Symmetric-Key Encryption

CS 466: Applied Cryptography

Adam O’Neill

Adapted from http://cseweb.ucsd.edu/~mihir/cse107/

Setting the Stage

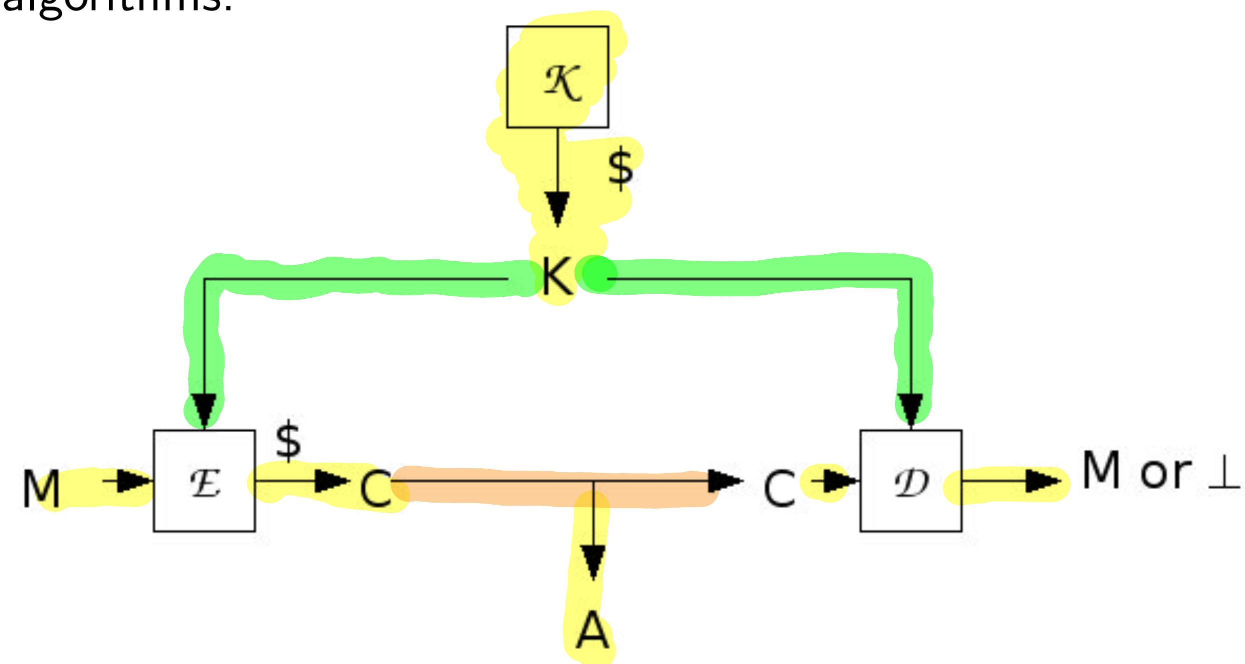
- We have studied our first lower-level primitive, blockciphers.

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.

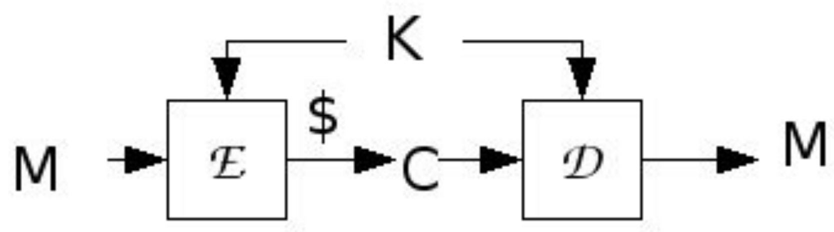
Syntax

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

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

K & M are fixed

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

A scheme will usually specify an associated message space.

Blockcipher Modes of Operation

assume msg length is multiple of block length.

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

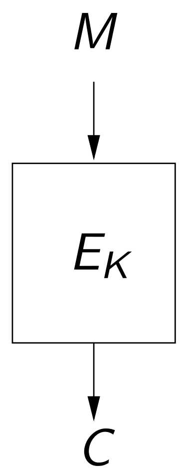
Notation: $x[i]$ is the i-th n-bit block of a string x, so that $x = x[1] \ldots x[m]$ if $|x| = nm$.

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.

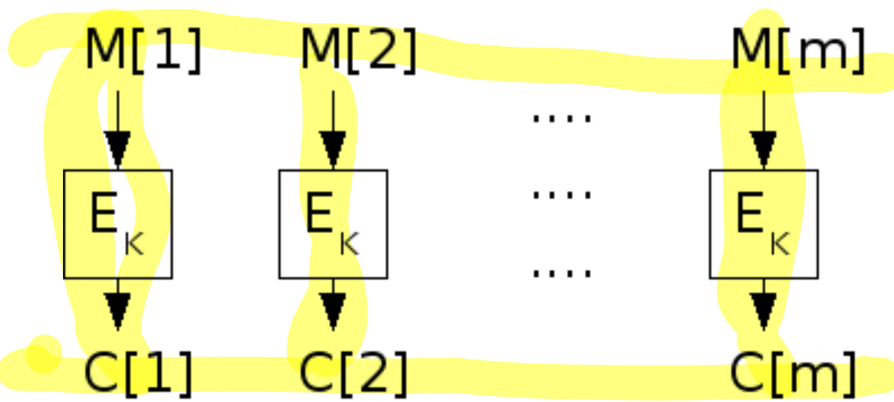
How do we encrypt a long message using a primitive that only applies to n-bit blocks?

Electronic Codebook Mode

(ECB)

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

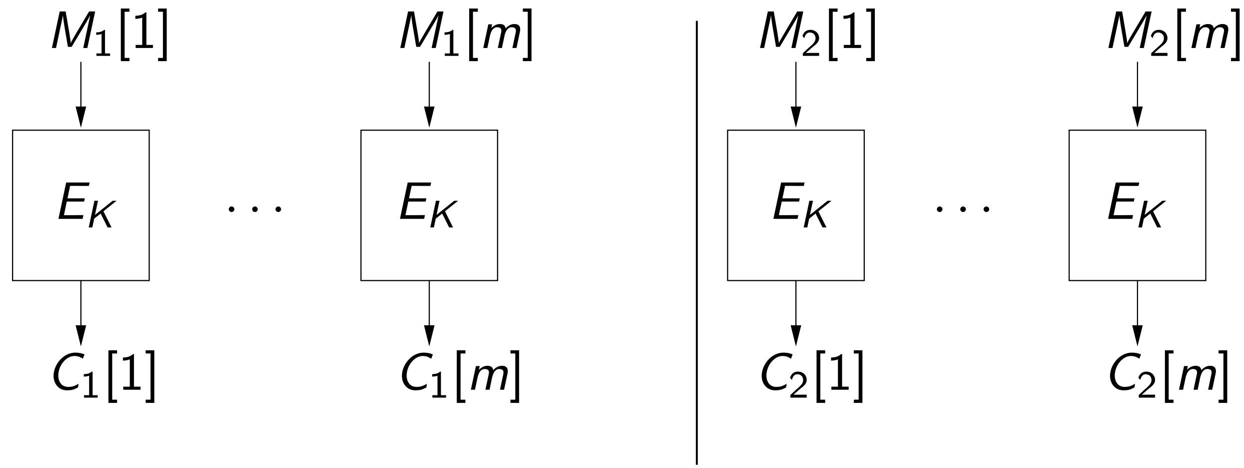
Alg $\mathcal{E}_K(M)$	**Alg** $\mathcal{D}_K(C)$
for $i = 1, \ldots, m$ do	for $i = 1, \ldots, m$ do
$\quad C[i] \leftarrow E_K(M[i])$	$\quad M[i] \leftarrow E_K^{-1}(C[i])$
return C	return M



Weakness of ECB

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

Why is the above true? Because E_K is deterministic:



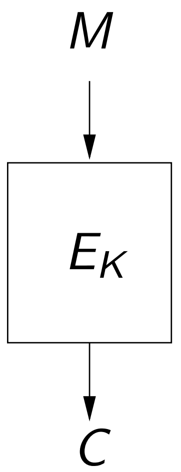
Why does this matter?

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?

Even if $M_1 = M_2$
it need not be the case
that $C_1 = C_2$.

[GM '84]

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

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

$M_1 = M_2$

then

$$Pr[C_1 = C_2]$$

small !!!

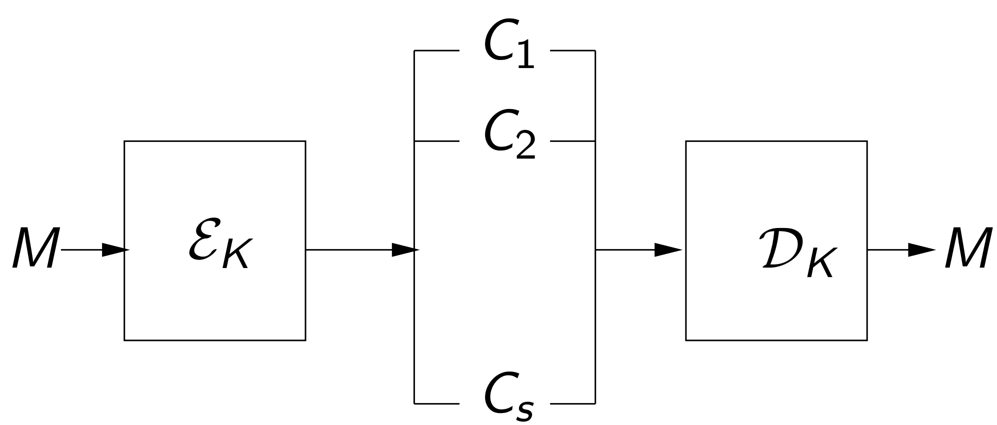
will (should) be small, where the probability is over the coins of $\mathcal{E}$.

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.

Mode of operation

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

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

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

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

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

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

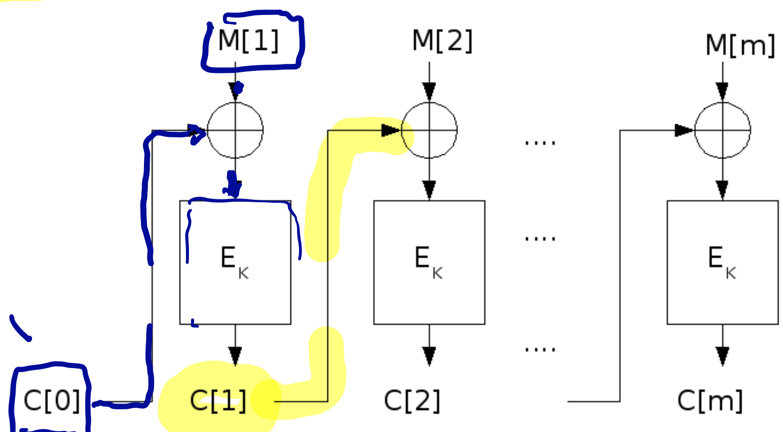
return C

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

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

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

return M



initialization vector "IV"

Correct decryption relies on E being a block cipher.

CTR-\$ Mode

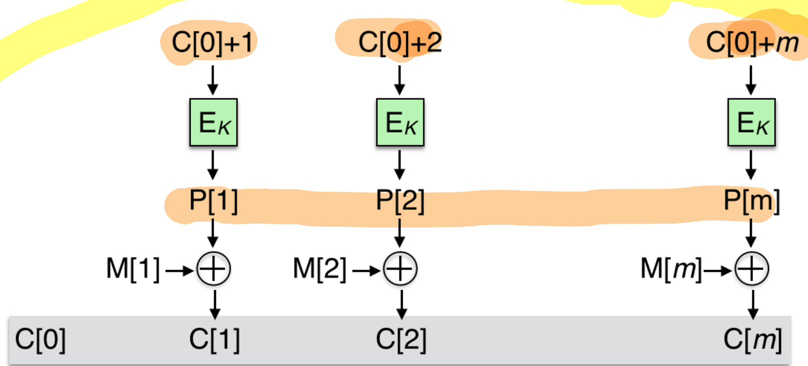
Let $E\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^\ell$ be a family of functions. If $X \in \{0,1\}^n$ and $i \in \mathbf{N}$ then $X + i$ denotes the n-bit string formed by converting X to an integer, adding i modulo 2^n, and converting the result back to an n-bit string. Below the message is a sequence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



pseudo one-time pad.

A simple way to encrypt a long message with a short key.

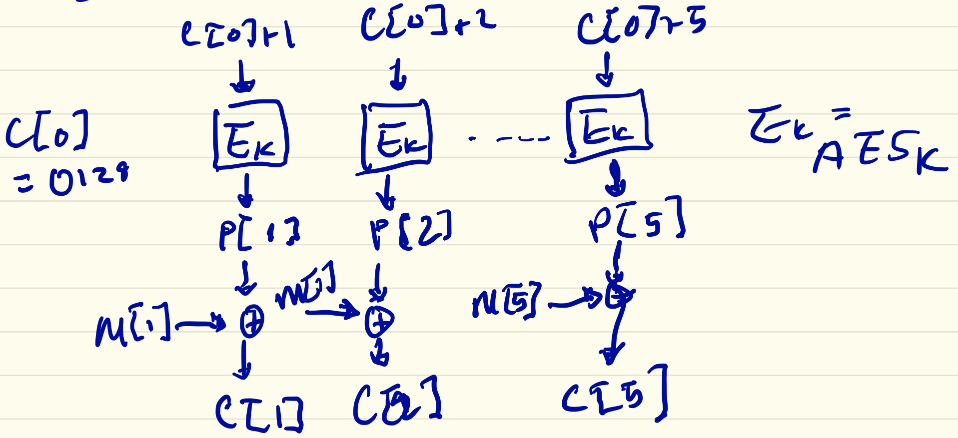
$$M = M[1]M[2]\ldots M[5]$$

$$M[i] \in \{0,1\}^{128}$$

$$K \in \{0,1\}^{128}$$

Question: how to use K to encrypt M if K will never be used again?

Answer: Use simplified version of CTR mode where $C[0] = 0^{128}$.



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

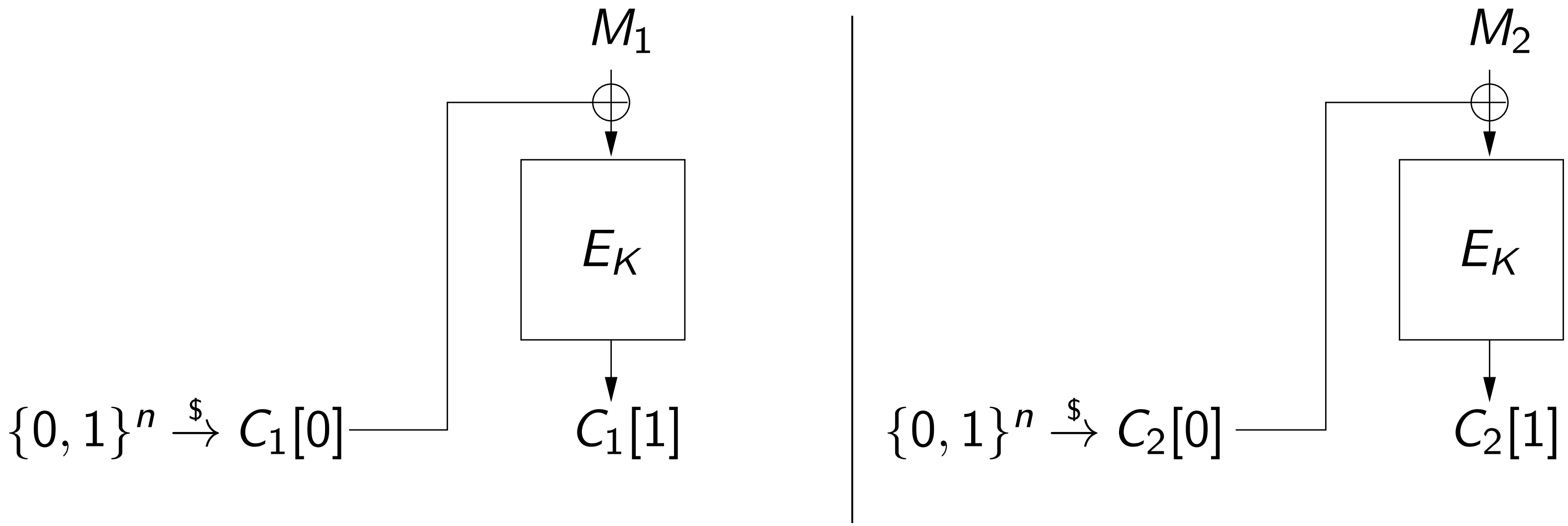
Alg $\mathcal{D}_K(C)$

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

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

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?

joint functions of the data

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 $1 \leq i \leq q$. 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.

1: "I'm in the Right game"

0: I'm in the Left game

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

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

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

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

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

Adaptive attack!

Message length restriction

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.

Query (m_0, m_1)

$|m_0| = |m_1|$

lengths of messages can vary across queries

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 ≤ 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?

$(0^n, 0^n)$ = query 1

$(1^n, 0^n)$ = query 2

left stream

right stream

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

legitimate adversary:

$|0^n| = |0^n|$

$|1^n| = |0^n|$

(x_1, x_2) (x_3, x_4) $x_1 \neq x_2 \neq x_3 \neq x_4$

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

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

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

Then

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

by def of blockcipher

$E_K(0^n) = E_K(0^n)$ since E is deterministic.

Left Game Analysis

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

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

procedure Initialize

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

procedure LR(M_0, M_1)

Return $\mathcal{E}_K(M_0)$

Then

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

$E_K(0^n) \neq E_K(1^n)$ since E_K is a perm.

$\mathcal{E}_K(0^n) \neq \mathcal{E}_K(1^n)$ by correctness of $\mathcal{E}_K$.

Conclusion

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

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

And A is very efficient, making only two queries.

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

Other Attacks?

- Can you find an attack where all messages queried to the LR oracle (counting both sides) are distinct?

Adversary A'

$c_1 \leftarrow LR(0^n 1^n, 0^n 0^n)$

$c_2 \leftarrow LR(1^n 0^n, 1^n 1^n)$

If $c_1[0] = c_2[1]$ ret 0

Else ret 1

Advantage:

$\mathrm{Adv}_{SE}^{\text{ind-cpa}}(A) =$

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

$- \Pr[\mathrm{LEFT}_{SE}^{A} \Rightarrow 1]$

Claim $\Pr[\mathrm{RIGHT}_{SE}^{A} \Rightarrow 1] = 1$.

proof:

$c_1[0] = E_K(0^n) \neq E_K(1^n)$

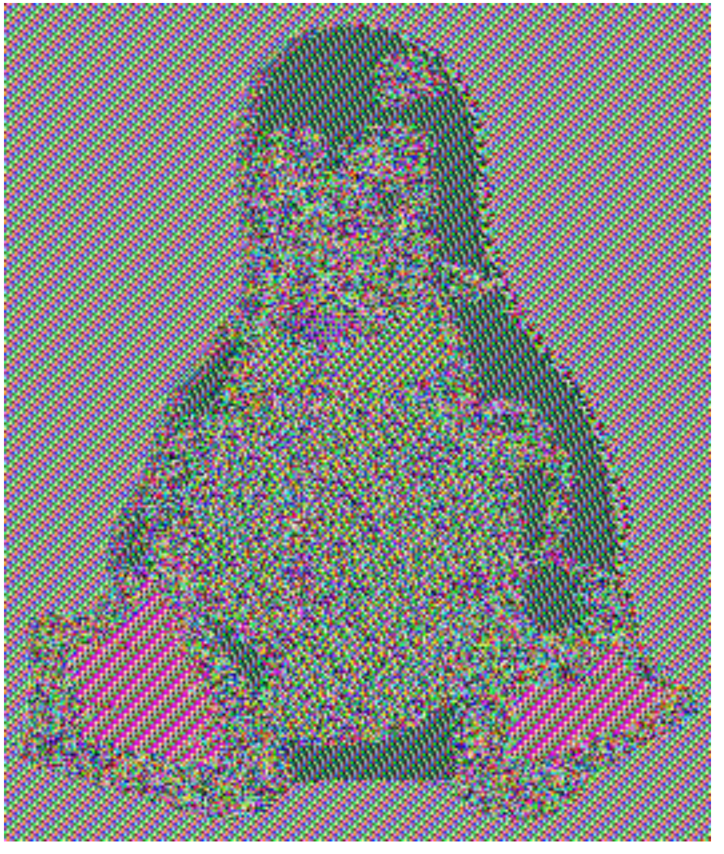
$= c_2[1]$

by def of blockcipher. ✓

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

running-time: 2 LR queries $+ O(n)$

ECB Penguin



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 $C_1 \stackrel{\$}{\leftarrow} \mathcal{E}_K(M_1)$ and $C_2 \stackrel{\$}{\leftarrow} \mathcal{E}_K(M_2)$ the adversary cannot

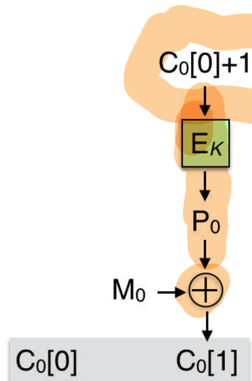
- get M_1
- get 1st bit of M_1
- get XOR of the 1st bits of M_1, M_2
- etc.

IV $\quad$ IV+1 $\quad \boxed{E_K} \cdots \boxed{E_K}$ $\quad$ IV+n

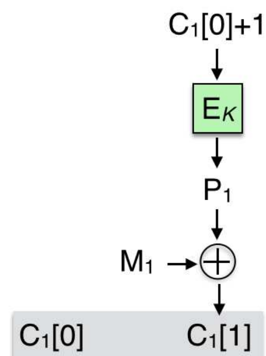
Security Analysis of CTR-$

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

If $C_0[1] = C_1[1]$ then $\left.\begin{matrix} E_K(x+1) \oplus M_0 \\ E_K(x+1) \oplus M_1 \end{matrix}\right\} =$ iff $M_0 = M_1$

$:= x$

The Adversary

q-query birthday attack adversary

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

IND-CPA adversary

adversary A

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

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

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

If $S \neq \emptyset$, then

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

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

return 0

1	0
2	0
$\vdots$	0
$\vdots$	$\vdots$
q	0

will discuss in detail next lecture

Right Game Analysis

adversary A

for $i = 1, \ldots, q$ do
  $C^i[0]C^i[1] \xleftarrow{\$} \mathbf{LR}(\langle i\rangle, \langle 0\rangle)$
$S \leftarrow \{(j,t)\colon C^j[0] = C^t[0] \text{ and } j < t\}$
If $S \neq \emptyset$, then
  $(j,t) \xleftarrow{\$} S$
  If $C^j[1] = C^t[1]$ then return 1
return 0

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

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

so

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

c(n, q) is the probability of a collison when choosing q items at random from domain of size n.

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

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

equal

unequal

so

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

not lucky → always outputs 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.

Excercise

The above attack on CTR\$ uses 1-block messages. Letting $\mathcal{SE}$ be the same scheme, give an adversary A that makes q **LR**-queries, each consisting of two m-block messages, and achieves

$$\mathbf{Adv}^{\mathrm{ind\text{-}cpa}}_{\mathcal{SE}}(A) = \Omega\left(\frac{mq^2}{2^n}\right)$$

The running time of A should be about $\mathcal{O}(mq(n+\ell) \cdot \log(mq(n+\ell)))$.

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 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 $q^2/2^n$.

For $E = \text{AES}$ 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 σ blocks. Then there is a prf-adversary B against E such that

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

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

Intuition

- 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).

Theorem for CBC-$

Theorem: [BDJR97] 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, the messages across them totaling at most σ blocks. Then there is a prf-adversary B against E such that

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

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

Exercise

You are hired at a top company with an extravagant salary. Your boss asks you how secure is CBC$ based on AES. Give a clear and full answer which includes an explanation of security metrics, their relative merits, attacks and proofs. This should include an interpretation of the theorem we just saw. Your description should cover both the value and the limitations of this theorem and give a realistic picture of security aimed at someone with little understanding of cryptography.

Regarding note on run-time
(on course website)

Symbolic	Asymptotic
T_{AES}	XOR
T_G, T_F	string comp.
	bit-wise comp.

Adversary A // PRF
// adversary

Choose $m_1, m_2 \in \{0,1\}^{128}$
arbitrarily

$c_1 \leftarrow F_n(m_1)$

$c_2 \leftarrow F_n(m_2)$

$c_1' \leftarrow AES_{m_1}(c_1)$

$c_2' \leftarrow AES_{m_2}(c_2)$

If $c_2' \oplus c_1' = 0^{128}$

ret 1

else ret 0

2 F_n queries + $2T_{AES}$ + $O(\ell)$. where
$\ell = 128$ for AES.

* Do NOT count computation <u>inside</u> <u>an</u> <u>oracle</u> in running-time of an adversary