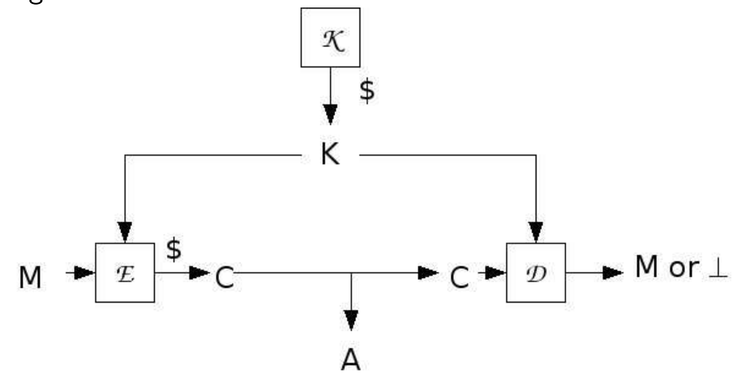
SYMMETRIC ENCRYPTION

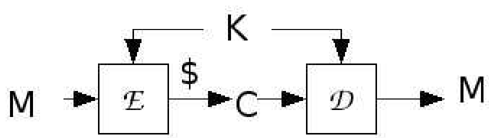
Syntax

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



- $\mathcal{K}$ is randomized
- $\mathcal{E}$ can be randomized or stateful
- $\mathcal{D}$ is deterministic

Correct decryption requirement



Formally: For all K and M we have

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

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

Example: OTP

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

Alg $\mathcal{K}$	Alg $\mathcal{E}_K(M)$	Alg $\mathcal{D}_K(C)$
$K \xleftarrow{\$} \{0,1\}^k$	$C \leftarrow K \oplus M$	$M \leftarrow K \oplus C$
return K	return C	return M

Correct decryption:

$$\begin{aligned} \mathcal{D}_K(\mathcal{E}_K(M)) &= \mathcal{D}_K(K \oplus M) \\ &= K \oplus (K \oplus M) \\ &= M \end{aligned}$$

Block cipher modes of operation

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

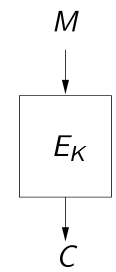
Notation: $x[i]$ is the i-th n-bit block of a string x, so that $x = x[1] \ldots x[m]$ if $|x| = nm$.

Always:

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

Block cipher modes of operation

Block cipher provides parties sharing K with



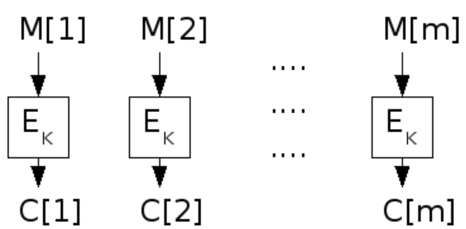
which enables them to encrypt a 1-block message.

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

ECB: Electronic Codebook Mode

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

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



Correct decryption relies on E being a block cipher, so that E_K is invertible

Evaluating Security

Sender encrypts some messages $M_1, \ldots, M_q$, namely

$$C_1 \stackrel{\$}{\leftarrow} \mathcal{E}_K(M_1), \ldots, C_q \stackrel{\$}{\leftarrow} \mathcal{E}_K(M_q)$$

and transmits $C_1, \ldots, C_q$ to receiver.

Adversary

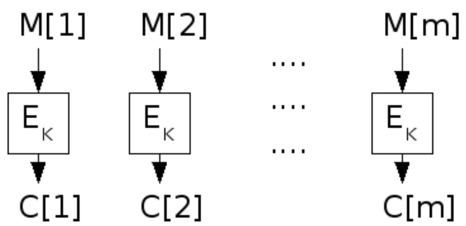
- Knows $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$
- Knows $C_1, \ldots, C_q$
- Is not given K!

Possible adversary goals:

- Recover K
- Recover M_1

But we will need to look beyond these

Security of ECB



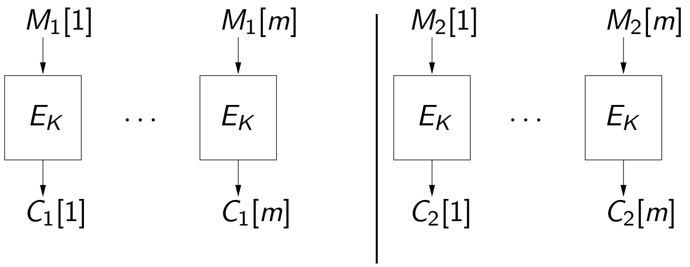
Adversary has ciphertext $C = C[1] \cdots C[m]$

Adversary task	Assessment	Why?
Compute K	seems hard	E is secure
Compute $M[1]$	seems hard	E is secure

Security of ECB

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

Why is the above true? Because E_K is deterministic:



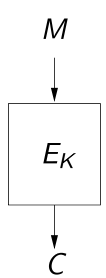
Why does this matter?

Security of ECB

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

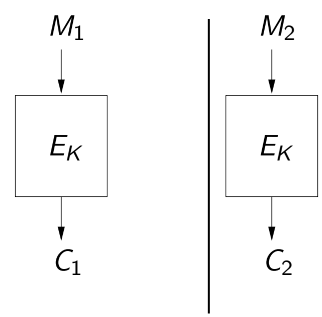
- FIRE or DON'T FIRE a missile
- BUY or SELL a stock
- Vote YES or NO

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



Security of ECB

Votes $M_1, M_2 \in \{Y, N\}$ are ECB encrypted and adversary sees ciphertexts $C_1 = E_K(M_1)$ and $C_2 = E_K(M_2)$



Adversary may have cast the first vote and thus knows M_1; say $M_1 = Y$. Then adversary can figure out M_2:

- If $C_2 = C_1$ then M_2 must be Y
- Else M_2 must be N

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?

Yes, if $\mathcal{E}$ is deterministic.

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

$$Pr[C_1 = C_2]$$

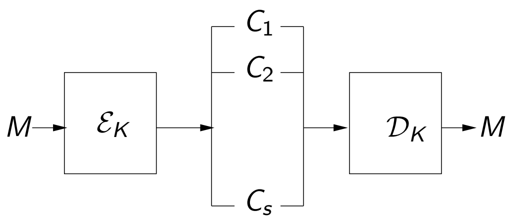
will (should) be small, where the probability is over the coins of $\mathcal{E}$.

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.

Stateful encryption

An alternative to randomization is to allow the encryption algorithm to maintain state. This might be a counter

- encrypt depending on counter value
- then update counter

We will see schemes that use this paradigm to get around the security weaknesses of deterministic encryption without using randomness.

More Modes of Operation

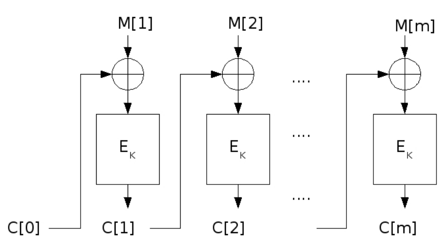
<u>Randomized</u>	<u>Stateful</u>
CBC$, CTR$	CBCC,CTRC

CBC$: Cipher Block Chaining with random IV mode

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

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 so that E_K is invertible

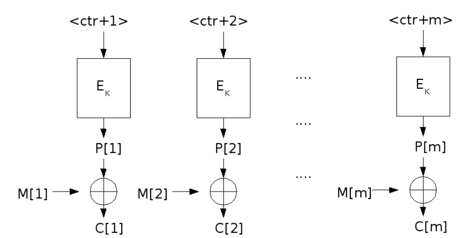
CTRC mode

Sender maintains a counter *ctr* that is initially 0 and is updated by $\mathcal{E}$

$\langle j \rangle$ = the n-bit binary representation of integer$j$ $(0 \le j < 2^n)$

Alg $\mathcal{E}_K(M)$
$C[0] \leftarrow$ ctr
for $i = 1, \ldots, m$ do
  $P[i] \leftarrow E_K(\langle ctr + i \rangle)$
  $C[i] \leftarrow P[i] \oplus M[i]$
ctr $\leftarrow$ ctr + m
return C

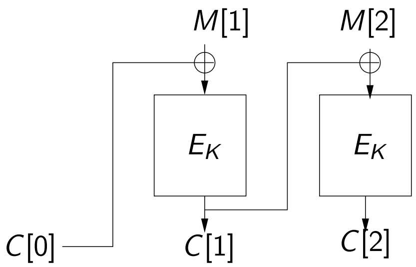
Alg $\mathcal{D}_K(C)$
ctr $\leftarrow C[0]$
for $i = 1, \ldots, m$ do
  $P[i] \leftarrow E_K(\langle ctr + i \rangle)$
  $M[i] \leftarrow P[i] \oplus C[i]$
return M



- Decryptor does not maintain a counter

Security of CBC$ against key recovery

If adversary has a plaintext M and corresponding ciphertext $C \xleftarrow{\$} \mathcal{E}_K(M)$ then it has input-output examples $(M[1] \oplus C[0], C[1]), (M[2] \oplus C[1], C[2])$ of E_K.

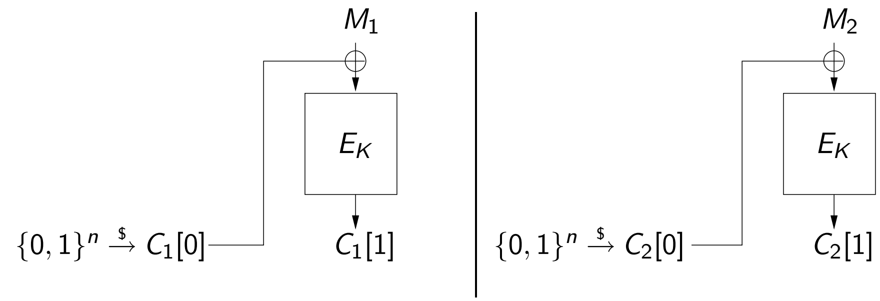


So chosen-message key recovery attacks on E can be mounted to recover K.

Conclusion: Security of CBC$ against key recovery is no better than that of the underlying block cipher.

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 $C_2 = C_2[0]C_2[1]$.

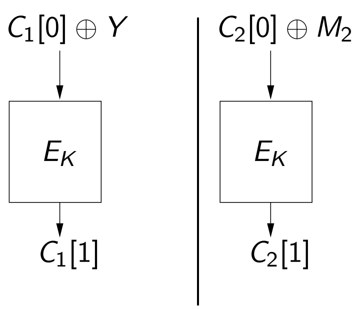
Suppose A knows that $M_1 = Y$.

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

NO!

Voting with CBC$

If $M_1 = Y$ we have



A knows $C_1[0]C_1[1]$ and $C_2[0]C_2[1]$. Now

- If $C_1[0] = C_2[0]$ then A can deduce that
  - If $C_2[1] = C_1[1]$ then $M_2 = Y$
  - If $C_2[1] \neq C_1[1]$ then $M_2 = N$
- But the probability that $C_1[0] = C_2[0]$ is very small.

Assessing security

So CBC$ is better than ECB. But is it secure?

CBC$ is the world's most widely used encryption scheme (SSL, SSH, TLS, ...) so knowing whether it is secure is important

To answer this we first need to decide and formalize what we mean by secure.

Types of encryption schemes

Special purpose: Used in a specific setting, to encrypt data of some known format or distribution. Comes with a

WARNING! only use under conditions X.

General purpose: Used to encrypt in many different settings, where the data format and distribution are not known in advance.

We want general purpose schemes because

- They can be standardized and broadly used.
- Once a scheme is out there, it gets used for everything anyway.
- General purpose schemes are easier to use and less subject to mis-use: it is hard for application designers to know whether condition X is met.

Security requirements

A priori information: What the adversary already knows about the data from the context. For example, it is drawn from $\{Y, N\}$

Data distribution or format: The data may be English or not; may have randomness or not; ...

Security should not rely on assumptions about these things.

E-mail encryption

E-mail data could be

- English text
- A pdf or executable file
- Votes

Want security in all these cases.

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 ...

Security requirements

We want to hide all partial information about the data stream.

Examples of partial information:

- 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

What we seek

We want a single "master" property MP of an encryption scheme such that

- MP can be easily specified
- We can evaluate whether a scheme meets it
- MP implies ALL the security conditions we want: it guarantees that a ciphertext reveals NO partial information about the plaintext.

Thus a scheme having MP means not only that if adversary has $C_1 \xleftarrow{\$} \mathcal{E}_K(M_1)$ and $C_2 \xleftarrow{\$} \mathcal{E}_K(M_2)$ then

- It can't get M_1
- It can't get 1st bit of M_1
- It can't get XOR 1st bits of M_1, M_2

but in fact implies "all" such information about M_1, M_2 is protected.

Seeking MP

So what is the master property MP?

It is a notion we call indistinguishability (IND). We will define

- IND-CPA: Indistinguishability under chosen-plaintext attack
- IND-CCA: Indistinguishability under chosen-ciphertext attack

Plan

- Define IND-CPA
- Examples of non-IND-CPA schemes
- See why IND-CPA is a "master" property, namely why it implies that ciphertexts leak no partial information about plaintexts
- Examples of IND-CPA schemes
- IND-CCA

Intuition for definition of IND

Consider encrypting one of two possible message streams, either

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

or

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

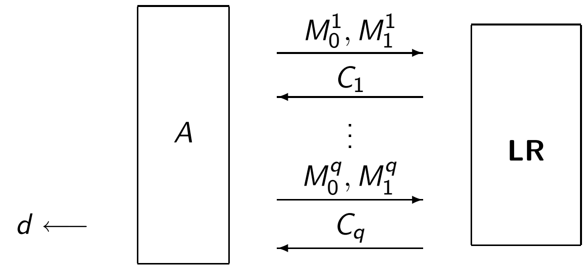
Adversary, given ciphertexts and both data streams, has to figure out which of the two streams was encrypted.

ind-cpa-adversaries

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

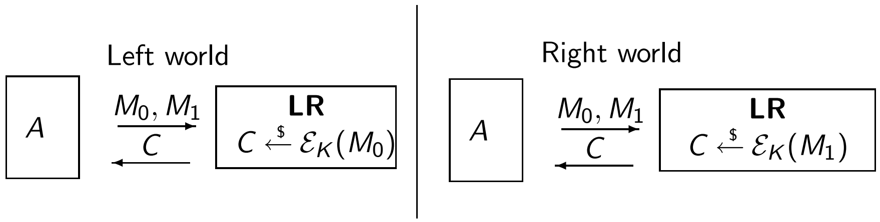
An ind-cpa adversary A has an oracle **LR**

- It can make a query M_0, M_1 consisting of any two equal-length messages
- It can do this many times
- Each time it gets back a ciphertext
- It eventually outputs a bit



ind-cpa-adversaries

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



A's output d	Intended meaning: I think I am in the
1	Right world
0	Left world

The harder it is for A to guess world it is in, the more "secure" $\mathcal{SE}$ is as an encryption scheme.

The games

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

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

Example

Let $E\colon \{0,1\}^k \times \{0,1\}^{128} \to \{0,1\}^{128}$ be a block cipher and let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be defined by

Alg $\mathcal{K}$	**Alg** $\mathcal{E}_K(M)$	**Alg** $\mathcal{D}_K(M)$
$K \xleftarrow{\$} \{0,1\}^k$	return $E_K(M)$	return $E_K^{-1}(M)$
return K		

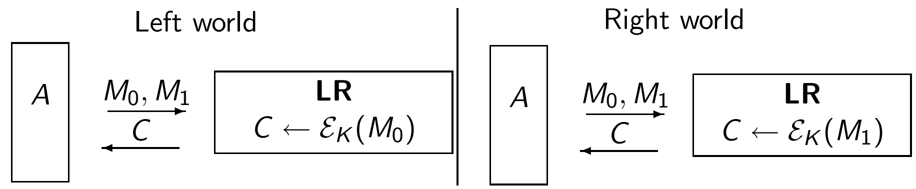
This scheme encrypts only 1-block messages.

Succinctly: $\mathcal{E}_K(M) = E_K(M)$

Example

Let $\mathcal{E}_K(M) = E_K(M)$ and let A be the following ind-cpa adversary

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

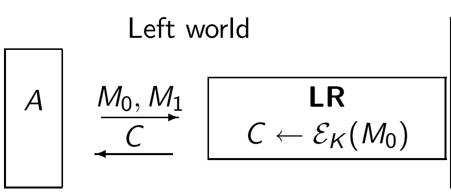


Then

$$\Pr\left[\mathrm{Left}^A_{\mathcal{SE}} \Rightarrow 1\right] = \qquad \Big| \qquad \Pr\left[\mathrm{Right}^A_{\mathcal{SE}} \Rightarrow 1\right] =$$

Example

Let $\mathcal{E}_K(M) = E_K(M)$



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

What happens

- $C_1 = \mathcal{E}_K(0^n) = E_K(0^n)$
- $C_2 = \mathcal{E}_K(1^n) = E_K(1^n) \neq E_K(0^n)$
- so $C_1 \neq C_2$ and A returns 0

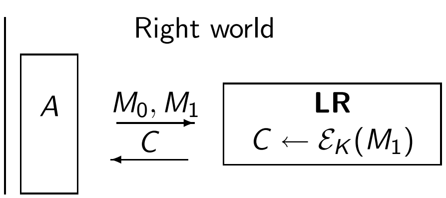
so

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

Example

Let $\mathcal{E}_K(M) = E_K(M)$

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



What happens

- $C_1 = \mathcal{E}_K(0^n) = E_K(0^n)$
- $C_2 = \mathcal{E}_K(0^n) = E_K(0^n)$
- so $C_1 = C_2$ and A returns 1

so

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

Example

Let $\mathcal{E}_K(M) = E_K(M)$

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

$$\begin{aligned}\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) &= \Pr\left[\text{Right}^A_{\mathcal{SE}} \Rightarrow 1\right] - \Pr\left[\text{Left}^A_{\mathcal{SE}} \Rightarrow 1\right] \\ &= 1 - 0 \\ &= 1\end{aligned}$$

The measure of success

Let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme and A be an ind-cpa adversary. Then

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

is a number between -1 and 1.

A "large" (close to 1) advantage means

- A is doing well
- $\mathcal{SE}$ is not secure

A "small" (close to 0 or ≤ 0) advantage means

- A is doing poorly
- $\mathcal{SE}$ resists the attack A is mounting

IND-CPA security

Adversary advantage depends on its

- strategy
- resources: Running time t and number q of oracle queries

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

Example: 80-bit security could mean that for all $n = 1, \ldots, 80$ we have

$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) \leq 2^{-n}$$

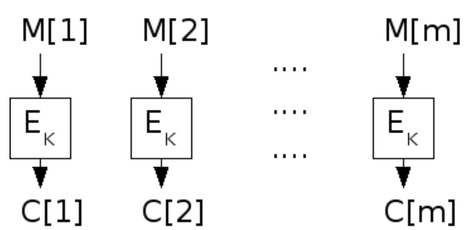
for any A with time and number of oracle queries at most 2^{80-n}.

Insecurity: $\mathcal{SE}$ is not IND-CPA (i.e. insecure) if there exists A using "few" resources that achieves "high" advantage.

ECB is not IND-CPA-secure

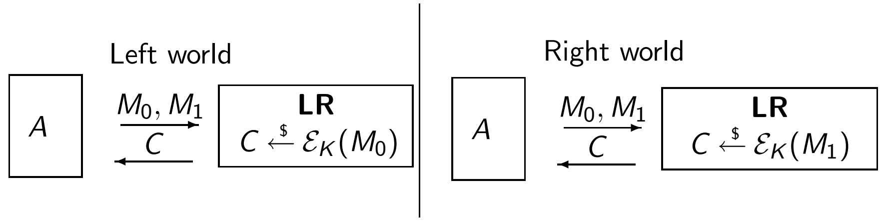
Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. Recall that ECB mode defines symmetric encryption scheme $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ with

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



ECB is not IND-CPA-secure

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



Can we design A so that

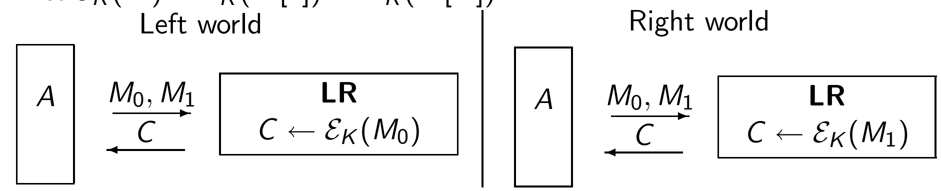
$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) = \Pr\left[\text{Right}^{A}_{\mathcal{SE}} \Rightarrow 1\right] - \Pr\left[\text{Left}^{A}_{\mathcal{SE}} \Rightarrow 1\right]$$

is close to 1?

Exploitable weakness of $\mathcal{SE}$: $M_1 = M_2$ implies $\mathcal{E}_K(M_1) = \mathcal{E}_K(M_2)$.

ECB is not IND-CPA-secure

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



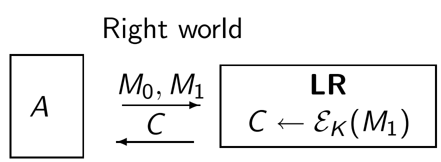
adversary A
$C_1 \leftarrow \mathbf{LR}(0^n, 0^n)$; $C_2 \leftarrow \mathbf{LR}(1^n, 0^n)$
if $C_1 = C_2$ then return 1 else return 0

ECB is not IND-CPA-secure: Right world analysis

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

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

Game $\text{Right}_{\mathcal{SE}}$
procedure Initialize
$K \xleftarrow{\$} \mathcal{K}$
procedure LR(M_0, M_1)
Return $\mathcal{E}_K(M_1)$



Then

$$\Pr\left[\text{Right}^{A}_{\mathcal{SE}} \Rightarrow 1\right] = 1$$

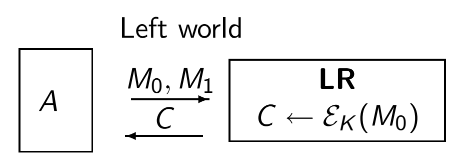
because $C_1 = E_K(0^n) = E_K(0^n) = C_2$.

ECB is not IND-CPA-secure: Left world analysis

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

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

Game $\text{Left}_{\mathcal{SE}}$
procedure Initialize
$K \xleftarrow{\$} \mathcal{K}$
procedure LR(M_0, M_1)
Return $\mathcal{E}_K(M_0)$



Then

$$\Pr\left[\text{Left}^{A}_{\mathcal{SE}} \Rightarrow 1\right] = 0$$

because $C_1 = E_K(0^n) \neq E_K(1^n) = C_2$.

ECB is not IND-CPA secure

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

$$\begin{aligned}\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) &= \overbrace{\Pr\left[\text{Right}^{A}_{\mathcal{SE}} = 1\right]}^{1} - \overbrace{\Pr\left[\text{Right}^{A}_{\mathcal{SE}} = 1\right]}^{0} \\ &= 1\end{aligned}$$

And A is very efficient, making only two queries.

Thus ECB is **not** IND-CPA secure.

Why is IND-CPA the "master" property?

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.

Why is this true?

XOR-insecurity implies IND-CPA-insecurity

Let $\text{lsb}(M)$ denote the last bit of M

Suppose we are given an adversary B such that

$$\begin{array}{l}\mathcal{E}_K(M_1) \xrightarrow{\$} C_1 \rightarrow \\ \mathcal{E}_K(M_2) \xrightarrow{\$} C_2 \rightarrow\end{array} \boxed{\quad B \quad} \rightarrow \text{lsb}(M_1) \oplus \text{lsb}(M_2)$$

for all M_1, M_2. Then we claim we can design an ind-cpa adversary A such that

$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) = 1 \,,$$

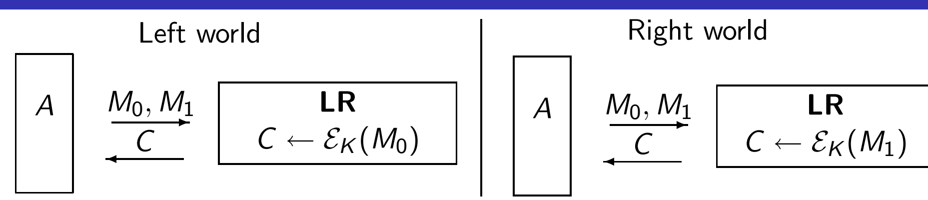
meaning $\mathcal{SE}$ is not IND-CPA secure.

Thus:

XOR-insecurity $\Rightarrow$ IND-CPA-insecurity

IND-CPA-security $\Rightarrow$ XOR-security

XOR-insecurity implies IND-CPA-insecurity



adversary A

- Makes two **LR** queries
- The left messages are $M_0^1 = 0^n$ and $M_0^2 = 0^n$.
  Why? Because $\text{lsb}(0^n) \oplus \text{lsb}(0^n) = 0$
- The right messages are $M_1^1 = 0^n$ and $M_1^2 = 1^n$.
  Why? Because $\text{lsb}(0^n) \oplus \text{lsb}(1^n) = 1$
- Gets back 2 ciphertexts C_1, C_2
- Runs $B(C_1, C_2)$ to compute $\text{lsb}(M_b^1) \oplus \text{lsb}(M_b^2)$ which equals b, indiciating whether Left or Right world

adversary A
$C_1 \leftarrow \mathbf{LR}(0^n, 0^n)$; $C_2 \leftarrow \mathbf{LR}(0^n, 1^n)$
$d \xleftarrow{\$} B(C_1, C_2)$; return d

XOR-insecurity implies IND-CPA-insecurity

Left world

A $\xrightarrow{M_0, M_1}$ **LR**: $C \leftarrow \mathcal{E}_K(M_0)$ $\xleftarrow{C}$

adversary A
$C_1 \leftarrow \mathbf{LR}(0^n, 0^n)\,;\; C_2 \leftarrow \mathbf{LR}(0^n, 1^n)$
$d \xleftarrow{\$} B(C_1, C_2)\,;\; \text{return } d$

What happens:

- $C_1 \xleftarrow{\$} \mathcal{E}_K(0^n)$ and $C_2 \xleftarrow{\$} \mathcal{E}_K(0^n)$
- The first bits of the encrypted messages XOR to 0
- so B returns 0

so

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

XOR-insecurity implies IND-CPA-insecurity

adversary A
$C_1 \leftarrow \mathbf{LR}(0^n, 0^n)\,;\; C_2 \leftarrow \mathbf{LR}(0^n, 1^n)$
$d \xleftarrow{\$} B(C_1, C_2)\,;\; \text{return } d$

Right world

A $\xrightarrow{M_0, M_1}$ **LR**: $C \leftarrow \mathcal{E}_K(M_1)$ $\xleftarrow{C}$

What happens:

- $C_1 \xleftarrow{\$} \mathcal{E}_K(0^n)$ and $C_2 \xleftarrow{\$} \mathcal{E}_K(1^n)$
- The first bits of the encrypted messages XOR to 1
- so B returns 1

so

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

XOR-insecurity implies IND-CPA-insecurity

So

$$\begin{aligned}\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) &= \Pr\left[\mathrm{Right}^A_{\mathcal{SE}} \Rightarrow 1\right] - \Pr\left[\mathrm{Left}^A_{\mathcal{SE}} \Rightarrow 1\right] \\ &= 1 - 0 \\ &= 1\end{aligned}$$

as claimed

Alternative formulation of advantage

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 $K \xleftarrow{\$} \mathcal{K}\,;\; b \xleftarrow{\$} \{0,1\}$	**procedure Finalize**(b') return $(b = b')$

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

Proof: Observe

$$\begin{aligned}\Pr\left[b' = 1 \mid b = 1\right] &= \Pr\left[\mathrm{Right}^A_{\mathcal{SE}} \Rightarrow 1\right] \\ \Pr\left[b' = 1 \mid b = 0\right] &= \Pr\left[\mathrm{Left}^A_{\mathcal{SE}} \Rightarrow 1\right]\end{aligned}$$

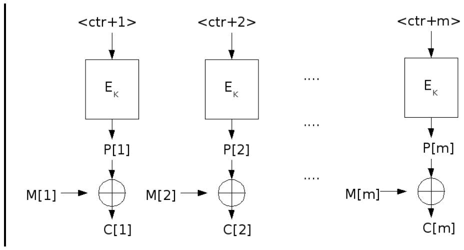
Proof (continued)

$$
\begin{aligned}
& \Pr\left[\mathrm{Guess}_{\mathcal{SE}}^{A} \Rightarrow \mathsf{true}\right] \\
&= \Pr\left[b = b'\right] \\
&= \Pr\left[b = b' \mid b = 1\right] \cdot \Pr\left[b = 1\right] + \Pr\left[b = b' \mid b = 0\right] \cdot \Pr\left[b = 0\right] \\
&= \Pr\left[b = b' \mid b = 1\right] \cdot \frac{1}{2} + \Pr\left[b = b' \mid b = 0\right] \cdot \frac{1}{2} \\
&= \Pr\left[b' = 1 \mid b = 1\right] \cdot \frac{1}{2} + \Pr\left[b' = 0 \mid b = 0\right] \cdot \frac{1}{2} \\
&= \Pr\left[b' = 1 \mid b = 1\right] \cdot \frac{1}{2} + \left(1 - \Pr\left[b' = 1 \mid b = 0\right]\right) \cdot \frac{1}{2} \\
&= \frac{1}{2} + \frac{1}{2} \cdot \left(\Pr\left[b' = 1 \mid b = 1\right] - \Pr\left[b' = 1 \mid b = 0\right]\right) \\
&= \frac{1}{2} + \frac{1}{2} \cdot \left(\Pr\left[\mathrm{Right}_{\mathcal{SE}}^{A} \Rightarrow 1\right] - \Pr\left[\mathrm{Left}_{\mathcal{SE}}^{A} \Rightarrow 1\right]\right) \\
&= \frac{1}{2} + \frac{1}{2} \cdot \mathbf{Adv}_{\mathcal{SE}}^{\mathrm{ind\text{-}cpa}}(A) .
\end{aligned}
$$

Security of CTRC

Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. Sender maintains a counter ctr, initially 0. The scheme is $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ where

Alg $\mathcal{E}_K(M)$
$C[0] \leftarrow$ ctr
for $i = 1, \ldots, m$ do
  $P[i] \leftarrow E_K(\langle ctr + i \rangle)$
  $C[i] \leftarrow P[i] \oplus M[i]$
$ctr \leftarrow ctr + m$
return C



Question: Is $\mathcal{SE}$ IND-CPA secure?

We cannot expect so if E is "bad". So, let's ask:

Question: Assuming E is good (a PRF) is $\mathcal{SE}$ IND-CPA secure?

IND-CPA security of CTRC

$\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ CTRC mode relative to block cipher E.

Question: If E is a PRF then is $\mathcal{SE}$ ind-cpa SECURE?

Answer: YES

And we can prove that the above answer is correct.

The above

- means CTRC has no "structural" weaknesses.
- Is not a triviality because it was not true for ECB.

Implications

Fact: If E is secure (PRF) then CTRC mode is a secure (IND-CPA) encryption scheme.

This means CTRC is a good, general purpose encryption scheme.

Ciphertexts leak NO partial information about messages.

Provides security regardless of message distribution. Votes can be securely encrypted.

We do not need to look for attacks on the scheme. We are guaranteed there are no attacks as long as E is secure.

Intuition for IND-CPA security of CTRC

Consider the CTRC scheme with E_K replaced by a random function **Fn**.

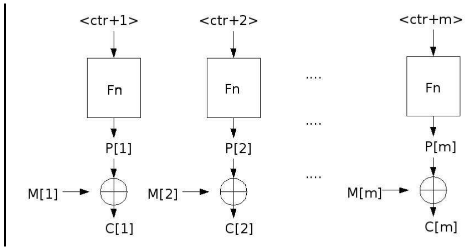
Alg $\mathcal{E}_{\mathbf{Fn}}(M)$ $C[0] \leftarrow$ ctr for $i = 1, \ldots, m$ do $\quad P[i] \leftarrow \mathbf{Fn}(\langle ctr + i \rangle)$ $\quad C[i] \leftarrow P[i] \oplus M[i]$ ctr $\leftarrow$ ctr + m return C	Alg $\mathcal{D}_{\mathbf{Fn}}(C)$ ctr $\leftarrow C[0]$ for $i = 1, \ldots, m$ do $\quad P[i] \leftarrow \mathbf{Fn}(\langle ctr + i \rangle)$ $\quad M[i] \leftarrow P[i] \oplus C[i]$ return M

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 the real CTRC is IND-CPA secure.

CTRC with a random function

Alg $\mathcal{E}_{\mathbf{Fn}}(M)$
$C[0] \leftarrow$ ctr
for $i = 1, \ldots, m$ do
$\quad P[i] \leftarrow \mathbf{Fn}(\langle ctr + i \rangle)$
$\quad C[i] \leftarrow P[i] \oplus M[i]$
$ctr \leftarrow ctr + m$
return C



Since **Fn** is random, the sequence $P[1] \cdots P[m]$ is random and the above is just one-time pad encryption, which is certainly IND-CPA secure.

So CTRC with a random function is IND-CPA secure.

IND-CPA security of CTRC

Theorem: Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a family of functions and let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be the corresponding CTRC mode symmetric encryption scheme. Let A be an ind-cpa adversary making at most q **LR** queries totalling at most σ blocks. Then there is a prf-adversary B such that

$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) \le 2 \cdot \mathbf{Adv}^{\text{prf}}_{E}(B).$$

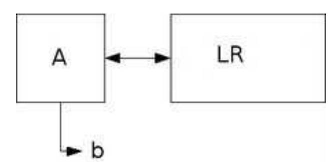
Furthermore B makes at most σ oracle queries and runs in time at most $t + \Theta(q + n\sigma)$.

Implication:

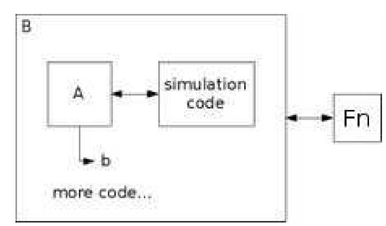
$$\begin{aligned} E \text{ a PRF} \quad &\Rightarrow \quad \mathbf{Adv}^{\text{prf}}_{E}(B) \text{ small} \\ &\Rightarrow \quad \mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A) \text{ small} \\ &\Rightarrow \quad \mathcal{SE} \text{ IND-CPA secure} \end{aligned}$$

Proof by reduction

A's world



B runs A, itself replying to A's oracle queries



Some notation

$\|M\|_n$ = number of n-bit blocks in M.

That is, $M = M[1]...M[m]$ where $m = \|M\|_n$.

$\langle j \rangle$ denotes the n-bit binary encoding of integer $j \in \{0, ..., 2^n - 1\}$.

Games for CTRC security proof

Game G_0

procedure Initialize
$K \xleftarrow{\$} \{0,1\}^k$; $b \xleftarrow{\$} \{0,1\}$
$ctr \leftarrow 0$

procedure LR(M_0, M_1)
$C[0] \leftarrow ctr$; $m \leftarrow \|M_b\|_n$
for $i = 1, ..., m$ do
  $P[\langle ctr + i \rangle] \leftarrow E_K(\langle ctr + i \rangle)$
  $C[i] \leftarrow P[\langle ctr + i \rangle] \oplus M_b[i]$
$ctr \leftarrow ctr + m$
return C

procedure Finalize(b')
return $(b = b')$

Game G_1

procedure Initialize
$b \xleftarrow{\$} \{0,1\}$; $ctr \leftarrow 0$

procedure LR(M_0, M_1)
$C[0] \leftarrow ctr$; $m \leftarrow \|M_b\|_n$
for $i = 1, ..., m$ do
  $P[\langle ctr + i \rangle] \xleftarrow{\$} \{0,1\}^n$
  $C[i] \leftarrow P[\langle ctr + i \rangle] \oplus M_b[i]$
$ctr \leftarrow ctr + m$
return C

procedure Finalize(b')
return $(b = b')$

Analysis

Claim 1: There is a prf-adversary B such that

$$\Pr\left[G_0^A \Rightarrow \text{true}\right] - \Pr\left[G_1^A \Rightarrow \text{true}\right] \leq \mathbf{Adv}_E^{\mathrm{prf}}(B).$$

adversary B
$b \xleftarrow{\$} \{0,1\}$; $ctr \leftarrow 0$;
$b' \xleftarrow{\$} A^{\mathbf{LR}}$
If $(b = b')$ then return 1
Else return 0

subroutine LR(M_0, M_1)
$C[0] \leftarrow ctr$; $m \leftarrow \|M_b\|_n$
for $i = 1, ..., m$ do
  $P[\langle ctr + i \rangle] \leftarrow \mathbf{Fn}(\langle ctr + i \rangle)$
  $C[i] \leftarrow P[\langle ctr + i \rangle] \oplus M_b[i]$
$ctr \leftarrow ctr + m$
return C

If $\mathbf{Fn} = E_K$ then B is providing A the environment of game G_0 so

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

If $\mathbf{Fn}$ is random then B is providing A the environment of game G_1 so

$$\Pr[\mathrm{Rand}_E^B \Rightarrow 1] = \Pr[G_1^A \Rightarrow \text{true}]$$

Analysis

Claim 1: There is a prf-adversary B such that

$$\Pr\left[G_0^A \Rightarrow \text{true}\right] - \Pr\left[G_1^A \Rightarrow \text{true}\right] \leq \mathbf{Adv}_E^{\mathrm{prf}}(B).$$

adversary B
  $b \xleftarrow{\$} \{0,1\}$; $ctr \leftarrow 0$;
  $b' \xleftarrow{\$} A^{\mathbf{LR}}$
  If $(b = b')$ then return 1
  Else return 0

subroutine LR(M_0, M_1)
  $C[0] \leftarrow ctr$; $m \leftarrow \|M_b\|_n$
  for $i = 1, ..., m$ do
    $P[\langle ctr + i \rangle] \leftarrow \mathbf{Fn}(\langle ctr + i \rangle)$
    $C[i] \leftarrow P[\langle ctr + i \rangle] \oplus M_b[i]$
  $ctr \leftarrow ctr + m$
  return C

Thus

$$\begin{aligned}\mathbf{Adv}_E^{\mathrm{prf}}(B) &= \Pr\left[\mathrm{Real}_E^B 1 \Rightarrow 1\right] - \Pr\left[\mathrm{Rand}_E^B \Rightarrow 1\right] \\ &= \Pr\left[G_0^A \Rightarrow \text{true}\right] - \Pr\left[G_1^A \Rightarrow \text{true}\right]\end{aligned}$$

which proves Claim 1.

Analysis

$$\Pr[G_0^A \Rightarrow \text{true}] = \Pr[G_1^A \Rightarrow \text{true}] + \underbrace{\left(\Pr[G_0^A \Rightarrow \text{true}] - \Pr[G_1^A \Rightarrow \text{true}]\right)}_{\leq \mathbf{Adv}_E^{\mathrm{prf}}(B)}$$

So,

$$\begin{aligned}\mathbf{Adv}_{\mathcal{SE}}^{\text{ind-cpa}}(A) &= 2 \cdot \Pr[G_0^A \Rightarrow \text{true}] - 1 \\ &\leq 2 \cdot \left(\Pr[G_1^A \Rightarrow \text{true}] + \mathbf{Adv}_E^{\mathrm{prf}}(B)\right) - 1 \\ &= 2 \cdot \mathbf{Adv}_E^{\mathrm{prf}}(B) + 2\Pr[G_1^A \Rightarrow \text{true}] - 1\end{aligned}$$

Claim 2: $\Pr[G_1^A \Rightarrow \text{true}] = \frac{1}{2}$

$$\text{So, } \mathbf{Adv}_{\mathcal{SE}}^{\text{ind-cpa}}(A) \leq 2 \cdot \mathbf{Adv}_E^{\mathrm{prf}}(B)$$

Proof of Claim 2 in CTRC analysis

Game G_1

procedure Initialize
$b \xleftarrow{\$} \{0,1\}$; $ctr \leftarrow 0$

procedure LR(M_0, M_1)
$C[0] \leftarrow ctr$; $m \leftarrow \|M_b\|_n$
for $i = 1, \ldots, m$ do
  $P[\langle ctr + i \rangle] \xleftarrow{\$} \{0,1\}^n$
  $C[i] \leftarrow P[\langle ctr + i \rangle] \oplus M_b[i]$
$ctr \leftarrow ctr + m$
return C

procedure Finalize(b')
return $(b = b')$

Game G_2

procedure Initialize
$b \xleftarrow{\$} \{0,1\}$; $ctr \leftarrow 0$

procedure LR(M_0, M_1)
$C[0] \leftarrow ctr$; $m \leftarrow \|M_0\|_n$
for $i = 1, \ldots, m$ do
  $C[i] \xleftarrow{\$} \{0,1\}^n$
return C

procedure Finalize(b')
return $(b = b')$

Claim 2: $\Pr[G_1^A \Rightarrow \text{true}] = \frac{1}{2}$.

Proof: **LR** in G_2 does not use bit b so

$$\Pr[G_1^A \Rightarrow \text{true}] = \Pr[G_2^A \Rightarrow \text{true}] = \frac{1}{2}.$$

IND-CPA security of CTRC

Theorem: Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a family of functions and let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be the corresponding CTRC mode symmetric encryption scheme. Let A be an ind-cpa adversary making at most q **LR** queries totalling at most σ blocks. Then there is a prf-adversary B such that

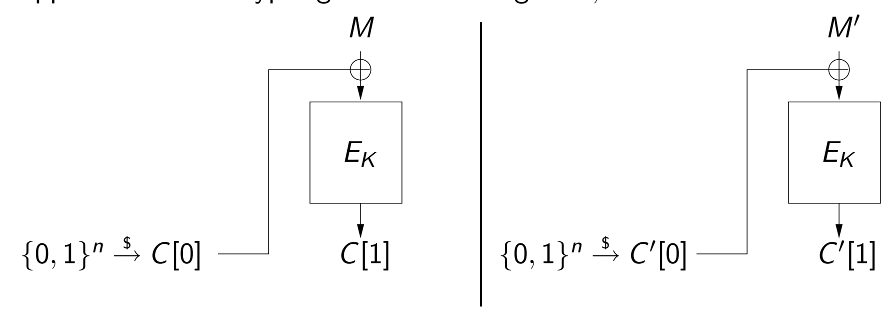
$$\mathbf{Adv}_{\mathcal{SE}}^{\text{ind-cpa}}(A) \leq 2 \cdot \mathbf{Adv}_E^{\mathrm{prf}}(B).$$

Furthermore B makes at most σ oracle queries and runs in time at most $t + \Theta(q + n\sigma)$.

Birthday attack on CBC$

Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. Let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be the CBC$ mode.

Suppose we are encrypting 1 block messages M, M' :



Observation: If $C[0] = C'[0]$ then

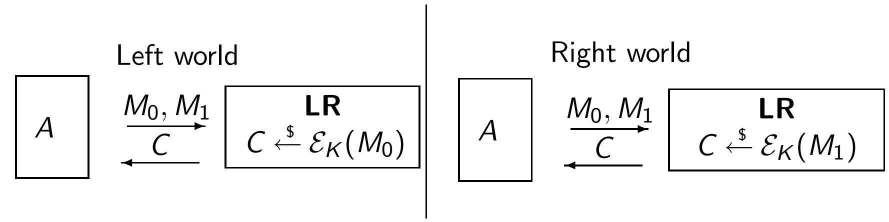
$$C[1] = C'[1] \text{ iff } M = M'$$

Birthday attack on CBC$

If 1 block messages are encrypted under CBC$, then message equality can be detected whenever the IVs are the same.

But if $\geq 2^{n/2}$ messages are encrypted, we expect by the birthday paradox to see collisions in IVs, so we will be able to break the scheme.

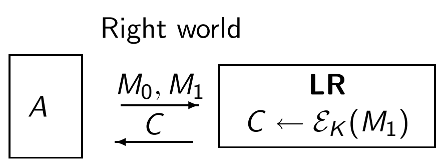
Birthday attack on CBC$



adversary A
  for $i = 1, \ldots, q$ do
    $C_i[0]C_i[1] \xleftarrow{\$} \mathbf{LR}(\langle i\rangle, \langle 0\rangle)$
  $S \leftarrow \{(j,\ell) \colon C_j[0] = C_\ell[0] \text{ and } 1 \leq j < \ell \leq q\}$
  If $S \neq \emptyset$, then
    $(j,\ell) \xleftarrow{\$} S$
    If $C_j[1] = C_\ell[1]$ then return 1
  return 0

Birthday attack on CBC$: Right world analysis

adversary A
for $i = 1, \ldots, q$ do
  $C_i[0]C_i[1] \xleftarrow{\$} \mathbf{LR}(\langle i\rangle, \langle 0\rangle)$
$S \leftarrow \{(j,\ell) \colon C_j[0] = C_\ell[0]$ and
    $1 \leq j < \ell \leq q\}$
If $S \neq \emptyset$, then
  $(j,\ell) \xleftarrow{\$} S$
  If $C_j[1] = C_\ell[1]$ then
    return 1
return 0



If $C_j[0] = C_\ell[0]$ then

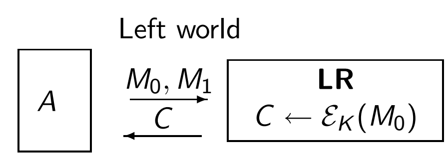
$$C_j[1] = E_K(\langle 0\rangle \oplus C_j[0]) = E_K(\langle 0\rangle \oplus C_\ell[0]) = C_\ell[1]$$

so

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

Birthday attack on CBC$: Left world analysis

adversary A
for $i = 1, \ldots, q$ do
  $C_i[0]C_i[1] \xleftarrow{\$} \mathbf{LR}(\langle i\rangle, \langle 0\rangle)$
$S \leftarrow \{(j,\ell) \colon C_j[0] = C_\ell[0]$ and
    $1 \leq j < \ell \leq q\}$
If $S \neq \emptyset$, then
  $(j,\ell) \xleftarrow{\$} S$
  If $C_j[1] = C_\ell[1]$ then
    return 1
return 0



If $C_j[0] = C_\ell[0]$ then

$$C_j[1] = E_K(\langle j\rangle \oplus C_j[0]) \neq E_K(\langle \ell\rangle \oplus C_\ell[0]) = C_\ell[1]$$

so

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

Birthday attack on CBC$

adversary A

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

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

$S \leftarrow \{(j, \ell) : C_j[0] = C_\ell[0]$ and $1 \le j < \ell \le q\}$

If $S \neq \emptyset$, then

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

  If $C_j[1] = C_\ell[1]$ then

    return 1

return 0

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

Birthday attack on CBC$

Conclusion: CBC$ 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 CBC$

So far: A q-query adversary can break CBC$ 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 σ 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 $q^2/2^n$.

Security of CBC$

Fact: If E is secure (PRF) then CBC$ mode can be used to securely encrypt up to $2^{n/2}$ blocks, where n is the block length of the block cipher.

This is not much for DES ($n = 64$, $2^{n/2} = 2^{32}$) but a lot for AES ($n = 128$, $2^{n/2} = 2^{64}$)

This means CBC$ is a good, general purpose encryption scheme.

Ciphertexts leak NO partial information about messages.

Provides security regardless of message distribution. Votes can be securely encrypted.

We do not need to look for attacks on the scheme. We are guaranteed there are no attacks as long as E is secure.

Security of CBC$

Theorem: 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 CBC$ 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 σ blocks. Then there is a prf-adversary B against E such that

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

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

Games for CBC$ Security Proof

Game G_0

procedure Initialize
$K \xleftarrow{\$} \{0,1\}^k$; $b \xleftarrow{\$} \{0,1\}$; $S \leftarrow \emptyset$

procedure LR(M_0, M_1)
$m \leftarrow \|M_b\|_n$; $C[0] \xleftarrow{\$} \{0,1\}^n$
for $i = 1, \ldots, n$ do
  $P \leftarrow C[i-1] \oplus M_b[i]$
  if $P \notin S$ then $\mathrm{T}[P] \leftarrow E_K(P)$
  $C[i] \leftarrow T[P]$
  $S \leftarrow S \cup \{P\}$
return C

procedure Finalize(b')
return $(b = b')$

Game G_1

procedure Initialize
$b \xleftarrow{\$} \{0,1\}$; $S \leftarrow \emptyset$

procedure LR(M_0, M_1)
$m \leftarrow \|M_b\|_n$; $C[0] \xleftarrow{\$} \{0,1\}^n$
for $i = 1, \ldots, n$ do
  $P \leftarrow C[i-1] \oplus M_b[i]$
  if $P \notin S$ then $\mathrm{T}[P] \xleftarrow{\$} \{0,1\}^n$
  $C[i] \leftarrow \mathrm{T}[P]$
  $S \leftarrow S \cup \{P\}$
return C

procedure Finalize(b')
return $(b = b')$

Security of CBC$

Then

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

But

$$\Pr\left[G_0^A \Rightarrow \text{true}\right] = \Pr\left[G_1^A \Rightarrow \text{true}\right] + \left(\Pr\left[G_0^A \Rightarrow \text{true}\right] - \Pr\left[G_1^A \Rightarrow \text{true}\right]\right)$$

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

$$\Pr\left[G_0^A \Rightarrow \text{true}\right] - \Pr\left[G_1^A \Rightarrow \text{true}\right] \le \mathbf{Adv}^{\text{prf}}_{E}(B)$$

Claim 2: $\Pr\left[G_1^A \Rightarrow \text{true}\right] \le \frac{1}{2} + \sigma^2 \cdot 2^{-n-1}$

So

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

Analysis

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

$$\Pr\left[G_0^A \Rightarrow \text{true}\right] - \Pr\left[G_1^A \Rightarrow \text{true}\right] \le \mathbf{Adv}^{\text{prf}}_{E}(B)$$

adversary B
$b \xleftarrow{\$} \{0,1\}$; $S \leftarrow \emptyset$
$b' \xleftarrow{\$} A^{\mathbf{LR}}$
if $(b = b')$ then return 1
else return 0

subroutine LR(M_0, M_1)
$m \leftarrow \|M_b\|_n$; $C[0] \xleftarrow{\$} \{0,1\}^n$
for $i = 1, \ldots, m$ do
  $P \leftarrow C[i-1] \oplus M_b[i]$
  if $P \notin S$ then $T[P] \leftarrow \mathbf{Fn}(P)$
  $C[i] \leftarrow T[P]$
  $S \leftarrow S \cup \{P\}$
return C

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

$$\Pr\left[\mathrm{Rand}_E^B \Rightarrow 1\right] = \Pr\left[G_1^A \Rightarrow \text{true}\right]$$

Analysis

Claim 2: $\Pr\left[G_1^A \Rightarrow \text{true}\right] \leq \frac{1}{2} + \frac{\sigma^2}{2^{n+1}}$

Introducing "bad"

Game G_1

procedure Initialize
$b \xleftarrow{\$} \{0,1\}$; $S \leftarrow \emptyset$

procedure LR(M_0, M_1)
$m \leftarrow \|M_b\|_n$; $C[0] \xleftarrow{\$} \{0,1\}^n$
for $i = 1, \ldots, n$ do
  $P \leftarrow C[i-1] \oplus M_b[i]$
  If $P \notin S$ then $\mathrm{T}[P] \xleftarrow{\$} \{0,1\}^n$
  $C[i] \leftarrow \mathrm{T}[P]$
  $S \leftarrow S \cup \{P\}$
return C

procedure Finalize(b')
return $(b = b')$

Game $\boxed{G_2}$, G_3

procedure Initialize
$b \xleftarrow{\$} \{0,1\}$; $S \leftarrow \emptyset$

procedure LR(M_0, M_1)
$m \leftarrow \|M_b\|_n$; $C[0] \xleftarrow{\$} \{0,1\}^n$
for $i = 1, \ldots, n$ do
  $P \leftarrow C[i-1] \oplus M_b[i]$
  $C[i] \xleftarrow{\$} \{0,1\}^n$
  If $P \in S$ then
    bad $\leftarrow$ true ; $\boxed{C[i] \leftarrow \mathrm{T}[P]}$
  $\mathrm{T}[P] \leftarrow C[i]$
  $S \leftarrow S \cup \{P\}$
return C

procedure Finalize(b')
return $(b = b')$

$$\Pr\left[G_1^A \Rightarrow \text{true}\right] = \Pr\left[G_2^A \Rightarrow \text{true}\right]$$

So far..

Claim 2: $\Pr[G_1^A \Rightarrow \text{true}] \leq \frac{1}{2} + \frac{\sigma^2}{2^{n+1}}$

$$\begin{aligned}\Pr[G_1^A \Rightarrow \text{true}] &= \Pr[G_2^A \Rightarrow \text{true}] \\ &= \Pr[G_3^A \Rightarrow \text{true}] + (\Pr[G_2^A \Rightarrow \text{true}] - \Pr[G_3^A \Rightarrow \text{true}])\end{aligned}$$

Will show:

- $\Pr[G_3^A \Rightarrow \text{true}] = \frac{1}{2}$
- $\Pr[G_2^A \Rightarrow \text{true}] - \Pr[G_3^A \Rightarrow \text{true}] \leq \frac{\sigma^2}{2^{n+1}}$

Analysis of G_3

Game G_3

procedure Initialize
$b \xleftarrow{\$} \{0,1\}$; $S \leftarrow \emptyset$

procedure Finalize(b')
return $(b = b')$

procedure LR(M_0, M_1)
$m \leftarrow \|M_b\|_n$; $C[0] \xleftarrow{\$} \{0,1\}^n$
for $i = 1, \ldots, n$ do
  $P \leftarrow C[i-1] \oplus M_b[i]$
  $C[i] \xleftarrow{\$} \{0,1\}^n$
  If $P \in S$ then bad $\leftarrow$ true
  $\mathrm{T}[P] \leftarrow C[i]$
  $S \leftarrow S \cup \{P\}$
return C

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

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

Fundamental Lemma of game playing

Games G, H are identical-until-bad if their code differs only in statements following the setting of bad to true.

Lemma: If G, H are identical-until-bad, then for any adversary A and any y

$$\left|\Pr\left[G^A \Rightarrow y\right] - \Pr\left[H^A \Rightarrow y\right]\right| \leq \Pr\left[H^A \text{ sets bad}\right]$$

Using the fundamental lemma

Game $\boxed{G_2}$, G_3

procedure Initialize
$b \xleftarrow{\$} \{0,1\}$; $S \leftarrow \emptyset$

procedure Finalize(b')
return $(b = b')$

procedure LR(M_0, M_1)
$m \leftarrow \|M_b\|_n$; $C[0] \xleftarrow{\$} \{0,1\}^n$
for $i = 1, \ldots, n$ do
  $P \leftarrow C[i-1] \oplus M_b[i]$
  $C[i] \xleftarrow{\$} \{0,1\}^n$
  If $P \in S$ then
    bad $\leftarrow$ true ; $\boxed{C[i] \leftarrow \mathrm{T}[P]}$
  $\mathrm{T}[P] \leftarrow C[i]$
  $S \leftarrow S \cup \{P\}$
return C

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

$$\Pr\left[G_2^A \Rightarrow \text{true}\right] - \Pr\left[G_3^A \Rightarrow \text{true}\right] \leq \Pr\left[G_3^A \text{ sets bad}\right].$$

Bounding the probability of bad in G_3

Game G_3

procedure Initialize
$b \xleftarrow{\$} \{0,1\}$; $S \leftarrow \emptyset$

procedure LR(M_0, M_1)
$m \leftarrow \|M_b\|_n$; $C[0] \xleftarrow{\$} \{0,1\}^n$
for $i = 1, \ldots, m$ do
  $P \leftarrow C[i-1] \oplus M_b[i]$
  $C[i] \xleftarrow{\$} \{0,1\}^n$
  If $P \in S$ then bad $\leftarrow$ true
  $\mathrm{T}[P] \leftarrow C[i]$
  $S \leftarrow S \cup \{P\}$
return C

procedure Finalize(b')
return $(b = b')$

Game G_4

procedure Initialize
$b \xleftarrow{\$} \{0,1\}$; $S \leftarrow \emptyset$

procedure LR(M_0, M_1)
$m \leftarrow \|M_0\|_n$
for $i = 1, \ldots, m$ do
  $P \xleftarrow{\$} \{0,1\}^n$
  $C[i-1] \leftarrow P \oplus M_b[i]$
  If $P \in S$ then bad $\leftarrow$ true
  $S \leftarrow S \cup \{P\}$
$C[m] \xleftarrow{\$} \{0,1\}^n$
return C

procedure Finalize(b')
return $(b = b')$

$$\Pr\left[G_3^A \text{ sets bad}\right] = \Pr\left[G_4^A \text{ sets bad}\right]$$

Bounding the probability of bad in G_4

The ℓ-th time the if-statement is executed, it has probability

$$\frac{\ell - 1}{2^n}$$

of setting bad. Thus

$$\begin{aligned}\Pr\left[G_4^A \text{ sets bad}\right] &\leq \sum_{\ell=1}^{\sigma} \frac{\ell-1}{2^n} \\ &= \frac{\sigma(\sigma-1)}{2^{n+1}} \\ &\leq \frac{\sigma^2}{2^{n+1}}\end{aligned}$$

How many LR queries?

The IND-CPA definition allows the adversary multiple queries to its LR oracle. This models the adversary distinguishing between whether the messages encrypted were one stream

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

or another stream

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

It turns out that allowing only one LR query captures the same security requirement up to a factor q in the advantage, as long as the adversary has a (plain) encryption oracle as well.

This can simplify analyses and the proof will illustrate the hybrid technique.

Find-then-guess

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

Game $\mathrm{FTGLeft}_{\mathcal{SE}}$	Game $\mathrm{FTGRight}_{\mathcal{SE}}$
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 $C \xleftarrow{\$} \mathcal{E}_K(M_1)$
procedure Enc(M)	**procedure Enc**(M)
return $C \xleftarrow{\$} \mathcal{E}_K(M)$	return $C \xleftarrow{\$} \mathcal{E}_K(M)$

Adversary B is allowed only one query to its LR oracle.

$$\mathbf{Adv}^{\mathrm{ftg}}_{\mathcal{SE}}(B) = \Pr\left[\mathrm{FTGRight}^B_{\mathcal{SE}} \Rightarrow 1\right] - \Pr\left[\mathrm{FTGLeft}^B_{\mathcal{SE}} \Rightarrow 1\right]$$

Find-then-guess

Proposition: Let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a symmetric encryption scheme and A an ind-cpa adversary making q oracle queries and having running time at most t. Then there is a ftg adversary B making one query to its LR oracle and q queries to its encryption oracle, such that

$$\mathbf{Adv}^{\mathrm{ind\text{-}cpa}}_{\mathcal{SE}}(A) \leq q \cdot \mathbf{Adv}^{\mathrm{ftg}}_{\mathcal{SE}}(B).$$

Furthermore, the running time of B is that of A.

Hybrid Technique: illustration

Suppose A makes queries

$$(M_0^1, M_1^1), (M_0^2, M_1^2), (M_0^3, M_1^3), (M_0^4, M_1^4)$$

Then we will define games G_0, G_1, G_2, G_3, G_4 so that

i	Messages encrypted in G_i^A
0	$M_1^1, M_1^2, M_1^3, M_1^4$
1	$M_0^1, M_1^2, M_1^3, M_1^4$
2	$M_0^1, M_0^2, M_1^3, M_1^4$
3	$M_0^1, M_0^2, M_0^3, M_1^4$
4	$M_0^1, M_0^2, M_0^3, M_0^4$

Hybrid Technique

Game G_i $(0 \le i \le q)$

procedure Initialize
$K \stackrel{\$}{\leftarrow} \mathcal{K}; \ell \leftarrow 0$

procedure LR(M_0, M_1)
$\ell \leftarrow \ell + 1$
If $\ell > i$ then $C \stackrel{\$}{\leftarrow} \mathcal{E}_K(M_1)$ else
$C \stackrel{\$}{\leftarrow} \mathcal{E}_K(M_0)$
Return C

Suppose A makes LR queries $(M_0^1, M_1^1), \ldots, (M_0^q, M_1^q)$. Then in G_i^A the messages encrypted are

$$M_0^1, \ldots, M_0^i, M_1^{i+1}, \ldots, M_1^q$$

Let

$$P_i = \Pr\left[G_i^A \Rightarrow 1\right].$$

Properties of the hybrid games

In G_0^A the messages encrypted are $M_1^1, \ldots, M_1^q$, so

$$\Pr\left[\mathrm{Right}_{\mathcal{SE}}^A \Rightarrow 1\right] = P_0.$$

In G_q^A the messages encrypted are $M_0^1, \ldots, M_0^q$, so

$$\Pr\left[\mathrm{Left}_{\mathcal{SE}}^A \Rightarrow 1\right] = P_q.$$

So,

$$\begin{aligned}\mathbf{Adv}_{\mathcal{SE}}^{\text{ind-cpa}}(A) &= P_0 - P_q \\ &= (P_0 - P_1) + (P_1 - P_2) + \ldots + (P_{q-1} - P_q)\end{aligned}$$

If $P_0 - P_q$ is large, so is at least one term in the sum. We design B to have advantage that term.

Design of B

adversary B
$\ell \leftarrow 0$
$g \stackrel{\$}{\leftarrow} \{1, \ldots, q\}$
$b' \stackrel{\$}{\leftarrow} A^{\mathrm{ELR}(\cdot,\cdot)}$
Return b'

subroutine ELR
$\ell \leftarrow \ell + 1$
If $\ell > g$ then $c \stackrel{\$}{\leftarrow} \mathcal{E}_K(M_1)$
If $\ell = g$ then $c \stackrel{\$}{\leftarrow}$ **LR**(M_0, M_1)
If $\ell < g$ then $c \stackrel{\$}{\leftarrow} \mathcal{E}_K(M_0)$

Suppose A's queries are $(M_0^1, M_1^1), \ldots, (M_0^q, M_1^q)$ and suppose B picks $g = i$. Then the messages encrypted are

$$M_0^1, \ldots, M_0^{i-1}, M_b^i, M_1^{i+1}, \ldots, M_1^q$$

so

$$\begin{aligned}\Pr\left[\mathrm{FTGRight}_{\mathcal{SE}}^B \Rightarrow 1 \mid g = i\right] &= P_{i-1} \\ \Pr\left[\mathrm{FTGLeft}_{\mathcal{SE}}^B \Rightarrow 1 \mid g = i\right] &= P_i\end{aligned}$$

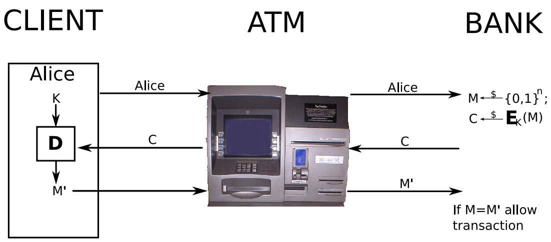
Analysis of B

$$\begin{aligned}\mathbf{Adv}_{\mathcal{SE}}^{\mathrm{ftg}}(B) &= \Pr\left[\mathrm{FTGRight}_{\mathcal{SE}}^B \Rightarrow 1\right] - \Pr\left[\mathrm{FTGLeft}_{\mathcal{SE}}^B \Rightarrow 1\right] \\ &= \sum_{i=1}^{q} \Pr\left[\mathrm{FTGRight}_{\mathcal{SE}}^B \Rightarrow \mid g = i\right] \cdot \Pr\left[g = i\right] \\ &\quad - \sum_{i=1}^{q} \Pr\left[\mathrm{FTGLeft}_{\mathcal{SE}}^B \Rightarrow 1 \mid g = i\right] \cdot \Pr\left[g = i\right] \\ &= \sum_{i=1}^{q} P_{i-1} \cdot \frac{1}{q} - \sum_{i=1}^{q} P_i \cdot \frac{1}{q} = \frac{1}{q} \sum_{i=1}^{q} (P_{i-1} - P_i) \\ &= \frac{1}{q}(P_0 - P_q) = \frac{1}{q} \mathbf{Adv}_{\mathcal{SE}}^{\text{ind-cpa}}(A)\end{aligned}$$

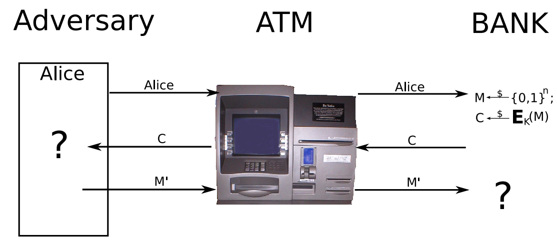
as desired.

Identification

ATM card contains a key $K \xleftarrow{\$} \mathcal{K}$ known also to Bank, where $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is a symmetric encryption scheme.

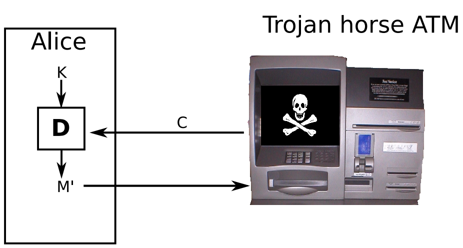


Attack Setting



Adversary transmits Alice's identity, but how can it answer the challenge (meaning decrypt C) without knowing Alice's key?

Active Attack

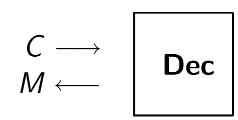


Tries to get K or learn how to decrypt by creating ciphertexts and getting the card to decrypt them.

This is called a chosen ciphertext attack.

Chosen-ciphertext attacks

New capability: Adversary has access to a decryption oracle



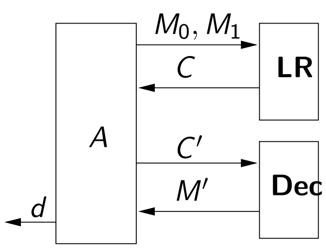
What is the adversary's goal?

In our example it was to get the key K, but based on the principles we have discussed before we would like to ask for more: no partial information on un-decrypted messages is leaked by the ciphertexts.

ind-cca adversaries

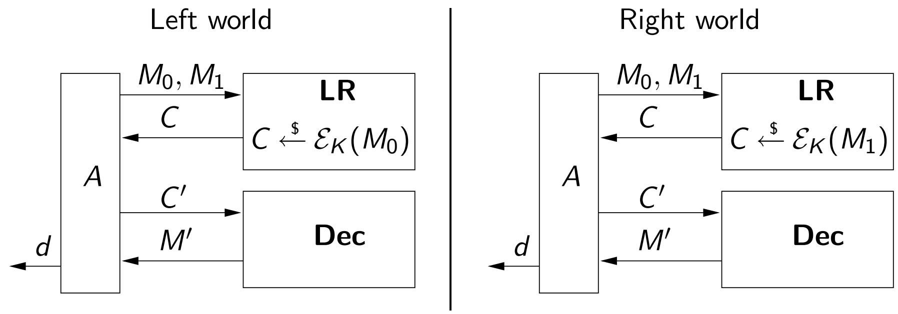
Let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme. An ind-cca adversary A

- Has access to a **LR** oracle
- Has access to a decryption oracle **Dec**
- Outputs a bit



IND-CCA

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



A's output d	Intended meaning: I think I am in the
1	Right world
0	Left world

The harder it is for A to guess world it is in, the more "secure" $\mathcal{SE}$ is as an encryption scheme.

The games

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

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 $C \xleftarrow{\$} \mathcal{E}_K(M_1)$
procedure Dec(C)	**procedure Dec**(C)
return $M \leftarrow \mathcal{D}_K(C)$	return $M \leftarrow \mathcal{D}_K(C)$

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-cca) advantage of A is

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

A problem

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 $C \xleftarrow{\$} \mathcal{E}_K(M_1)$
procedure Dec(C)	**procedure Dec**(C)
return $M \leftarrow \mathcal{D}_K(C)$	return $M \leftarrow \mathcal{D}_K(C)$

We can ALWAYS design A with advantage 1, meaning ALL schemes are insecure.

adversary A
$C \xleftarrow{\$}$ **LR**$(0^n, 1^n)$; $M \leftarrow$ **Dec**(C)
if $M = 0^n$ then return 0 else return 1

Then

$$\Pr\left[\mathrm{Left}_{\mathcal{SE}}^{A} \Rightarrow 1\right] = 0 \quad \Big| \quad \Pr\left[\mathrm{Right}_{\mathcal{SE}}^{A} \Rightarrow 1\right] = 1$$

Avoiding the problem

Encryption can only hide information about un-decrypted messages!

We address this by making the following rule:

- An ind-cca adversary A is not allowed to query **Dec** on a ciphertext previously returned by **LR**

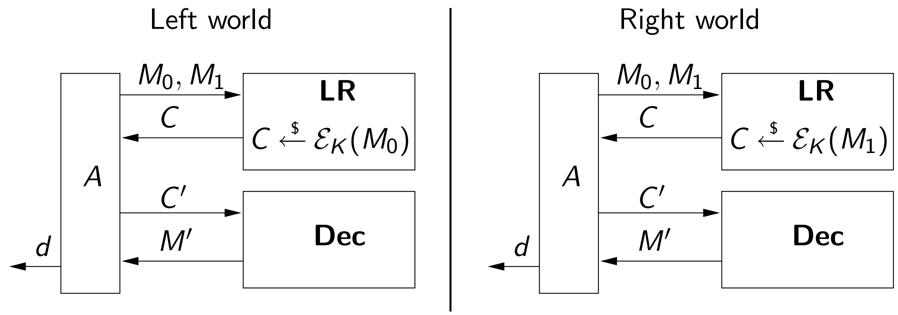
Adversary from before breaks rule:

adversary A
$C \xleftarrow{\$} \mathbf{LR}(0^n, 1^n)$; $M \leftarrow \mathbf{Dec}(C)$
if $M = 0^n$ then return 0 else return 1

IND-CCA attack on CBC\$

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

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



Can we design A so that

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

is close to 1?

IND-CCA attack on CBC\$

What we would like to do:

adversary A
$C \xleftarrow{\$} \mathbf{LR}(0^n, 1^n)$; $M \leftarrow \mathbf{Dec}(C)$
if $M = 0^n$ then return 0 else return 1

but querying C is not allowed. Instead we will

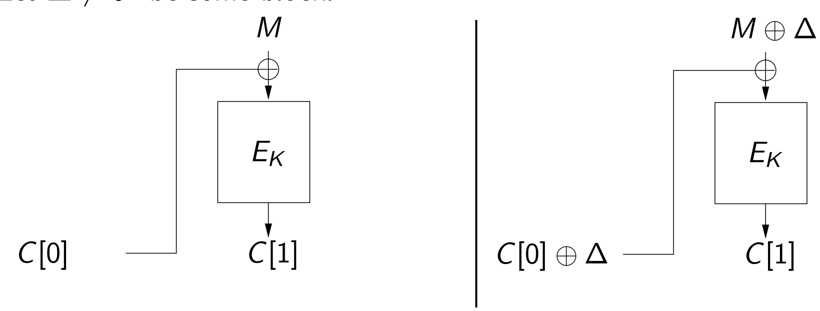
$$C \to \boxed{\text{ModifyC}} \to C' \to \boxed{\mathbf{Dec}} \to M' \to \boxed{\text{ModifyM}} \to M$$

so that $M = \mathcal{D}_K(C)$ but $C' \neq C$. Then

adversary A
$C \xleftarrow{\$} \mathbf{LR}(0^n, 1^n)$
$C' \leftarrow \text{ModifyC}(C)$; $M' \leftarrow \mathbf{Dec}(C')$; $M \leftarrow \text{ModifyM}(M')$
if $M = 0^n$ then return 0 else return 1

The Modify process

Let $\Delta \neq 0^n$ be some block.



$$C[0]C[1] \to \boxed{\begin{array}{c}\text{ModifyC}\\ C'[0] \leftarrow C[0] \oplus \Delta\end{array}} \to C'[0]C[1]$$

$$C'[0]C[1] \to \boxed{\mathbf{Dec}} \to M' = M \oplus \Delta$$

$$M' \to \boxed{\begin{array}{c}\text{ModifyM}\\ M \leftarrow M' \oplus \Delta\end{array}} \to M$$

IND-CCA attack on CBC\$: Right world analysis

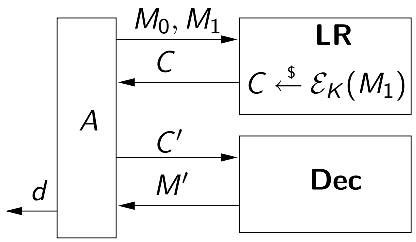
adversary A
$C[0]C[1] \xleftarrow{\$} \mathbf{LR}(0^n, 1^n)\,;\ \Delta \leftarrow 1^n$
$C'[0] \leftarrow C[0] \oplus \Delta\,;\ M' \leftarrow \mathbf{Dec}(C'[0]C[1])\,;\ M \leftarrow M' \oplus \Delta$
if $M = 0^n$ then return 0 else return 1

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

procedure Initialize
$K \xleftarrow{\$} \mathcal{K}$

procedure LR(M_0, M_1)
Return $C \xleftarrow{\$} \mathcal{E}_K(M_0)$

procedure Dec(C)
return $M \leftarrow \mathcal{D}_K(C)$



Then

$$\Pr\left[\mathrm{Right}_{\mathcal{SE}}^{A} \Rightarrow 1\right] = 1$$

because $C[0]C[1] \xleftarrow{\$} \mathcal{E}_K(1^n)$ so $M = 1^n \neq 0^n$.

IND-CCA attack on CBC\$: Left world analysis

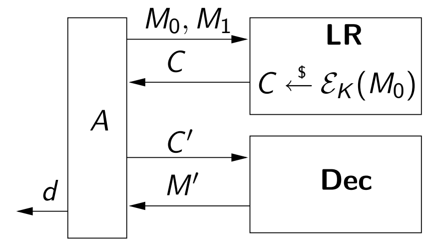
adversary A
$C[0]C[1] \xleftarrow{\$} \mathbf{LR}(0^n, 1^n)\,;\ \Delta \leftarrow 1^n$
$C'[0] \leftarrow C[0] \oplus \Delta\,;\ M' \leftarrow \mathbf{Dec}(C'[0]C[1])\,;\ M \leftarrow M' \oplus \Delta$
if $M = 0^n$ then return 0 else return 1

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

procedure Initialize
$K \xleftarrow{\$} \mathcal{K}$

procedure LR(M_0, M_1)
Return $C \xleftarrow{\$} \mathcal{E}_K(M_0)$

procedure Dec(C)
return $M \leftarrow \mathcal{D}_K(C)$



Then

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

because $C[0]C[1] \xleftarrow{\$} \mathcal{E}_K(1^n)$ so $M = 0^n$.

IND-CCA attack on CBC

adversary A
$C[0]C[1] \xleftarrow{\$} \mathbf{LR}(0^n, 1^n)\,;\ \Delta \leftarrow 1^n$
$C'[0] \leftarrow C[0] \oplus \Delta\,;\ M' \leftarrow \mathbf{Dec}(C'[0]C[1])\,;\ M \leftarrow M' \oplus \Delta$
if $M = 0^n$ then return 0 else return 1

$$\begin{aligned}\mathbf{Adv}_{\mathcal{SE}}^{\mathrm{ind\text{-}cca}}(A) &= \overbrace{\Pr\left[\mathrm{Right}_{\mathcal{SE}}^{A} \Rightarrow 1\right]}^{1} - \overbrace{\Pr\left[\mathrm{Left}_{\mathcal{SE}}^{A} \Rightarrow 1\right]}^{0}\\ &= 1\end{aligned}$$

And A is very efficient, making only two queries.

Thus CBC\$ is **not** IND-CCA secure.

Protecting against CCAs

Can you think of a way to design a scheme that is IND-CCA secure?

We will see such a scheme later, after we have some more tools.