Introduction to Modern Cryptography
Recitation 1

Orit Moskovich
Tel Aviv University
November 2, 2016

Encryption Scheme

- Gen: Probabilistic algorithm that outputs a key k chosen according to some distribution
- $\mathcal{K}$: The key space
- $\mathcal{M}$: The message space
- Enc: Encryption algorithm
  Takes as input a key $k \in \mathcal{K}$ and a message $m \in \mathcal{M}$, and outputs a ciphertext c. Denote by $Enc_k(m) = c$.
- $\mathcal{C}$: The set of all possible ciphertexts that can be output by $Enc_k(m)$
- Dec: Decryption algorithm
  Takes as input a key $k \in \mathcal{K}$ and a ciphertext $c \in C$ and outputs a message $m \in \mathcal{M}$. Denote by $Dec_k(c) = m$.

Encryption Scheme

- Enc: Encryption algorithm
  Takes as input a key $k \in \mathcal{K}$ and a message $m \in \mathcal{M}$, and outputs a ciphertext c. Denote by $Enc_k(m) = c$.
- Dec: Decryption algorithm
  Takes as input a key $k \in \mathcal{K}$ and a ciphertext $c \in C$ and outputs a message $m \in \mathcal{M}$. Denote by $Dec_k(c) = m$.

- Correctness: For every message $m \in \mathcal{M}$ and key k:

$$Dec_k\big(Enc_k(m)\big) = m$$

Perfect Secrecy

- We assume the adversary knows the probability distribution over $\mathcal{M}$
- Then the adversary observes some ciphertext
- **Goal:** observing this ciphertext should have no effect on the knowledge of the adversary
- True for any $m \in \mathcal{M}$
- True for an adversary with unbounded computational power

➢ a ciphertext reveals nothing about the underlying plaintext

Perfect Secrecy (Perfect Cipher)

- a ciphertext reveals nothing about the underlying plaintext

Definition. An encryption scheme (Gen, Enc, Dec) over a message space M is **perfectly secret** if

- for every probability distribution M over $\mathcal{M}$
- for every message $m \in \mathcal{M}$
- and for every ciphertext $c \in \mathcal{C}$
- for which $\Pr_{k \leftarrow \mathcal{K}}[c = Enc_k(m)] > 0$:

$$\Pr[M = m \mid Enc_k(M) = c] = \Pr[M = m]$$

Perfect Indistinguishability

- Impossible to distinguish between
  an encryption of m_0 and an encryption of m_1

Experiment 0

Choose random key k
Output $c_0 = Enc_k(m_0)$

$\equiv$

Experiment 1

Choose random key k
Output $c_1 = Enc_k(m_1)$

Perfect Indistinguishability

Definition. An encryption scheme (Gen, Enc, Dec) over a message space M is **perfectly indistinguishable** if

- for every messages $m_0, m_1 \in \mathcal{M}$
- and for every ciphertext $c \in \mathcal{C}$

$$\Pr_{k \leftarrow \mathcal{K}}[Enc_k(m_0) = c] = \Pr_{k \leftarrow \mathcal{K}}[Enc_k(m_1) = c]$$

Perfect Indistinguishability

Lemma. An encryption scheme (Gen, Enc, Dec)
is **perfectly indistinguishable** $\Leftrightarrow$ it is **perfectly secret**

Adversarial Indistinguishability

- Define an experiment involving an adversary A
- A is trying to distinguish the encryption of one plaintext from the encryption of another

Adversarial indistinguishability experiment for A:

1. The adversary A outputs a pair of messages $m_0, m_1 \in \mathcal{M}$
2. A random key k is generated using Gen, and a random bit $b \leftarrow \{0,1\}$
3. The ciphertext $c = Enc_k(m_b)$ is computed and given to A
4. A outputs a bit b'

$$A \text{ wins} \Leftrightarrow b = b'$$

Adversarial Indistinguishability

Adversarial indistinguishability experiment for A:

1. The adversary A outputs a pair of messages $m_0, m_1 \in \mathcal{M}$
2. A random key k is generated using Gen, and a random bit $b \leftarrow \{0,1\}$
3. The ciphertext $c = Enc_k(m_b)$ is computed and given to A
4. A outputs a bit b'

$$A \text{ wins} \Leftrightarrow b = b'$$

Definition. An encryption scheme (Gen, Enc, Dec) over a message space M is **adversarial indistinguishable** if for every adversary A it holds that $\Pr[A \text{ wins}] = \frac{1}{2}$

Vigenère is not perfectly indistinguishable

t	h	e		m	a	n		a	n	d		t	h	e		w	o	m	a	n
b	e	a		d	s	b		e	a	d		s	b	e		a	d	s	b	d
V	M	F		Q	T	P		F	O	H		M	J	J		X	S	F	C	S

Example. Assume a message space of two-character strings, and where the period is chosen uniformly in $\{1,2\}$.

We show an adversary A who wins the experiment w.p. $> \frac{1}{2}$

Vigenère is not perfectly indistinguishable

Example. Assume a message space of two-character strings, and where the period is chosen uniformly in $\{1,2\}$.

We show an adversary A who wins the experiment w.p. $> \frac{1}{2}$

1. The adversary A outputs a pair of messages $m_0 = 00, m_1 = 01$
2. A random key k is generated using Gen, and a random bit $b \leftarrow \{0,1\}$
3. The ciphertext $c = c_1 c_2 = Enc_k(m_b)$ is computed and given to A
4. A outputs a bit $b' = \begin{cases} 0 & \text{if } c_1 = c_2 \\ 1 & \text{otherwise} \end{cases}$

Vigenère is not perfectly indistinguishable

1. The adversary A outputs a pair of messages $m_0 = 00, m_1 = 01$
2. A random key k is generated using Gen, and a random bit $b \leftarrow \{0,1\}$
3. The ciphertext $c = c_1 c_2 = Enc_k(m_b)$ is computed and given to A
4. A outputs a bit $b' = \begin{cases} 0 & \text{if } c_1 = c_2 \\ 1 & \text{otherwise} \end{cases}$

$$
\begin{aligned}
&\Pr[A \text{ wins}] \\
&= \Pr\left[A\left(Enc(m_b)\right) = 0 \middle| b = 0\right] \cdot \Pr[b = 0] \\
&\quad + \Pr\left[A\left(Enc(m_b)\right) = 1 \middle| b = 1\right] \cdot \Pr[b = 1] \\
&= \frac{1}{2}\Pr\left[A\left(Enc(m_0)\right) = 0\right] + \frac{1}{2}\Pr\left[A\left(Enc(m_1)\right) = 1\right]
\end{aligned}
$$

Vigenère is not perfectly indistinguishable

1. The adversary A outputs a pair of messages $m_0 = 00, m_1 = 01$
2. A random key k is generated using Gen, and a random bit $b \leftarrow \{0,1\}$
3. The ciphertext $c = c_1 c_2 = Enc_k(m_b)$ is computed and given to A
4. A outputs a bit $b' = \begin{cases} 0 & \text{if } c_1 = c_2 \\ 1 & \text{otherwise} \end{cases}$

$$
\begin{aligned}
&\Pr[A \text{ wins}] \\
&= \Pr\left[A\left(Enc(m_b)\right) = 0 \middle| b = 0\right] \cdot \Pr[b = 0] \\
&\quad + \Pr\left[A\left(Enc(m_b)\right) = 1 \middle| b = 1\right] \cdot \Pr[b = 1] \\
&= \frac{1}{2}\Pr\left[A\left(Enc(m_0)\right) = 0\right] + \frac{1}{2}\Pr\left[A\left(Enc(m_1)\right) = 1\right]
\end{aligned}
$$

Vigenère is not perfectly indistinguishable

1. The adversary A outputs a pair of messages $m_0 = 00, m_1 = 01$
2. A random key k is generated using Gen, and a random bit $b \leftarrow \{0,1\}$
3. The ciphertext $c = c_1 c_2 = Enc_k(m_b)$ is computed and given to A
4. A outputs a bit $b' = \begin{cases} 0 & \text{if } c_1 = c_2 \\ 1 & \text{otherwise} \end{cases}$

$$\Pr[A(Enc(m_0)) = 0] = ?$$

A key of period 1 is chosen

A key of period 2 is chosen,
and both characters of the key are equal

$$\Pr[A(Enc(m_0)) = 0] = \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{26}$$

Vigenère is not perfectly indistinguishable

1. The adversary A outputs a pair of messages $m_0 = 00, m_1 = 01$
2. A random key k is generated using Gen, and a random bit $b \leftarrow \{0,1\}$
3. The ciphertext $c = c_1 c_2 = Enc_k(m_b)$ is computed and given to A
4. A outputs a bit $b' = \begin{cases} 0 & \text{if } c_1 = c_2 \\ 1 & \text{otherwise} \end{cases}$

$$
\begin{aligned}
&\Pr[A \text{ wins}] \\
&= \Pr\left[A\left(Enc(m_b)\right) = 0 \middle| b = 0\right] \cdot \Pr[b = 0] \\
&\quad + \Pr\left[A\left(Enc(m_b)\right) = 1 \middle| b = 1\right] \cdot \Pr[b = 1] \\
&= \frac{1}{2}\Pr\left[A\left(Enc(m_0)\right) = 0\right] + \frac{1}{2}\Pr\left[A\left(Enc(m_1)\right) = 1\right]
\end{aligned}
$$

Vigenère is not perfectly indistinguishable

1. The adversary A outputs a pair of messages $m_0 = 00, m_1 = 01$
2. A random key k is generated using Gen, and a random bit $b \leftarrow \{0,1\}$
3. The ciphertext $c = c_1 c_2 = Enc_k(m_b)$ is computed and given to A
4. A outputs a bit $b' = \begin{cases} 0 & \text{if } c_1 = c_2 \\ 1 & \text{otherwise} \end{cases}$

$$\Pr[A(Enc(m_1)) = 1] = 1 - \Pr[A(Enc(\underline{m_1})) = 0] = ?$$

A key of period 2 is chosen,
and the first character of the key is one more than the second

$$\Pr[A(Enc(m_1)) = 1] = 1 - \Pr[A(Enc(m_1)) = 0] = 1 - \frac{1}{2} \cdot \frac{1}{26}$$

Vigenère is not perfectly indistinguishable

1. The adversary A outputs a pair of messages $m_0 = 00, m_1 = 01$
2. A random key k is generated using Gen, and a random bit $b \leftarrow \{0,1\}$
3. The ciphertext $c = c_1 c_2 = Enc_k(m_b)$ is computed and given to A
4. A outputs a bit $b' = \begin{cases} 0 & \text{if } c_1 = c_2 \\ 1 & \text{otherwise} \end{cases}$

$$
\begin{aligned}
&\Pr[A \text{ wins}] \\
&= \Pr\left[A\left(Enc(m_b)\right) = 0 \middle| b = 0\right] \cdot \Pr[b = 0] \\
&\quad + \Pr\left[A\left(Enc(m_b)\right) = 1 \middle| b = 1\right] \cdot \Pr[b = 1] \\
&= \frac{1}{2}\Pr\left[A\left(Enc(m_0)\right) = 0\right] + \frac{1}{2}\Pr\left[A\left(Enc(m_1)\right) = 1\right] = \cdots > \frac{1}{2}
\end{aligned}
$$

One time pad is perfectly indistinguishable

- Fix an integer $\ell > 0$
- $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}^{\ell}$
- Gen: chooses a string k from $\mathcal{K}$ according to the uniform distribution
- $Enc_k(m) = m \oplus k$
- $Dec_k(c) = c \oplus k$

Theorem. The one-time pad encryption scheme is perfectly secret

One time pad is perfectly indistinguishable

Theorem. The one-time pad encryption scheme is perfectly secret

- *Reminder.* An encryption scheme (Gen, Enc, Dec) over a message space M is **perfectly indistinguishable** if

$$\Pr_{k \leftarrow \mathcal{K}}[Enc_k(m_0) = c] = \Pr_{k \leftarrow \mathcal{K}}[Enc_k(m_1) = c]$$

- Let $c \in \mathcal{C}, m \in \mathcal{M}$
- $\Pr_{k \leftarrow \mathcal{K}}[Enc_k(m) = c] = \Pr[m \oplus k = c] = \Pr[m \oplus c = k] = \frac{1}{2^\ell}$

Back to Adversarial Indistinguishability

Adversarial indistinguishability experiment for A:

1. The adversary A outputs a pair of messages $m_0, m_1 \in \mathcal{M}$
2. A random key k is generated using Gen, and a random bit $b \leftarrow \{0,1\}$
3. The ciphertext $c = Enc_k(m_b)$ is computed and given to A
4. A outputs a bit b'

Lemma. An encryption scheme (Gen, Enc, Dec)
is **perfectly indistinguishable** $\Leftrightarrow$ for every adversary A it holds that
$\Pr[A \text{ wins}] = \frac{1}{2}$

Adversarial Indistinguishability

Proof. **Not perfectly indistinguishable** $\Longrightarrow \Pr[A \text{ wins}] > \frac{1}{2}$

- Assume the encryption scheme (Gen, Enc, Dec) is not perfectly indistinguishable
- $\exists\, m_0, m_1, c'$ s.t. $\Pr_{k \leftarrow \mathcal{K}}[Enc_k(m_0) = c'] > \Pr_{k \leftarrow \mathcal{K}}[Enc_k(m_1) = c']$

1. The adversary A outputs the messages m_0, m_1
2. A random key k is generated using Gen, and a random bit $b \leftarrow \{0,1\}$
3. The ciphertext $c = Enc_k(m_b)$ is computed and given to A
4. A outputs a bit $b' = \begin{cases} 0 & \text{if } c = c' \\ \text{coin flip} & \text{otherwise} \end{cases}$