

Security Notions

Pascal Lafourcade

Université Joseph Fourier, Verimag

3rd December 2009

Last Time

- ▶ Symetric Encryption
- ▶ Encryption Modes
- ▶ Diffie-Hellman
- ▶ Hash Functions
- ▶ Applications

Outline

Different Adversaries

Outline

Different Adversaries

Intuition of Computational Security

Outline

Different Adversaries

Intuition of Computational Security

Definitions of Computational Security

Outline

Different Adversaries

Intuition of Computational Security

Definitions of Computational Security

Examples

- RSA

- ElGamal

Outline

Different Adversaries

Intuition of Computational Security

Definitions of Computational Security

Examples

- RSA

- EIGamal

Famous Example OAEP

Outline

Different Adversaries

Intuition of Computational Security

Definitions of Computational Security

Examples

- RSA

- EIGamal

Famous Example OAEP

Attack on ECB

Outline

Different Adversaries

Intuition of Computational Security

Definitions of Computational Security

Examples

- RSA

- ElGamal

Famous Example OAEP

Attack on ECB

Conclusion

Outline

Different Adversaries

Intuition of Computational Security

Definitions of Computational Security

Examples

- RSA

- ElGamal

Famous Example OAEP

Attack on ECB

Conclusion

Which adversary?



Adversary Model

Qualities of the adversary:

- ▶ **Clever:** Can perform all operations he wants
- ▶ **Limited time:**
 - ▶ Do not consider attack in 2^{60} .
 - ▶ Otherwise a Brute force by enumeration is always possible.

Model used: **Any Turing Machine.**

- ▶ Represents all possible algorithms.
- ▶ Probabilistic: adversary can generate keys, random number...

Adversary Models

The adversary is given access to oracles :

- encryption of all messages of his choice
- decryption of all messages of his choice

Three classical security levels:

- ▶ Chosen-Plain-text Attacks (CPA)
- ▶ Non adaptive Chosen-Cipher-text Attacks (CCA1)
only before the challenge
- ▶ Adaptive Chosen-Cipher-text Attacks (CCA2)
unlimited access to the oracle (except for the challenge)



Chosen-Plain-text Attacks (CPA)



Adversary can obtain all cipher-texts from any plain-texts.
It is always the case with a Public Encryption scheme.

Non adaptive Chosen-Cipher-text Attacks (CCA1)



Adversary knows the public key, has access to a **decryption oracle multiple times before to get the challenge** (cipher-text), also called “Lunchtime Attack” introduced by M. Naor and M. Yung ([NY90]).

Adaptive Chosen-Cipher-text Attacks (CCA2)



Adversary knows the public key, has access to a **decryption oracle multiple times before and AFTER to get the challenge**, but of course cannot decrypt the challenge (cipher-text) introduced by C. Rackoff and D. Simon ([RS92]).

Summary of Adversaries

CCA2: $\mathcal{O}_1 = \mathcal{O}_2 = \{\mathcal{D}\}$ Adaptive Chosen Cipher text Attack



CCA1: $\mathcal{O}_1 = \{\mathcal{D}\}$, $\mathcal{O}_2 = \emptyset$ Non-adaptive Chosen Cipher-text Attack



CPA: $\mathcal{O}_1 = \mathcal{O}_2 = \emptyset$ Chosen Plain text Attack



Outline

Different Adversaries

Intuition of Computational Security

Definitions of Computational Security

Examples

RSA

ElGamal

Famous Example OAEP

Attack on ECB

Conclusion

One-Wayness (OW)

Put your message in a translucent bag, but you cannot read the text.



One-Wayness (OW)

Put your message in a translucent bag, but you cannot read the text.



Without the private key, it is computationally **impossible to recover the plain-text.**

Is it secure ?



Is it secure ?



Is it secure ?



- ▶ you cannot read the text but you can distinguish which one has been encrypted.

Is it secure ?



- ▶ you cannot read the text but you can distinguish which one has been encrypted.
- ▶ Does not exclude to recover half of the plain-text
- ▶ Even worse if one has already partial information of the message:
 - ▶ Subject: XXXX
 - ▶ From: XXXX

Indistinguishability (IND)

Put your message in a black bag, you can not read anything.



Now a black bag is of course IND and it implies OW.

Indistinguishability (IND)

Put your message in a black bag, you can not read anything.



Now a black bag is of course IND and it implies OW.

The adversary is not able to **guess in polynomial-time even a bit of the plain-text knowing the cipher-text**, notion introduced by S. Goldwasser and S.Micali ([GM84]).

Is it secure?



Is it secure?



Is it secure?



- ▶ It is possible to scramble it in order to produce a new cipher. In more you know the relation between the two plain text because you know the moves you have done.

Non Malleability (NM)

Put your message in a black box.



But in a black box you cannot touch the cube (message), hence NM implies IND.

Non Malleability (NM)

Put your message in a black box.



But in a black box you cannot touch the cube (message), hence NM implies IND.

The adversary should **not be able to produce a new cipher-text** such that the plain-texts are meaningfully related, notion introduced by D. Dolev, C. Dwork and M. Naor in 1991 ([DDN91,BDPR98,BS99]).

Summary of Security Notions

Non Malleability



Indistinguishability



One-Wayness



Outline

Different Adversaries

Intuition of Computational Security

Definitions of Computational Security

Examples

RSA

ElGamal

Famous Example OAEP

Attack on ECB

Conclusion

Asymmetric Encryption

An asymmetric encryption scheme $\mathcal{S} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is defined by

- ▶ \mathcal{K} : **key generation**
- ▶ \mathcal{E} : **encryption**
- ▶ \mathcal{D} : **decryption**

$$\mathcal{K}(\eta) = (k_e, k_d)$$

$$\mathcal{E}_{k_e}(m, r) = c$$

$$\mathcal{D}(c, k_d) = m$$

One-Wayness (OW)

Adversary \mathcal{A} : any polynomial time Turing Machine (PPTM)

Basic security notion: One-Wayness (OW)



Without the private key, it is computationally impossible to recover the plain text:

$$\Pr_{m,r}[\mathcal{A}(c) = m \mid c = E(m, r)]$$

is negligible.

Indistinguishability (IND)



Game Adversary: $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$

1. The adversary \mathcal{A}_1 is given the public key pk .
2. The adversary \mathcal{A}_1 chooses two messages m_0, m_1 .
3. $b = 0, 1$ is chosen at random and $c = E(m_b)$ is given to the adversary.
4. The adversary \mathcal{A}_2 answers b' .

The probability $Pr[b = b'] - \frac{1}{2}$ should be negligible.

The IND-CPA Games



Given an encryption scheme $\mathcal{S} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$. An adversary is a pair $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ of polynomial-time probabilistic algorithms, $b \in \{0, 1\}$.

Let $\text{IND}_{CPA}^b(\mathcal{A})$ be the following algorithm:

- ▶ Generate $(pk, sk) \xleftarrow{R} \mathcal{K}(\eta)$.
- ▶ $(s, m_0, m_1) \xleftarrow{R} \mathcal{A}_1(\eta, pk)$
- ▶ Sample $b \xleftarrow{R} \{0, 1\}$.
- ▶ $b' \xleftarrow{R} \mathcal{A}_2(\eta, pk, s, \mathcal{E}(pk, m_b))$
- ▶ return b' .

Then, we define the advantage against the IND-CPA game by:

$$\text{ADV}_{\mathcal{S}, \mathcal{A}}^{\text{IND}_{CPA}}(\eta) = \Pr[b' \xleftarrow{R} \text{IND}_{CPA}^1(\mathcal{A}) : b' = 1] - \Pr[b' \xleftarrow{R} \text{IND}_{CPA}^0(\mathcal{A}) : b' = 1]$$

The IND-CCA1 Games



Given an encryption scheme $\mathcal{S} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$. An adversary is a pair $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ of polynomial-time probabilistic algorithms, $b \in \{0, 1\}$.

Let $\text{IND}_{\text{CCA1}}^b(\mathcal{A})$ be the following algorithm:

- ▶ Generate $(pk, sk) \xleftarrow{R} \mathcal{K}(\eta)$.
- ▶ $(s, m_0, m_1) \xleftarrow{R} \mathcal{A}_1^{\mathcal{O}_1}(\eta, pk)$ **where** $\mathcal{O}_1 = \mathcal{D}$
- ▶ Sample $b \xleftarrow{R} \{0, 1\}$.
- ▶ $b' \xleftarrow{R} \mathcal{A}_2(\eta, pk, s, \mathcal{E}(pk, m_b))$
- ▶ return b' .

Then, we define the advantage against the IND-CCA1 game by:

$$\text{ADV}_{\mathcal{S}, \mathcal{A}}^{\text{IND}_{\text{CCA1}}}(\eta) = \Pr[b' \xleftarrow{R} \text{IND}_{\text{CCA1}}^1(\mathcal{A}) : b' = 1] - \Pr[b' \xleftarrow{R} \text{IND}_{\text{CCA1}}^0(\mathcal{A}) : b' = 1]$$

The IND-CCA2 Games



Given an encryption scheme $\mathcal{S} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$. An adversary is a pair $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ of polynomial-time probabilistic algorithms, $b \in \{0, 1\}$.

Let $\text{IND}_{\text{CCA2}}^b(\mathcal{A})$ be the following algorithm:

- ▶ Generate $(pk, sk) \xleftarrow{R} \mathcal{K}(\eta)$.
- ▶ $(s, m_0, m_1) \xleftarrow{R} \mathcal{A}_1^{\mathcal{O}_1}(\eta, pk)$ where $\mathcal{O}_1 = \mathcal{D}$
- ▶ Sample $b \xleftarrow{R} \{0, 1\}$.
- ▶ $b' \xleftarrow{R} \mathcal{A}_2^{\mathcal{O}_2}(\eta, pk, s, \mathcal{E}(pk, m_b))$ **where** $\mathcal{O}_2 = \mathcal{D}$
- ▶ return b' .

Then, we define the advantage against the IND-CCA2 game by:

$$\text{ADV}_{\mathcal{S}, \mathcal{A}}^{\text{IND}_{\text{CCA2}}}(\eta) = \Pr[b' \xleftarrow{R} \text{IND}_{\text{CCA2}}^1(\mathcal{A}) : b' = 1] - \Pr[b' \xleftarrow{R} \text{IND}_{\text{CCA2}}^0(\mathcal{A}) : b' = 1]$$

Summary



Given $\mathcal{S} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, $\text{IND}_{\text{XXX}}^b(\mathcal{A})$ follows:

- ▶ Generate $(pk, sk) \xleftarrow{R} \mathcal{K}(\eta)$.
- ▶ $(s, m_0, m_1) \xleftarrow{R} \mathcal{A}_1^{\mathcal{O}_1}(\eta, pk)$
- ▶ Sample $b \xleftarrow{R} \{0, 1\}$.
- ▶ $b' \xleftarrow{R} \mathcal{A}_2^{\mathcal{O}_2}(\eta, pk, s, \mathcal{E}(pk, m_b))$
- ▶ return b' .

$$\text{ADV}_{\mathcal{S}, \mathcal{A}}^{\text{IND}_{\text{XXX}}}(\eta) =$$

$$\Pr[b' \xleftarrow{R} \text{IND}_{\text{XXX}}^1(\mathcal{A}) : b' = 1] - \Pr[b' \xleftarrow{R} \text{IND}_{\text{XXX}}^0(\mathcal{A}) : b' = 1]$$



IND-CPA: $\mathcal{O}_1 = \mathcal{O}_2 = \emptyset$ Chosen Plain text Attack

IND-CCA1: $\mathcal{O}_1 = \{\mathcal{D}\}$, $\mathcal{O}_2 = \emptyset$ Non-adaptive Chosen Cipher text Attack

IND-CCA2: $\mathcal{O}_1 = \mathcal{O}_2 = \{\mathcal{D}\}$ Adaptive Chosen Cipher text Attack.

IND-XXX Security



Definition

An encryption scheme is *IND-XXX secure*, if for any adversary \mathcal{A} the function $\text{ADV}_{\mathcal{S}, \mathcal{A}}^{\text{IND-XXX}}$ is negligible.

Exercise

Prove that

$$\begin{aligned}
 \text{ADV}_{\mathcal{S}, \mathcal{A}}^{\text{IND}^{\text{XXX}}}(\eta) &= \Pr[b' \stackrel{R}{\leftarrow} \text{IND}^1(\mathcal{A}) : b' = 1] \\
 &\quad - \Pr[b' \stackrel{R}{\leftarrow} \text{IND}^0(\mathcal{A}) : b' = 1] \\
 &= 2\Pr[b' \stackrel{R}{\leftarrow} \text{IND}^b(\mathcal{A}) : b' = b] - 1
 \end{aligned}$$

Definition of Non Malleability



Game Adversary: $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$

1. The adversary \mathcal{A}_1 is given the public key pk .
2. The adversary \mathcal{A}_1 chooses a message space M .
3. Two messages m and m^* are chosen at random in M and $c = E(m; r)$ is given to the adversary.
4. The adversary \mathcal{A}_2 outputs a binary relation R and a cipher-text c' .

Probability $Pr[R(m, m')] - Pr[R(m, m^*)]$ is negligible,
where $m' = \mathcal{D}(c')$

Non-Malleability - XXX

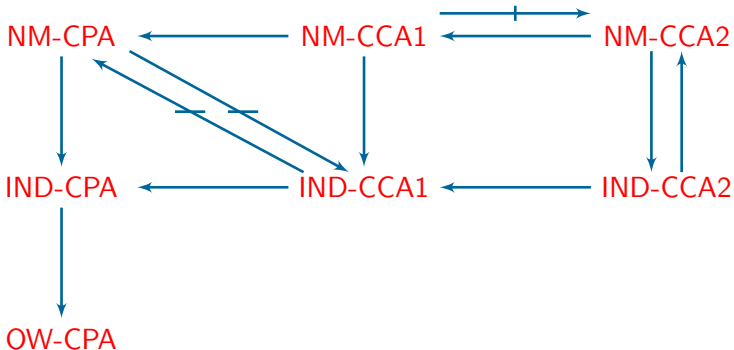


- ▶ Let $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ and $A = (A_1, A_2)$.
- ▶ For $b \in \{0, 1\}$ we define the experiment $\mathbf{Exp}_{\mathcal{PE}, A}^{atk-b}(k)$:
 $(pk, sk) \leftarrow \mathcal{K}(k)$; $(M, s) \leftarrow A_1^{O_1(\cdot)}(pk)$; $x_0, x_1 \leftarrow M$
 $y \leftarrow \mathcal{E}_{pk}(x_b)$; $(\mathcal{R}, \vec{y}) \leftarrow A_2^{O_2(\cdot)}(M, s, y)$; $\vec{x} \leftarrow \mathcal{D}_{pk}(\vec{y})$;
 If $y \notin \vec{y} \wedge \perp \notin \vec{x} \wedge \mathcal{R}(x_b, \vec{x})$ then $d \leftarrow 1$ else $d \leftarrow 0$
 Return d
- ▶ For $atk \in \{cpa, cca1, cca2\}$ and $k \in \mathbb{N}$, the advantage

$$\mathbf{Adv}_{\mathcal{PE}, A}^{atk}(k) = Pr \left[\mathbf{Exp}_{\mathcal{PE}, A}^{atk-1}(k) = 1 \right] - Pr \left[\mathbf{Exp}_{\mathcal{PE}, A}^{atk-0}(k) = 1 \right]$$

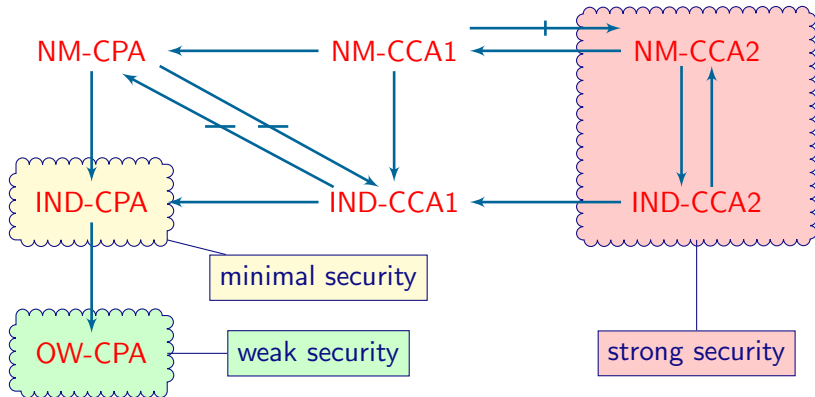
has to be negligible for \mathcal{PE} to be considered secure, assuming A , M and \mathcal{R} can be computed in time $p(k)$.

Relations



*“Relations Among Notions of Security for Public-Key Encryption Schemes”, **Crypto’98**, by Mihir Bellare, Anand Desai, David Pointcheval and Phillip Rogaway [BDPR’98]*

Relations



"Relations Among Notions of Security for Public-Key Encryption Schemes", **Crypto'98**, by Mihir Bellare, Anand Desai, David Pointcheval and Phillip Rogaway [BDPR'98]

Outline

Different Adversaries

Intuition of Computational Security

Definitions of Computational Security

Examples

RSA

ElGamal

Famous Example OAEP

Attack on ECB

Conclusion

Example: RSA

public	private
$n = pq$	$d = e^{-1} \pmod{\phi(n)}$
e (public key)	(private key)

RSA Encryption

- ▶ $E(m) = m^e \pmod n$
- ▶ $D(c) = c^d \pmod n$

OW-CPA = RSA problem by definition!

But not semantically secure because it is deterministic.

Recall Elgamal

- ▶ $G = (\langle g \rangle, *)$ finite cyclic group of prime order q .
- ▶ x : **private** key.
- ▶ $y = g^x$: **public** key.

$$\mathcal{E}(m; r) = (g^r, y^r m) \rightarrow (c, d) \text{ and } \mathcal{D}(c, d) = \frac{d}{c^x}$$

OW = CDH Assumption
IND-CPA = DDH Assumption

OW-CPA for Elgamal

Exercise

Prove that under CDH assumption El-Gamal is OW-CPA.

OW-CPA for Elgamal

Exercise

Prove that under CDH assumption El-Gamal is OW-CPA.

Consider an adversary A that can invert random Elgamal encryptions. We will show that this quantity is negligible. We first use A to build an adversary D for computing the Diffie-Hellman function:

D : Adversary to compute the Diffie-Hellman function:

On input (g^a, g^b) , we must output g^{ab} .

1. Give g^a to A as the public key.
2. Pick a random $d \in G$ and give (g^b, d) to A as the ciphertext.
3. When A outputs $m = \frac{d}{g^{ab}}$, we output $\frac{d}{m}$.

IND-CPA for Elgamal

Exercise

Prove that under DDH assumption El-Gamal is IND-CPA.

Outline

Different Adversaries

Intuition of Computational Security

Definitions of Computational Security

Examples

RSA

ElGamal

Famous Example OAEP

Attack on ECB

Conclusion

Optimal Asymmetric Encryption Padding (OAEP)

The OAEP cryptosystem $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ obtained from a permutation f , whose inverse is denoted by g . And two hash functions:

$$G : \{0, 1\}^{k_0} \rightarrow \{0, 1\}^{k-k_0}$$

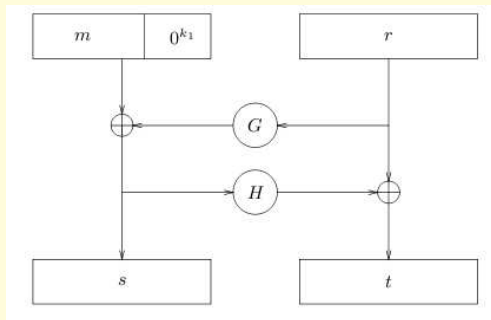
$$H : \{0, 1\}^{k-k_0} \rightarrow \{0, 1\}^{k_0}$$

$\mathcal{K}(1^k)$: specifies an instance of the function f , and of its inverse g .
The public key pk is therefore f and the private key sk is g .

OAEP: Encryption

$\mathcal{E}_{pk}(m, r) = c$ with $m \in \{0, 1\}^n$, and $r \leftarrow \{0, 1\}^{k_0}$

$$s = (m || 0^{k_1}) \oplus G(r), t = r \oplus H(s)$$



$$c = f(s, t)$$

OAEP: Decryption

 $\mathcal{D}_{sk}(c)$

$$g(c) = (s, t)$$

$$r = t \oplus H(s)$$

$$M = s \oplus G(r)$$

If $[M]_{k_1} = 0^{k_1}$, the algorithm returns $[M]^n$, otherwise it returns "Reject"

- ▶ $[M]_{k_1}$ denotes the k_1 least significant bits of M
- ▶ $[M]^n$ denotes the n most significant bits of M

Results and References

OAEP was first proved IND-CPA then IND-CCA1 and finally IND-CCA2 secure under some assumptions.

1. M. Bellare, P. Rogaway. “Optimal Asymmetric Encryption – How to encrypt with RSA”. Extended abstract in Advances in Cryptology - Eurocrypt '94 Proceedings, LNCS Vol. 950, A. Springer-Verlag, 1995.
2. Victor Shoup. “OAEP Reconsidered”. IBM Zurich Research Lab, September 18, 2001.
3. Eiichiro Fujisaki, Tatsuaki Okamoto, David Pointcheval, and Jacques Stern. “RSA– OAEP is secure under the RSA assumption”. In J. Kilian, ed., Advances in Cryptology – CRYPTO 2001, vol. 2139 of LNCS, SpringerVerlag, 2001.
4. P. Paillier and J. Villar, “Trading One-Wayness against Chosen-Ciphertext Security in Factoring-Based Encryption”, Advances in Cryptology – Asiacrypt 2006.

Others Cryptosystems

- ▶ Bellare & Rogaway'93:

$$f(r)||x \oplus G(r)||H(x||r)$$

- ▶ Zheng & Seberry'93:

$$f(r)||G(r) \oplus (x||H(x))$$

- ▶ OAEP'94 (Bellare & Rogaway):

$$f(s||r \oplus H(s))$$

where $s = x0^k \oplus G(r)$

- ▶ OAEP+'02 (Shoup):

$$f(s||r \oplus H(s))$$

where $s = x \oplus G(r)||H'(r||x)$.

- ▶ Fujisaki & Okamoto'99:

$$\mathcal{E}((x||r); H(x||r))$$

where \mathcal{E} is IND-CPA.

Outline

Different Adversaries

Intuition of Computational Security

Definitions of Computational Security

Examples

- RSA

- ElGamal

Famous Example OAEP

Attack on ECB

Conclusion

ECB Attack

Let us fix a block cipher $\mathcal{E} : \mathcal{K} \times \{0, 1\}^n \rightarrow \{0, 1\}^n$. and $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ an ECB symmetric encryption scheme, where the size of each block is n .

We build an adversary A with a high IND-CPA advantage.

$$\mathcal{E}_K(LR(m_l, m_r, b)) = \begin{cases} \mathcal{E}_K(m_l) & \text{if } b = 1 \\ \mathcal{E}_K(m_r) & \text{if } b = 0 \end{cases}$$

Adversary A

Adversary $A^{\mathcal{E}_K(LR(\cdot, \cdot, b))}$

$M_0 \leftarrow 0^n || 1^n;$

$M_1 \leftarrow 0^{2n};$

$C[1]C[2] \leftarrow \mathcal{E}_K(LR(M_0, M_1, b))$

If $C[1] = C[2]$ then return 1 else return 0

$X[i]$ denotes the i -th block of a string X , a block being a sequence of n bits.

Proof

$$\Pr[\text{Exp}_{S\mathcal{E}}^{\text{IND-CPA } 0}(A) = 1] = 0$$

$$\Pr[\text{Exp}_{S\mathcal{E}}^{\text{IND-CPA } 1}(A) = 1] = 1$$

Why?

Proof

$$\Pr[\text{Exp}_{S\mathcal{E}}^{\text{IND-CPA } 0}(A) = 1] = 0$$

$$\Pr[\text{Exp}_{S\mathcal{E}}^{\text{IND-CPA } 1}(A) = 1] = 1$$

Why?

- ▶ If $b = 1$, then the oracle returns $C[1]C[2] = \mathcal{E}_K(0^n) || \mathcal{E}_K(0^n)$, so $C[1] = C[2]$ and A returns 1.

Proof

$$\Pr[\text{Exp}_{S\mathcal{E}}^{\text{IND-CPA } 0}(A) = 1] = 0$$

$$\Pr[\text{Exp}_{S\mathcal{E}}^{\text{IND-CPA } 1}(A) = 1] = 1$$

Why?

- ▶ If $b = 1$, then the oracle returns $C[1]C[2] = \mathcal{E}_K(0^n) || \mathcal{E}_K(0^n)$, so $C[1] = C[2]$ and A returns 1.
- ▶ if $b = 0$, the oracle returns $C[1]C[2] = \mathcal{E}_K(0^n) || \mathcal{E}_K(1^n)$. Hence $C[1] \neq C[2]$. So A returns 0 in this case.

Proof

$$\Pr[\text{Exp}_{S\mathcal{E}}^{\text{IND-CPA } 0}(A) = 1] = 0$$

$$\Pr[\text{Exp}_{S\mathcal{E}}^{\text{IND-CPA } 1}(A) = 1] = 1$$

Why?

- ▶ If $b = 1$, then the oracle returns $C[1]C[2] = \mathcal{E}_K(0^n) \parallel \mathcal{E}_K(0^n)$, so $C[1] = C[2]$ and A returns 1.
- ▶ if $b = 0$, the oracle returns $C[1]C[2] = \mathcal{E}_K(0^n) \parallel \mathcal{E}_K(1^n)$. Hence $C[1] \neq C[2]$. So A returns 0 in this case.

$$\text{Adv}_{S\mathcal{E}}^{\text{IND-CPA}}(A) = 1 - 0 = 1$$

This means that the ECB encryption scheme is insecure.

Exercise

1. Find an attack on CBC with counter IV.
2. Prove that CBC with random IV is not IND-CCA2 secure.
3. Notice that CBC with random IV is IND-CPA secure.

Outline

Different Adversaries

Intuition of Computational Security

Definitions of Computational Security

Examples

RSA

ElGamal

Famous Example OAEP

Attack on ECB

Conclusion

Summary

Today

- ▶ Classical Symmetric Encryption
- ▶ Security Notions
- ▶ Examples

Next Time, Last Time

- ▶ Other Crypto-Systems like McEliece public key encryption algorithm based on algebraic coding theory.

Thank you for your attention

Questions ?