r) \oplus m)]$

Is E semantically secure under CPA?

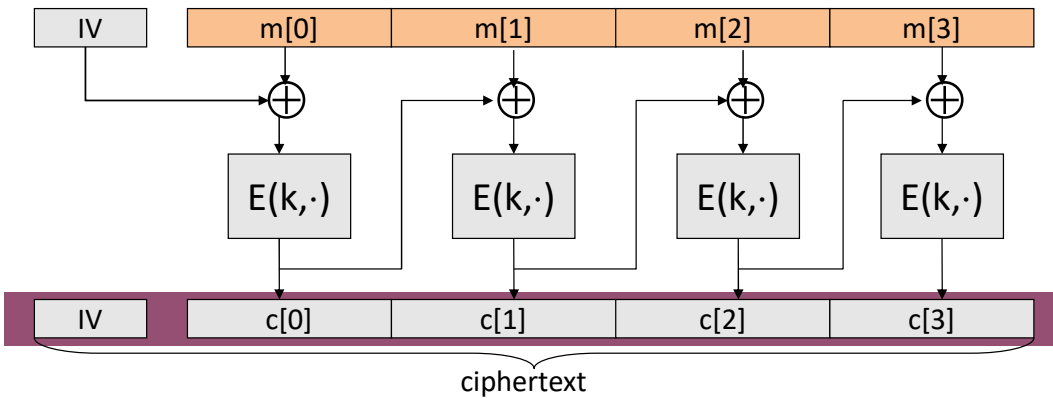
Solution 2: nonce-based Encryption



- nonce n : a value that changes from msg to msg.
(k,n) pair never used more than once
- method 1: nonce is a **counter** (e.g. packet counter) [SSL, IPsec]
 - used when encryptor keeps state from msg to msg
 - if decryptor has same state, need not send nonce with CT
- method 2: nonce is **random** [File Encryption]

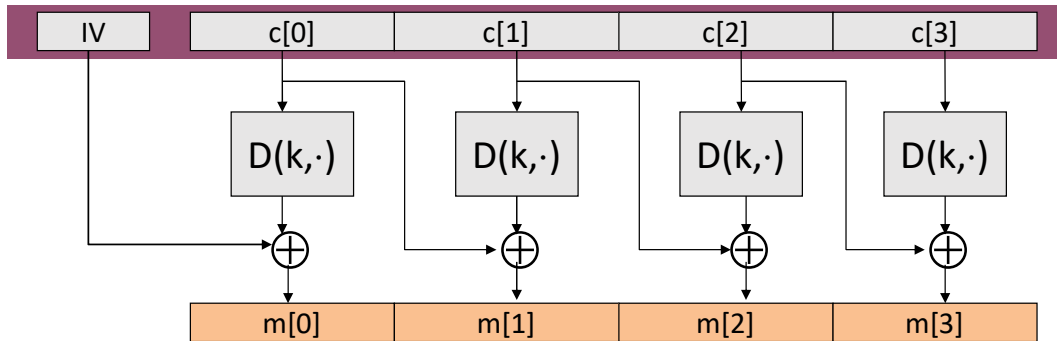
CBC (Cipher Block Chaining) mode

Let (E,D) be a PRP. $E_{\text{CBC}}(k,m)$: choose **random** Initialization Vector and do:



Decryption Circuit

In symbols: $c[0] = E(k, IV \oplus m[0]) \Rightarrow m[0] = D(k, c[0]) \oplus IV$



CPA Security of CBC

- CBC Theorem: For small enough $L > 0$,
If E is a secure PRP over (K, X) then
 E_{CBC} is CPA-secure over (K, X^L, X^{L+1}) .
- In particular, security error in CBC = $(2 \times \text{sec. error in PRP}) + (q^2 L^2 / |X|)$
- What if IV was predictable? Is it still CPA-secure?

Bug in SSL/TLS 1.0: IV for record # i is last CT block of record # $(i-1)$

What happens if adversary can predict IV

Insecure!

$k \leftarrow K$

IV_1

Adv

$\xleftarrow{0}$

$c_1 \leftarrow (IV_1, E(k, 0 \oplus IV_1))$

$\xrightarrow{\quad}$
 $m_0 = m_1 \neq m_0$
 $\xleftarrow{IV_1 \oplus IV_2}$

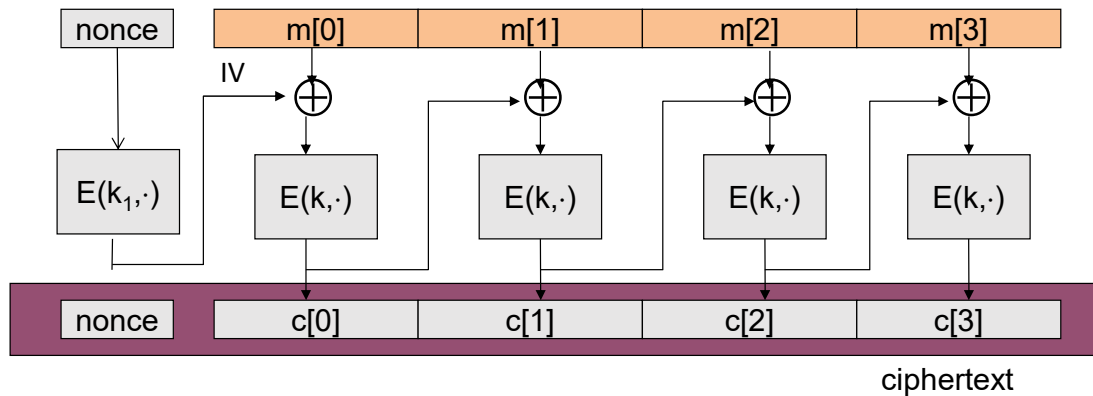
Suppose Adv predicts IV_2

IV_2

If $m_0 = 0$
 $c_2 \leftarrow (IV_2, ?)$
Else $c_2 \leftarrow ?$

CBC (Cipher Block Chaining) mode: Version 2

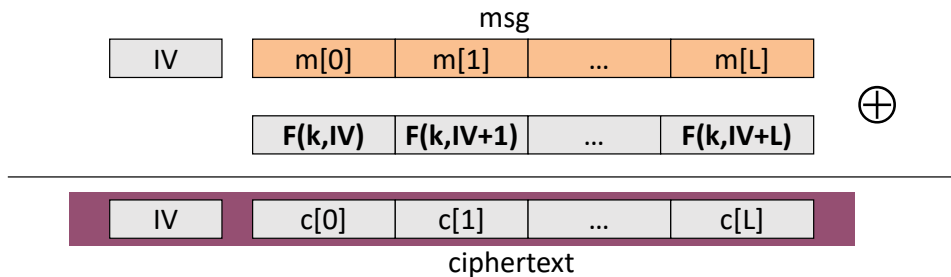
- Cipher block chaining with unique nonce: $\text{key} = (k, k_1)$
unique nonce means: (key, n) pair is used for only one message



Rand-ctr mode

Let $F: K \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a secure *PRF*.

$E(k,m)$: choose a random $IV \in \{0,1\}^n$ and do:



(1) Can use PRF instead of PRP and (2) is parallelizable.

Summary

- DES: some attacks and strengthenings
- AES: substitution-permutation network
- Modes of operation of block-ciphers