DD2448 Foundations of Cryptography
Lecture 11

Douglas Wikström
KTH Royal Institute of Technology
dog@kth.se

April 21, 2020

CPA Security

CPA Security (1/3)

- RSA clearly provides some kind of "security", but it is clear that we need to be more careful with what we ask for.

CPA Security (1/3)

- RSA clearly provides some kind of "security", but it is clear that we need to be more careful with what we ask for.
- Intuitively, we want to leak no information of the encrypted plaintext.

CPA Security (1/3)

- RSA clearly provides some kind of "security", but it is clear that we need to be more careful with what we ask for.
- Intuitively, we want to leak no **knowledge** of the encrypted plaintext.

CPA Security (1/3)

- RSA clearly provides some kind of "security", but it is clear that we need to be more careful with what we ask for.
- Intuitively, we want to leak no **knowledge** of the encrypted plaintext.
- In other words, no function of the plaintext can efficiently be guessed notably better from its ciphertext than without it.

CPA Security (2/3)

$\mathbf{Exp}^{b}_{\mathcal{CS},A}$ **(CPA Security Experiment).**

1. **Generate Public Key.** $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^n)$.
2. **Adversarial Choice of Messages.** $(m_0, m_1, s) \leftarrow A(\mathsf{pk})$.
3. **Guess Message.** Return the first output of $A(\mathsf{E}_{\mathsf{pk}}(m_b), s)$.

CPA Security (2/3)

$\mathbf{Exp}^{b}_{\mathcal{CS},A}$ **(CPA Security Experiment).**

1. **Generate Public Key.** $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^n)$.
2. **Adversarial Choice of Messages.** $(m_0, m_1, s) \leftarrow A(\mathsf{pk})$.
3. **Guess Message.** Return the first output of $A(\mathsf{E}_{\mathsf{pk}}(m_b), s)$.

Definition. A cryptosystem $\mathcal{CS} = (\mathsf{Gen}, \mathsf{E}, \mathsf{D})$ is said to be **CPA secure** if for every polynomial time algorithm A

$$|\Pr[\mathrm{Exp}^{0}_{\mathcal{CS},A} = 1] - \Pr[\mathrm{Exp}^{1}_{\mathcal{CS},A} = 1]|$$

is negligible.

CPA Security (3/3)

Every CPA secure cryptosystem must be probabilistic!

CPA Security (3/3)

Every CPA secure cryptosystem must be probabilistic!

Theorem. Suppose that $\mathcal{CS} = (\mathsf{Gen}, \mathsf{E}, \mathsf{D})$ is a CPA secure cryptosystem.

Then the related cryptosystem where a $t(n)$-list of messages, with $t(n)$ polynomial, is encrypted by **repeated independent encryption** of each component using the **same public key** is also CPA secure.

CPA Security (3/3)

Every CPA secure cryptosystem must be probabilistic!

Theorem. Suppose that $\mathcal{CS} = (\mathsf{Gen}, \mathsf{E}, \mathsf{D})$ is a CPA secure cryptosystem.

Then the related cryptosystem where a $t(n)$-list of messages, with $t(n)$ polynomial, is encrypted by **repeated independent encryption** of each component using the **same public key** is also CPA secure.

CPA security is useful!