# Foundations of Applied Cryptography

Adam O'Neill

Based on http://cseweb.ucsd.edu/~mihir/cse207/

# Setting the Stage

- We have studied our first lower-level primitive, blockciphers.

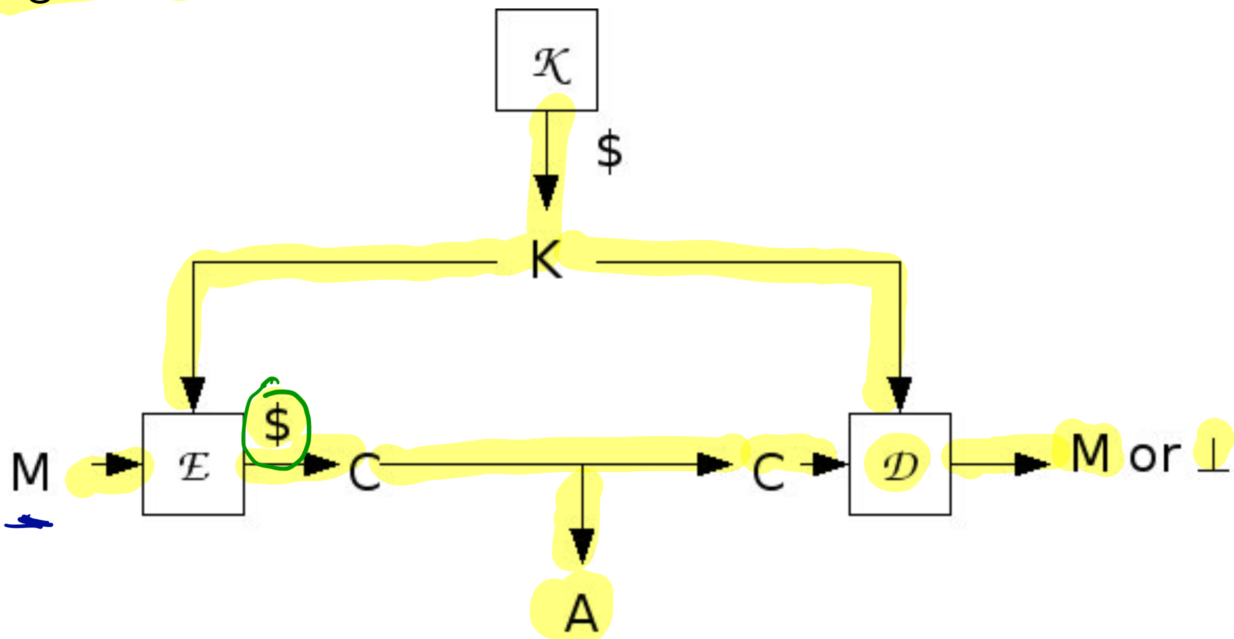
# Setting the Stage

- We have studied our first lower-level primitive, blockciphers.
- Today we will study how to use it to build our first higher-level primitive, symmetric-key encryption.

# Syntax

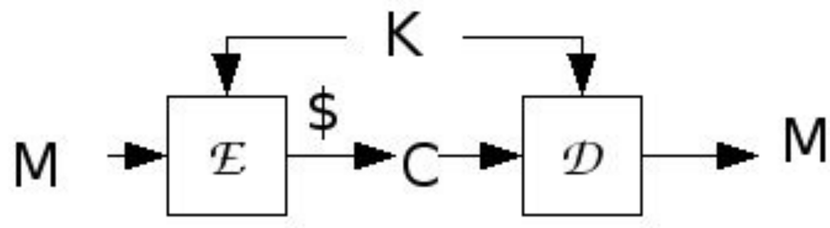
w/ msg sp $\mathcal{M}$

A symmetric encryption scheme $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ consists of three algorithms:




$\mathcal{K}$ and $\mathcal{E}$ may be randomized, but $\mathcal{D}$ must be deterministic.

# Correctness




**More formally:** For all keys $K$ that may be output by $\mathcal{K}$, and for all $M$ in the *message space*, we have

$$Pr[\mathcal{D}_K(\mathcal{E}_K(M)) = M] = 1 ,$$

where the probability is over the coins of $\mathcal{E}$.

A scheme will usually specify an associated message space.

# Blockcipher Modes of Operation

$E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ a block cipher

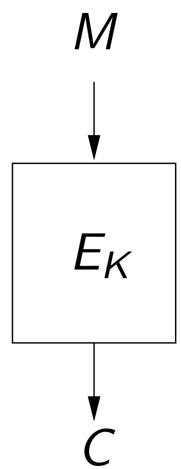
Notation: $x[i]$ is the i-th n-bit block of a string x, so that $x = x[1] \ldots x[m]$ if $|x| = nm$.

Always:

Alg $\mathcal{K}$
$K \xleftarrow{\$} \{0,1\}^k$
return K

# Modes of operation

Block cipher provides parties sharing $K$ with




which enables them to encrypt a 1-block message.

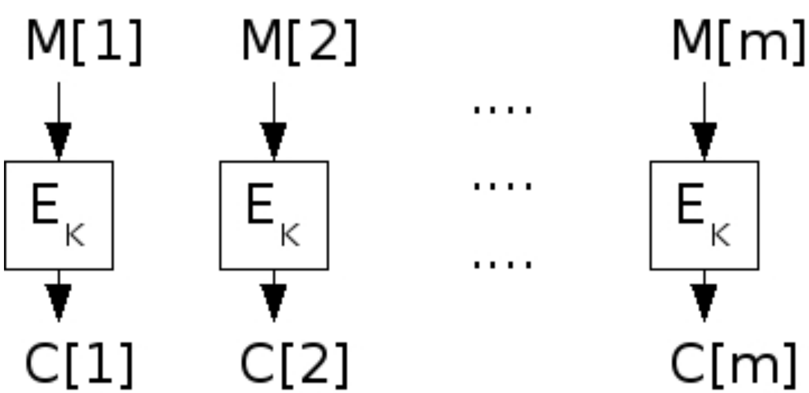
How do we encrypt a long message using a primitive that only applies to n-bit blocks?

# Electronic Codebook Mode

(ECB)

$\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ where:

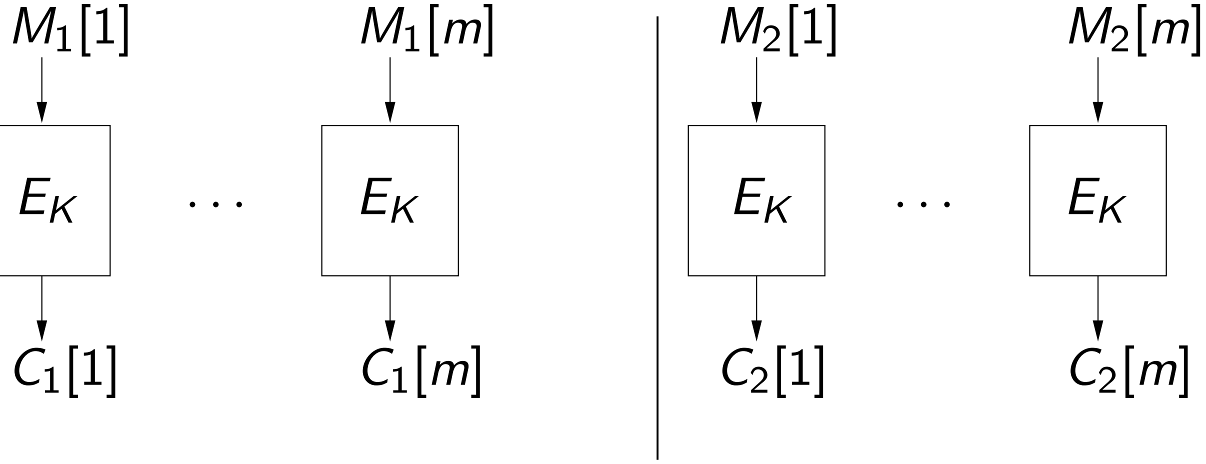
| **Alg** $\mathcal{E}_K(M)$ | **Alg** $\mathcal{D}_K(C)$ |
|---|---|
| for $i = 1, \ldots, m$ do | for $i = 1, \ldots, m$ do |
| $\quad C[i] \leftarrow E_K(M[i])$ | $\quad M[i] \leftarrow E_K^{-1}(C[i])$ |
| return C | return M |



# Weakness of ECB

Weakness: $M_1 = M_2 \Rightarrow C_1 = C_2$

Why is the above true? Because $E_K$ is deterministic:



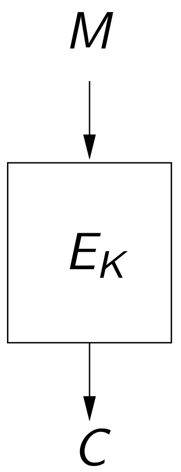

Why does this matter?

# Weakness of ECB

Suppose we know that there are only two possible messages, $Y = 1^n$ and $N = 0^n$, for example representing

- FIRE or DON'T FIRE a missile
- BUY or SELL a stock
- Vote YES or NO

Then ECB algorithm will be $\mathcal{E}_K(M) = E_K(M)$.



# Is this avoidable?

Let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be ANY encryption scheme.

Suppose $M_1, M_2 \in \{Y, N\}$ and

- Sender sends ciphertexts $C_1 \leftarrow \mathcal{E}_K(M_1)$ and $C_2 \leftarrow \mathcal{E}_K(M_2)$
- Adversary $A$ knows that $M_1 = Y$

Adversary says: If $C_2 = C_1$ then $M_2$ must be Y else it must be N.

Does this attack work?

# Introducing Randomized Encryption

For encryption to be secure it must be randomized

That is, algorithm $\mathcal{E}_K$ flips coins.

If the same message is encrypted twice, we are likely to get back different answers. That is, if $M_1 = M_2$ and we let

$$C_1 \xleftarrow{\$} \mathcal{E}_K(M_1) \text{ and } C_2 \xleftarrow{\$} \mathcal{E}_K(M_2)$$

then

$$Pr[C_1 = C_2]$$

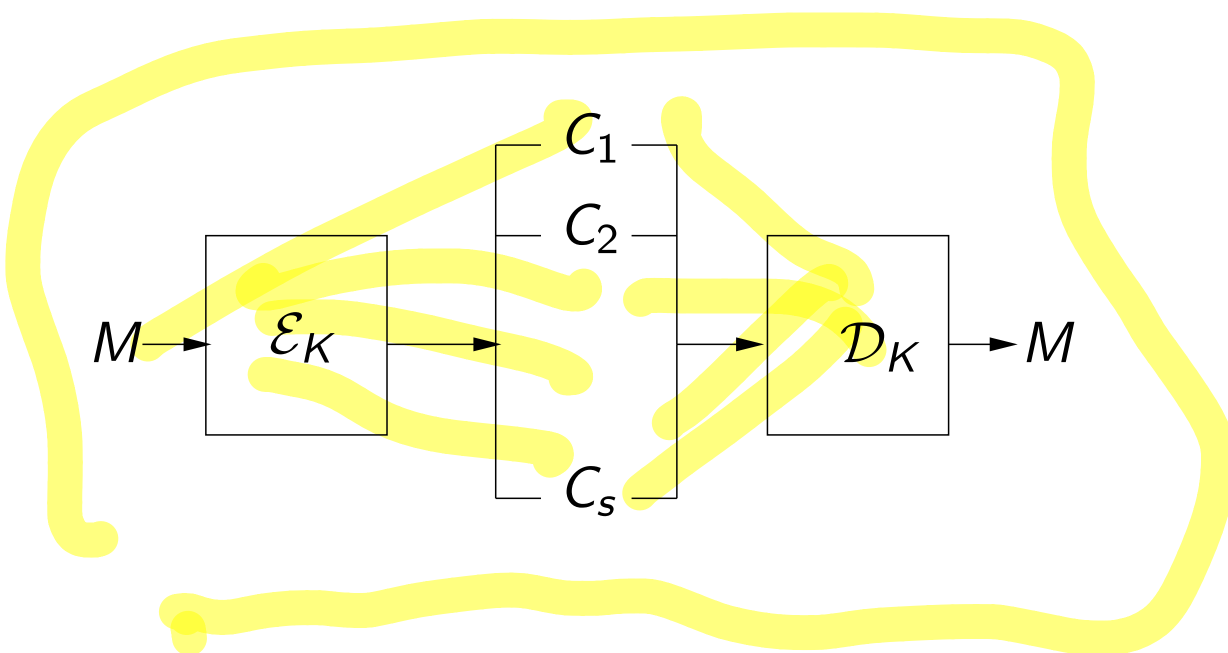
will (should) be small, where the probability is over the coins of $\mathcal{E}$.

# Randomized Encryption

There are many possible ciphertexts corresponding to each message.

If so, how can we decrypt?

We will see examples soon.



# Randomized Encryption

A fundamental departure from classical and conventional notions of encryption.

Clasically, encryption (e.g., substitution cipher) is a code, associating to each message a unique ciphertext.

Now, we are saying no such code is secure, and we look to encryption mechanisms which associate to each message a number of different possible ciphertexts.

# CBC-\$:
# Cipher-block Chaining Mode with Random IV

$\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ where:

**Alg** $\mathcal{E}_K(M)$

$C[0] \xleftarrow{\$} \{0,1\}^n$

for $i = 1, \ldots, m$ do

  $C[i] \leftarrow E_K(M[i] \oplus C[i-1])$

return $C$

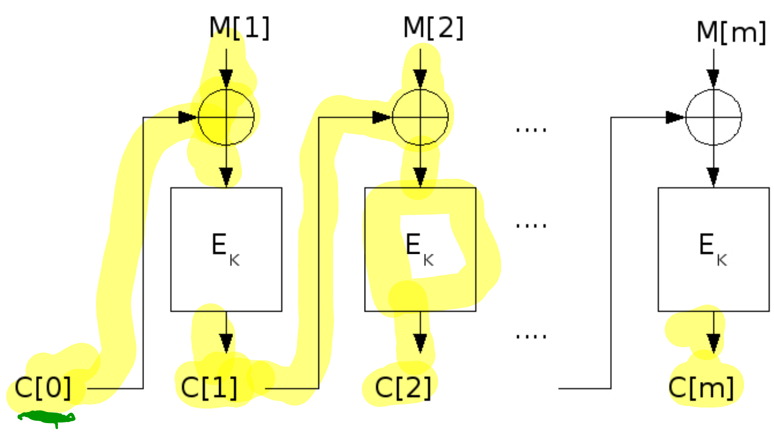
initialization vector (IV)

**Alg** $\mathcal{D}_K(C)$

for $i = 1, \ldots, m$ do

  $M[i] \leftarrow E_K^{-1}(C[i]) \oplus C[i-1]$

return $M$




Correct decryption relies on $E$ being a block cipher.

# CTR-\$ Mode

Let $E$: $\{0,1\}^k \times \{0,1\}^n \to \{0,1\}^\ell$ be a family of functions. If $X \in \{0,1\}^n$ and $i \in \mathbf{N}$ then $X + i$ denotes the $n$-bit string formed by converting $X$ to an integer, adding $i$ modulo $2^n$, and converting the result back to an $n$-bit string. Below the message is a sequence of $\ell$-bit blocks:

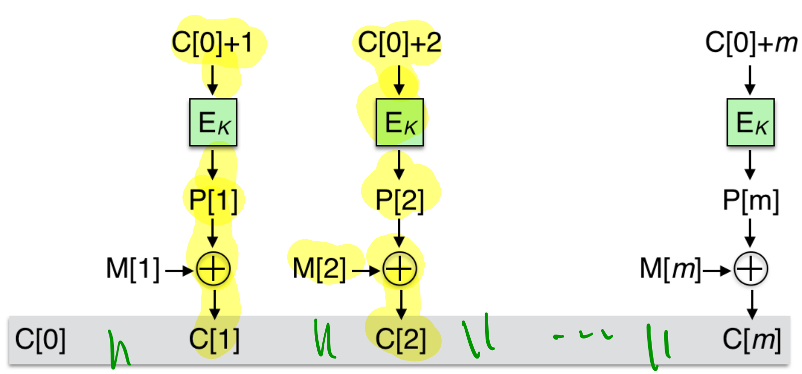
**Alg** $\mathcal{E}_K(M)$

$C[0] \xleftarrow{\$} \{0,1\}^n$
for $i = 1, \ldots, m$ do
  $P[i] \leftarrow E_K(C[0] + i)$
  $C[i] \leftarrow P[i] \oplus M[i]$
return $C$

**Alg** $\mathcal{D}_K(C)$

for $i = 1, \ldots, m$ do
  $P[i] \leftarrow E_K(C[0] + i)$
  $M[i] \leftarrow P[i] \oplus C[i]$
return $M$

C[0]=0




P[1] || ... || P[m]

pseudo OTP

# CTR-$ Mode

**Alg** $\mathcal{E}_K(M)$

$C[0] \xleftarrow{\$} \{0,1\}^n$
for $i = 1, \ldots, m$ do
  $P[i] \leftarrow E_K(C[0] + i)$
  $C[i] \leftarrow P[i] \oplus M[i]$
return $C$

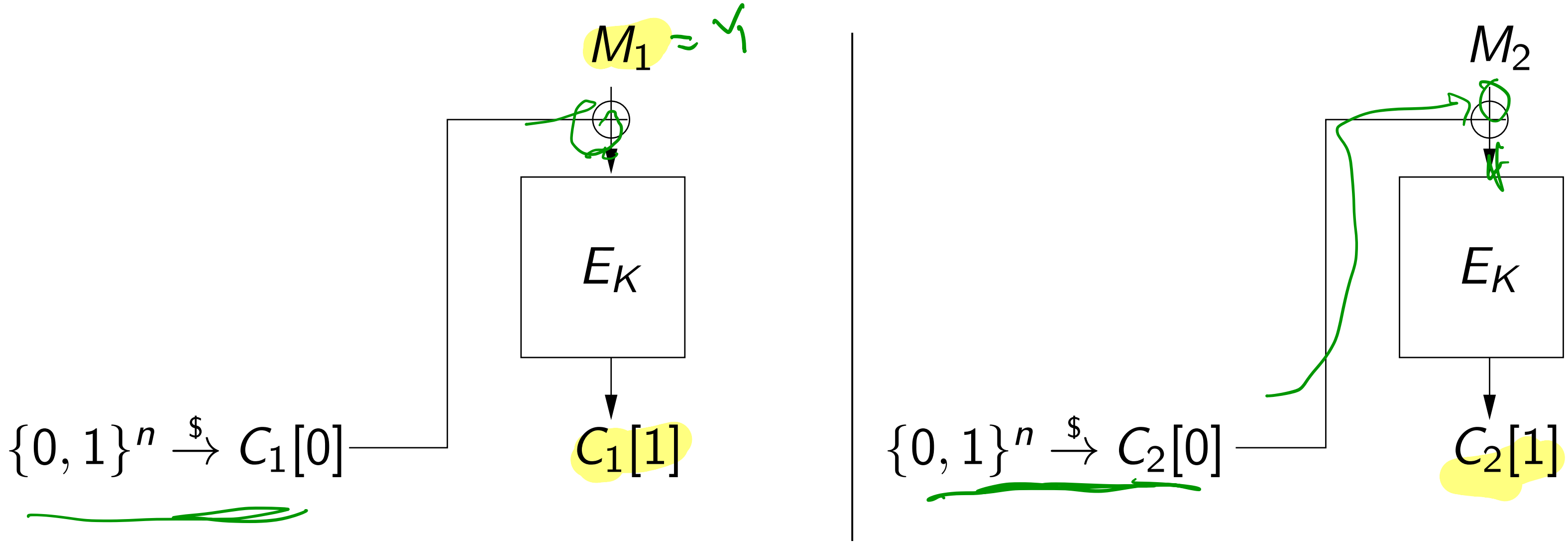
**Alg** $\mathcal{D}_K(C)$

for $i = 1, \ldots, m$ do
  $P[i] \leftarrow E_K(C[0] + i)$
  $M[i] \leftarrow P[i] \oplus C[i]$
return M

- $\mathcal{D}$ does not use $E_K^{-1}$! This is why CTR$ can use a family of functions $E$ that is not required to be a blockcipher.
- Encryption and Decryption are parallelizable.

# Voting with CBC-$

Suppose we encrypt $M_1, M_2 \in \{Y, N\}$ with CBC\$.




Adversary $A$ sees $C_1 = C_1[0]C_1[1]$ and $C_2 = C_2[0]C_2[1]$.

Suppose $A$ knows that $M_1 = Y$.

Can $A$ determine whether $M_2 = Y$ or $M_2 = N$?

# Assessing Security

- How to determine which modes of operations are “good” ones?

# Assessing Security

- How to determine which modes of operations are "good" ones?
- E.g., CBC-$ seems better than ECB. But is it secure? Or are there still attacks?

# Assessing Security

- How to determine which modes of operations are "good" ones?
- E.g., CBC-$ seems better than ECB. But is it secure? Or are there still attacks?
- Important since CBC-$ is widely used.

# Security requirements

Suppose sender computes

$$C_1 \xleftarrow{\$} \mathcal{E}_K(M_1)\,;\ \cdots\ ;\ C_q \xleftarrow{\$} \mathcal{E}_K(M_q)$$

Adversary $A$ has $C_1, \ldots, C_q$

| What if $A$ | |
|---|---|
| Retrieves $K$ | Bad! |
| Retrieves $M_1$ | Bad! |

But also we want to hide all partial information about the data stream, such as

- Does $M_1 = M_2$?
- What is first bit of $M_1$?
- What is XOR of first bits of $M_1, M_2$?

Something we won't hide: the length of the message

# Intuition

The master property MP is called IND-CPA (indistinguishability under chosen plaintext attack).

Consider encrypting one of two possible message streams, either

$$M_0^1, \ldots, M_0^q$$

or

$$M_1^1, \ldots, M_1^q \;,$$

where $|M_0^i| = |M_1^i|$ for all $1 \le i \le q$. Adversary, given ciphertexts $C^1, \ldots,$ $C^q$ and both data streams, has to figure out which of the two streams was encrypted.

We will even let the adversary pick the messages: It picks $(M_0^1, M_1^1)$ and gets back $C^1$, then picks $(M_0^2, M_1^2)$ and gets back $C^2$, and so on.

left stream: $M_0^1, \ldots, M_0^q$ right stream: $M_1^1, \ldots, M_1^q$

# IND-CPA

Let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme

| Game $\mathrm{Left}_{\mathcal{SE}}$ | Game $\mathrm{Right}_{\mathcal{SE}}$ |
|---|---|
| **procedure Initialize** | **procedure Initialize** |
| $K \xleftarrow{\$} \mathcal{K}$ | $K \xleftarrow{\$} \mathcal{K}$ |
| **procedure LR**$(M_0, M_1)$ | **procedure LR**$(M_0, M_1)$ |
| Return $C \xleftarrow{\$} \mathcal{E}_K(M_0)$ | Return $C \xleftarrow{\$} \mathcal{E}_K(M_1)$ |

Associated to $\mathcal{SE}, A$ are the probabilities

$$\Pr\left[\mathrm{Left}_{\mathcal{SE}}^{A} \Rightarrow 1\right] \quad \Big| \quad \Pr\left[\mathrm{Right}_{\mathcal{SE}}^{A} \Rightarrow 1\right]$$

that $A$ outputs 1 in each world. The (ind-cpa) advantage of $A$ is

$$\mathbf{Adv}_{\mathcal{SE}}^{\text{ind-cpa}}(A) = \Pr\left[\mathrm{Right}_{\mathcal{SE}}^{A} \Rightarrow 1\right] - \Pr\left[\mathrm{Left}_{\mathcal{SE}}^{A} \Rightarrow 1\right]$$

# Message length restriction

$(m_0, m_1) \Rightarrow |m_0| = |m_1|$

It is required that $|M_0| = |M_1|$ in any query $M_0, M_1$ that $A$ makes to **LR**. An adversary $A$ violating this condition is considered invalid.

This reflects that encryption is not aiming to hide the length of messages.

# Advantage Interpretation

$\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) \approx 1$ means $A$ is doing well and $\mathcal{SE}$ is not ind-cpa-secure.

$\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) \approx 0$ (or $\leq 0$) means $A$ is doing poorly and $\mathcal{SE}$ resists the attack $A$ is mounting.

Adversary resources are its running time $t$ and the number $q$ of its oracle queries, the latter representing the number of messages encrypted.

**Security:** $\mathcal{SE}$ is IND-CPA-secure if $\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A)$ is "small" for ALL $A$ that use "practical" amounts of resources.

**Insecurity:** $\mathcal{SE}$ is not IND-CPA-secure if we can specify an explicit $A$ that uses "few" resources yet achieves "high" ind-cpa-advantage.

# Security Analysis of ECB

Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. Recall that ECB mode defines symmetric encryption scheme $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ with

$$\mathcal{E}_K(M) = E_K(M[1])E_K(M[2]) \cdots E_K(M[m])$$

Can we design $A$ so that

$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) = \Pr\left[\text{Right}^{A}_{\mathcal{SE}} \Rightarrow 1\right] - \Pr\left[\text{Left}^{A}_{\mathcal{SE}} \Rightarrow 1\right]$$

is close to 1?

# Adversary

Let $\mathcal{E}_K(M) = E_K(M[1]) \cdots E_K(M[m])$.

**adversary** $A$

$C_1 \leftarrow \mathbf{LR}(0^n, 0^n)\,;\; C_2 \leftarrow \mathbf{LR}(1^n, 0^n)$

if $C_1 = C_2$ then return 1 else return 0

$$\mathrm{Adv}^{\mathrm{ind\text{-}cpa}}(A) = \Pr[\mathrm{RIGHT}^A \Rightarrow 1] - \Pr[\mathrm{LEFT}^A \Rightarrow 1]$$

$\to 1$ $\mathcal{E}$ is deterministic

$\to 0$ $E_K$ is a permutation for all $K$

# Analysis

# IND-CPA

We claim that if encryption scheme $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is IND-CPA secure then the ciphertext hides ALL partial information about the plaintext.

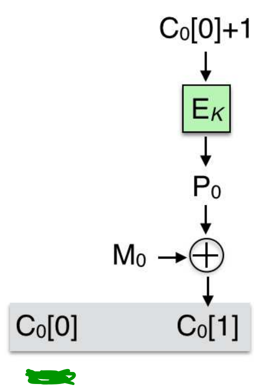
For example, from $C_1 \xleftarrow{\$} \mathcal{E}_K(M_1)$ and $C_2 \xleftarrow{\$} \mathcal{E}_K(M_2)$ the adversary cannot

- get $M_1$
- get 1st bit of $M_1$
- get XOR of the 1st bits of $M_1, M_2$
- etc.

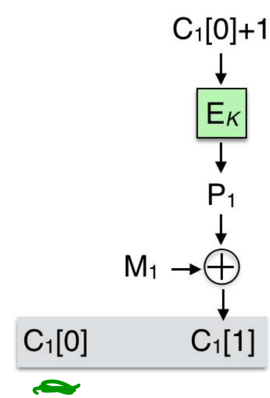
# Security Analysis of CTR-\$

Let $E : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a blockcipher and $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ the corresponding CTR\$ symmetric encryption scheme. Suppose 1-block messages $M_0, M_1$ are encrypted:

$$C_0[0]C_0[1] \xleftarrow{\$} \mathcal{E}(K, M_0)$$




$$C_1[0]C_1[1] \xleftarrow{\$} \mathcal{E}(K, M_1)$$




Let us say we are **lucky** If $C_0[0] = C_1[0]$. If so:

$$C_0[1] = C_1[1] \text{ if and only if } M_0 = M_1$$

So if we are lucky we can detect message equality and violate IND-CPA.

# The Adversary

birthday attack on IV of CTR-$

Let $1 \leq q < 2^n$ be a parameter and let $\langle i \rangle$ be integer $i$ encoded as an $\ell$-bit string.

$\Pr[S \neq \emptyset] = C(2^n, q)$

$\approx \frac{q^2}{2^n}$

**adversary** $A_q$

for $i = 1, \ldots, q$ do

  $C^i[0]C^i[1] \xleftarrow{\$} \mathbf{LR}(\langle i \rangle, \boxed{\langle 0 \rangle})$

$S \leftarrow \{(j,t) : C^j[0] = C^t[0] \text{ and } j < t\}$

If $S \neq \emptyset$, then

  $(j,t) \xleftarrow{\$} S$

  If $C^j[1] = C^t[1]$ then return 1

return 0

$\Pr[\mathrm{RIGHT}^A \Rightarrow 1]$

$= C(2^n, q)$

$\Pr[\mathrm{LEFT}^A \Rightarrow 1] = 0.$

$IV \rightarrow 0^n$  $IV \rightarrow 0^n$

# Right Game Analysis

**adversary $A$**

for $i = 1, \ldots, q$ do

$\quad C^i[0]C^i[1] \xleftarrow{\$} \mathbf{LR}(\langle i \rangle, \langle 0 \rangle)$

$S \leftarrow \{(j,t)\colon C^j[0] = C^t[0] \text{ and } j < t\}$

If $S \neq \emptyset$, then

$\quad (j,t) \xleftarrow{\$} S$

$\quad$ If $C^j[1] = C^t[1]$ then return 1

return 0

Game $\mathrm{Right}_{\mathcal{SE}}$

**procedure Initialize**

$K \xleftarrow{\$} \mathcal{K}$

**procedure LR**$(M_0, M_1)$

$C[0] \xleftarrow{\$} \{0,1\}^n$

$P \leftarrow E(K, C[0]+1)$

$C[1] \leftarrow P \oplus M_1$

Return $C[0]C[1]$

If $C^j[0] = C^t[0]$ (lucky) then

$$C^j[1] = \langle 0 \rangle \oplus E_K(C^j[0]+1) = \langle 0 \rangle \oplus E_K(C^t[0]+1) = C^t[1]$$

so

$$\Pr\left[\mathrm{Right}_{\mathcal{SE}}^A \Rightarrow 1\right] = \Pr\left[S \neq \emptyset\right] = C(2^n, q)$$

# Left game analysis

**adversary** $A$

for $i = 1, \ldots, q$ do

$\quad C^i[0]C^i[1] \xleftarrow{\$} \mathbf{LR}(\langle i \rangle, \langle 0 \rangle)$

$S \leftarrow \{(j,t)\colon C^j[0] = C^t[0] \text{ and } j < t\}$

If $S \neq \emptyset$, then

$\quad (j,t) \xleftarrow{\$} S$

$\quad$ If $C^j[1] = C^t[1]$ then return 1

return 0

Game $\mathrm{Left}_{\mathcal{SE}}$

**procedure Initialize**

$K \xleftarrow{\$} \mathcal{K}$

**procedure LR**$(M_0, M_1)$

$C[0] \xleftarrow{\$} \{0,1\}^n$

$P \leftarrow E(K, C[0]+1)$

$C[1] \leftarrow P \oplus M_0$

Return $C[0]C[1]$

If $C^j[0] = C^t[0]$ (lucky) then

$$C^j[1] = \langle j \rangle \oplus E_K(C^j[0]+1) \neq \langle t \rangle \oplus E_K(C^t[0]+1) = C^t[1]$$

so

$$\Pr\left[\mathrm{Left}^A_{\mathcal{SE}} \Rightarrow 1\right] = 0.$$

# Conclusion

$$
\begin{aligned}
\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) &= \Pr\left[\text{Right}^{A}_{\mathcal{SE}}\Rightarrow 1\right] - \Pr\left[\text{Left}^{A}_{\mathcal{SE}}\Rightarrow 1\right] \\
&= C(2^n, q) - 0 \;\geq\; 0.3 \cdot \frac{q(q-1)}{2^n}
\end{aligned}
$$

Conclusion: CTR\$ can be broken (in the IND-CPA sense) in about $2^{n/2}$ queries, where $n$ is the block length of the underlying block cipher, regardless of the cryptanalytic strength of the block cipher.

# Security of CTR-$

So far: A $q$-query adversary can break CTR\$ with advantage $\approx \frac{q^2}{2^{n+1}}$

Question: Is there any better attack?

# Security of CTR-$

So far: A $q$-query adversary can break CTR$ with advantage $\approx \frac{q^2}{2^{n+1}}$

Question: Is there any better attack?

Answer: NO!

We can prove that the best $q$-query attack short of breaking the block cipher has advantage at most

$$\frac{\sigma^2}{2^n}$$

where $\sigma$ is the total number of blocks encrypted.

Example: If $q$ 1-block messages are encrypted then $\sigma = q$ so the adversary advantage is not more than $q^2/2^n$.

For $E =$ AES this means up to $2^{64}$ blocks may be securely encrypted, which is good.

# Theorem Statement

Theorem: [BDJR98] Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher and $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ the corresponding CTR\$ symmetric encryption scheme. Let $A$ be an ind-cpa adversary against $\mathcal{SE}$ that has running time $t$ and makes at most $q$ **LR** queries, these totalling at most $\sigma$ blocks. Then there is a prf-adversary $B$ against $E$ such that

$$\boxed{\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) \le 2 \cdot \mathbf{Adv}^{\text{prf}}_{E}(B) + \frac{\sigma^2}{2^n}}$$

Furthermore, $B$ makes at most $\sigma$ oracle queries and has running time $t + \Theta(\sigma \cdot n)$.

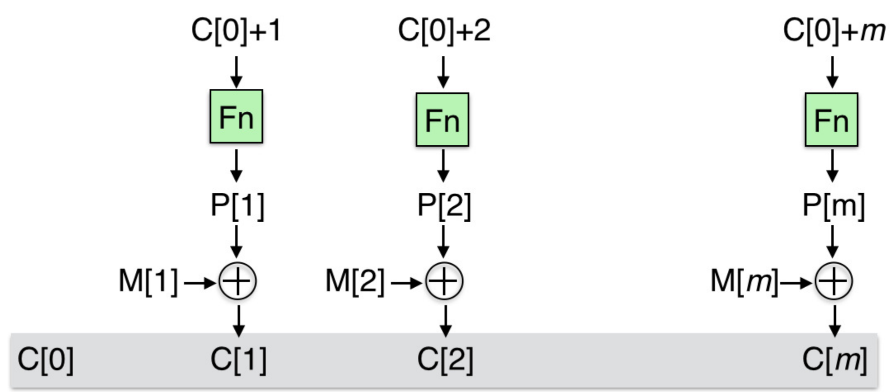
$$\frac{1}{2}\left(\mathrm{Adv}(A) - \frac{\sigma^2}{2^n}\right) \le \mathrm{Adv}(B)$$

# Proof Inuition/Preliminaries

Consider the CTR\$ scheme with $E_K$ replaced by a random function **Fn** with range $\{0,1\}^\ell$.

**Alg** $\mathcal{E}_{\mathbf{Fn}}(M)$

$C[0] \xleftarrow{\$} \{0,1\}^n$
for $i = 1, \ldots, m$ do
  $P[i] \leftarrow \mathbf{Fn}(C[0] + i)$
  $C[i] \leftarrow P[i] \oplus M[i]$
return $C$




Analyzing this is a thought experiment, but we can ask whether it is IND-CPA secure.

If so, the assumption that $E$ is a PRF says CTR\$ with $E$ is IND-CPA secure.

A PRF "rolls up" an exponentially ~~…~~ long random tape. Why?

The tape is $F_k(\langle 1 \rangle) \| F_k(\langle 2 \rangle) \| \ldots$

Let $E$ be the event that the points

$$C_1[0]+1, \ldots, C_1[0]+m, \ldots, C_q[0]+1, \ldots, C_q[0]+m\ ,$$

on which **Fn** is evaluated across the $q$ encryptions, are all distinct.

**Case 1:** $E$ happens. Then the encryption is a one-time-pad: ciphertexts are random, independent strings, regardless of which message is encrypted. So $A$ has zero advantage.

**Case 2:** $E$ doesn't happen. Then $A$ may have high advantage but it does not matter because $\Pr[E]$ doesn't happen is small. (It is the small additive term in the theorem.)

Let $N, q, m \geq 1$ be integers and let $\mathbf{Z}_N = \{0, 1, \ldots, N-1\}$. Let $+$ be addition modulo $N$. Consider the game

For $i = 1, \ldots, q$ do
$\quad c_i \xleftarrow{\$} \mathbf{Z}_N$ ; $I_i \leftarrow \{c_i + 1, \ldots, c_i + m\}$

For $1 \leq i < j \leq q$ define the events

$$\mathrm{B}_{i,j} \; : \; I_i \cap I_j \neq \emptyset \quad \text{and} \quad \mathrm{B} \; : \; \bigvee_{1 \leq i < j \leq q} \mathrm{B}_{i,j} \; .$$

Then let

$$\mathrm{IIP}(N, q, m) = \Pr[\mathrm{B}] \; .$$

**Problem:** Upper bound $\mathrm{IIP}(N, q, m)$ as a function of $N, q, m$.

**Claim:** $\mathrm{IIP}(N, q, m) \leq \frac{q(q-1)}{2} \frac{(2m-1)}{N}$

# Two formulations of advantage

# A Game-Playing Proof

Let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a symmetric encryption scheme and $A$ an adversary.

| | |
|---|---|
| Game $\mathrm{Guess}_{\mathcal{SE}}$ | **procedure LR**$(M_0, M_1)$ |
| | return $C \xleftarrow{\$} \mathcal{E}_K(M_b)$ |
| **procedure Initialize** | **procedure Finalize**$(b')$ |
| $K \xleftarrow{\$} \mathcal{K}\,;\ b \xleftarrow{\$} \{0,1\}$ | return $(b = b')$ |

Proposition: $\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) = 2 \cdot \Pr\left[\mathrm{Guess}^{A}_{\mathcal{SE}} \Rightarrow \mathsf{true}\right] - 1.$

The proof uses a sequence of games and invokes the fundamental lemma of game playing [BR96].

The games have the following **Initialize** and **Finalize** procedures:

| **Initialize** // $G_0$ | **Initialize** // $G_1, G_2, G_3$ | **Finalize** // All games |
|---|---|---|
| $b \stackrel{\$}{\leftarrow} \{0,1\}$ ; $S \leftarrow \emptyset$ <br> $K \stackrel{\$}{\leftarrow} \{0,1\}^k$ | $b \stackrel{\$}{\leftarrow} \{0,1\}$ ; $S \leftarrow \emptyset$ | Return $(b = b')$ |

For brevity we omit writing these procedures explicitly in the games, but you should remember they are there.

Also for brevity if $G$ is a game and $A$ is an adversary then we let

$$\Pr[G^A] = \Pr[G^A \Rightarrow \text{true}]$$

| Game $G_0$ | Game $G_1$ |
| --- | --- |
| **procedure LR**$(M_0, M_1)$ | **procedure LR**$(M_0, M_1)$ |
| $C[0] \xleftarrow{\$} \{0,1\}^n$ | $C[0] \xleftarrow{\$} \{0,1\}^n$ |
| for $i = 1, ..., m$ do | for $i = 1, ..., m$ do |
| $\quad P \leftarrow C[0] + i$ | $\quad P \leftarrow C[0] + i$ |
| $\quad$ if $P \notin S$ then $\mathsf{T}[P] \leftarrow E_K(P)$ | $\quad$ if $P \notin S$ then $\mathsf{T}[P] \xleftarrow{\$} \{0,1\}^\ell$ |
| $\quad C[i] \leftarrow T[P] \oplus M_b[i]$ | $\quad C[i] \leftarrow \mathsf{T}[P] \oplus M_b[i]$ |
| $\quad S \leftarrow S \cup \{P\}$ | $\quad S \leftarrow S \cup \{P\}$ |
| return $C$ | return $C$ |

Then

$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) = 2 \cdot \Pr\left[G_0^A\right] - 1$$

Clearly $\Pr[G_0^A] = \Pr[G_1^A] + \big(\Pr[G_0^A] - \Pr[G_1^A]\big)$.

Claim 1: We can design prf-adversary $B$ so that

$$\Pr[G_0^A] - \Pr[G_1^A] \le \mathbf{Adv}_E^{\mathrm{prf}}(B)$$

Claim 2: $\Pr[G_1^A] \le \frac{1}{2} + \frac{(q-1)\sigma}{2^n}$

Given these, we have

$$\begin{aligned}
\mathbf{Adv}_{\mathcal{SE}}^{\mathrm{ind\text{-}cpa}}(A) &\le 2 \cdot \left(\frac{1}{2} + \frac{(q-1)\sigma}{2^n}\right) - 1 + 2 \cdot \mathbf{Adv}_E^{\mathrm{prf}}(B) \\
&= \frac{2(q-1)\sigma}{2^n} + 2 \cdot \mathbf{Adv}_E^{\mathrm{prf}}(B)
\end{aligned}$$

which proves the theorem. It remains to prove the claims.

**adversary** $B$

$b \xleftarrow{\$} \{0,1\}$ ; $S \leftarrow \emptyset$
$b' \xleftarrow{\$} A^{\mathrm{LRSim}}$
if $(b = b')$ then return 1
else return 0

**subroutine** $\mathrm{LRSim}(M_0, M_1)$
$C[0] \xleftarrow{\$} \{0,1\}^n$
for $i = 1, ..., m$ do
    $P \leftarrow C[0] + i$
    if $P \notin S$ then $T[P] \leftarrow \mathbf{Fn}(P)$
    $C[i] \leftarrow T[P] \oplus M_b[i]$
    $S \leftarrow S \cup \{P\}$
return $C$

$$\Pr\left[\mathrm{Real}_E^B \Rightarrow 1\right] = \Pr\left[G_0^A\right]$$

$$\Pr\left[\mathrm{Rand}_{\{0,1\}^n}^B \Rightarrow 1\right] = \Pr\left[G_1^A\right]$$

Subtracting, we get Claim 1.

Game $G_1$

**procedure LR**$(M_0, M_1)$

$C[0] \xleftarrow{\$} \{0,1\}^n$

for $i = 1, \dots, m$ do

$\quad P \leftarrow C[0] + i$

$\quad$ If $P \notin S$ then

$\quad\quad \mathsf{T}[P] \xleftarrow{\$} \{0,1\}^\ell$

$\quad C[i] \leftarrow \mathsf{T}[P] \oplus M_b[i]$

$\quad S \leftarrow S \cup \{P\}$

return $C$

Game $\boxed{G_2}$ , $G_3$

**procedure LR**$(M_0, M_1)$

$C[0] \xleftarrow{\$} \{0,1\}^n$

for $i = 1, \dots, m$ do

$\quad P \leftarrow C[0] + i$

$\quad C[i] \xleftarrow{\$} \{0,1\}^\ell$

$\quad$ If $P \in S$ then

$\quad\quad \mathsf{bad} \leftarrow \mathsf{true}$ ; $\boxed{C[i] \leftarrow \mathsf{T}[P] \oplus M_b[i]}$

$\quad \mathsf{T}[P] \leftarrow C[i] \oplus M_b[i]$

$\quad S \leftarrow S \cup \{P\}$

return $C$

$$\Pr[G_1^A] = \Pr[G_2^A] = \Pr[G_3^A] + \left(\Pr[G_2^A] - \Pr[G_3^A]\right)$$

Game $G_3$

**procedure LR**$(M_0, M_1)$

$C[0] \xleftarrow{\$} \{0,1\}^n$

for $i = 1, ..., m$ do

$\quad P \leftarrow C[0] + i$; $C[i] \xleftarrow{\$} \{0,1\}^\ell$

$\quad$ If $P \in S$ then $\mathsf{bad} \leftarrow \mathsf{true}$

$\quad \mathsf{T}[P] \leftarrow C[i] \oplus M_b[i]$; $S \leftarrow S \cup \{P\}$

return $C$

Ciphertext $C$ in $G_3$ is always random, independently of $b$, so

$$\Pr\left[G_3^A\right] = \frac{1}{2}.$$

Game $\boxed{G_2}$ , $G_3$

**procedure LR**$(M_0, M_1)$

$C[0] \xleftarrow{\$} \{0,1\}^n$

for $i = 1, ..., m$ do

$\quad P \leftarrow C[0] + i;\ C[i] \xleftarrow{\$} \{0,1\}^\ell$

$\quad$ If $P \in S$ then

$\quad\quad \mathsf{bad} \leftarrow \mathsf{true};\ \boxed{C[i] \leftarrow \mathsf{T}[P] \oplus M_b[i]}$

$\quad \mathsf{T}[P] \leftarrow C[i] \oplus M_b[i];\ S \leftarrow S \cup \{P\}$

return $C$

$G_2$ and $G_3$ are identical-until-bad, so Fundamental Lemma implies

$$\Pr\left[G_2^A\right] - \Pr\left[G_3^A\right] \leq \Pr\left[G_3^A \,\mathrm{sets}\, \mathsf{bad}\right].$$

Game $G_3$

**procedure LR**$(M_0, M_1)$

$C[0] \xleftarrow{\$} \{0,1\}^n$

for $i = 1, ..., m$ do

$\quad P \leftarrow C[0] + i;\ C[i] \xleftarrow{\$} \{0,1\}^\ell$

$\quad$ If $P \in S$ then $\mathsf{bad} \leftarrow \mathsf{true}$

$\quad \mathsf{T}[P] \leftarrow C[i] \oplus M_b[i];\ S \leftarrow S \cup \{P\}$

return $C$

$$\begin{aligned}
\Pr\left[G_3^A \,\mathrm{sets}\, \mathsf{bad}\right] &\leq \mathrm{IIP}(2^n, q, m) \leq \frac{q(q-1)}{2}\frac{2m-1}{2^n} \\
&\leq \frac{mq(q-1)}{2^n} \\
&\leq \frac{(q-1)\sigma}{2^n}\ .
\end{aligned}$$

- Analogous theorem holds for CBC-\$.

- Analogous theorem holds for CBC-$.
- Provides a quantitative guarantee on how many blocks can be securely encrypted using these modes (assuming the underlying block cipher is good).

# Semantic Security