Perfect Secrecy

CS 5158/6058 Data Security and Privacy

Spring 2018

Instructor: Boyang Wang

Perfect Secrecy

- Observing ciphertext c has <u>no effect</u> on an adversary's knowledge regarding message m

Theorem An encryption scheme $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ is **perfectly secret** if for every probability distribution over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$:

$$\Pr[M = m | C = c] = \Pr[M = m]$$

Perfect Secrecy

- The distribution of the ciphertext does not depend on distribution of the plaintext

Lemma An encryption scheme $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ is **perfectly secret** if for every $m, m' \in \mathcal{M}$ and every $c \in \mathcal{C}$

$$\Pr[\mathsf{Enc}_K(m) = c] = \Pr[\mathsf{Enc}_K(m') = c]$$

where the probabilities are over choice of K and any randomness of Enc.

Security Game

- Ciphertexts of m_0, m_1 are <u>indistinguishable</u>.

Given $\Pi = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$, **security game** $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$:

1. Adversary $\mathcal{A}$ outputs $m_0, m_1 \in \mathcal{M}$ with $|m_0| = |m_1|$
2. Challenger flips a (fair) coin $b \in \{0, 1\}$, compute $c_b \leftarrow \mathsf{Enc}_k(m_b)$, where $k \leftarrow \mathsf{KeyGen}(1^l)$, and return c_b to $\mathcal{A}$
3. $\mathcal{A}$ guesses a bit b'
4. Output 1 if $b' = b$, otherwise 0; $\mathcal{A}$ wins if it is 1

Security Game

- Random guess is 1/2, but cannot do better

Def. Encryption scheme $\Pi = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$, with message space $\mathcal{M}$ is **perfectly indistinguishable** if for every $\mathcal{A}$ it holds that

$$\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = \frac{1}{2}$$

- Adversary does not have <u>any advantage</u>

$$\mathrm{Adv}^{\mathsf{eav}}_{\mathcal{A},\Pi} = \left| \Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] - \frac{1}{2} \right| = 0$$

Vigenere Cipher

- Vigenere Cipher is <u>not</u> perfectly indistinguishable
- Example: message $\mathcal{M}$ = {**`aa`**, **`ab`**}, key is a string of 1 or 2 (key length is uniformly chosen)

1. Adversary $\mathcal{A}$ chooses $m_0 = aa$ and $m_1 = ab$
2. Challenger flips a coin, obtains b and $c_b \leftarrow \mathsf{Enc}_k(m_b)$
3. Given $c_b = c_{b1}c_{b2}$, Adversary $\mathcal{A}$ guesses $b' = 0$ if $c_{b1} = c_{b2}$; otherwise $b' = 1$
4. $\mathcal{A}$ wins iff $b' = b$

Analysis on Vigenere Cipher

- Adversary A wins if b’=0|b=0 or b’=1|b=1
- Random guess 1/2, prove A can win <u>greater than1/2</u>

$$
\begin{aligned}
& \Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\mathsf{VC}} = 1] \\
= \quad & \Pr[b=0] \cdot \Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\mathsf{VC}} = 1 | b=0] \\
& + \quad \Pr[b=1] \cdot \Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\mathsf{VC}} = 1 | b=1] \\
= \quad & \frac{1}{2} \cdot \Pr[b'=0|b=0] + \frac{1}{2} \cdot \Pr[b'=1|b=1]
\end{aligned}
$$

Analysis on Vigenere Cipher

- $b'=0|b=0$ ($c_b=c_{b1}c_{b2}, c_{b1}=c_{b2}|m_0=$**`aa`**) has two cases:
  - Key length is 1 (k_1), any k_1 in {0,1, …, 25}
    - E.g., **`aa`** + k_1k_1 = **`XX`**
  - Key length is 2 (k_1k_2), and <u>k_1,k_2 are same</u>
    - E.g., **`aa`** + $k_1k_2 = k_1k_1$ = **`XX`**

$$\Pr[b' = 0|b = 0] = \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{26} \approx 0.52$$

Analysis on Vigenere Cipher

- $b'=1|b=1(c_b=c_{b1}c_{b2}, c_{b1}!=c_{b2}|m_1=\mathbf{ab})$ has two cases:
  - Key length is 1 (k_1), any k_1 in {0,1, …, 25}
    - E.g., **`ab`** + k_1k_1 = **`XY`**
  - Key length is 2 (k_1k_2), and <u>k_2 is not k_1-1</u>
    - E.g, **`ab`** + k_1k_2 = $k_1(k_1-1)$ = **`XX`**

- <u>Practice:</u> Pr[b'=1|b=1] = ?

$$\Pr[b' = 1 | b = 1] = \frac{1}{2} + \frac{1}{2} \cdot (1 - \frac{1}{26}) \approx 0.98$$

Analysis on Vigenere Cipher

- Put everything together

$$
\begin{aligned}
& \Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\mathsf{VC}} = 1] \\
= \quad & \frac{1}{2} \cdot \Pr[b' = 0 | b = 0] + \frac{1}{2} \cdot \Pr[b' = 1 | b = 1] \\
\approx \quad & \frac{1}{2} \cdot 0.52 + \frac{1}{2} \cdot 0.98 \\
= \quad & 0.75 \quad > \quad \frac{1}{2}
\end{aligned}
$$

Analysis on Vigenere Cipher

- <u>Practice:</u> message $\mathcal{M}$ = {`aaa`, `aab`}, key is a string of 1, 2 or 3 (uniformly chosen)
- Complete the steps for adversary A in the game

1. Adversary $\mathcal{A}$ chooses ????
2. Challenger flips a coin, obtains b and ????
3. Given $c_b = c_{b1}c_{b2}c_{b3}$, Adversary $\mathcal{A}$ guesses $b' = 0$ if $c_{b2} = c_{b3}$; otherwise $b' = 1$
4. $\mathcal{A}$ wins iff ???

Analysis on Vigenere Cipher

- Practice: message $\mathcal{M}$ = {**aaa**, **aab**}, key is a string of 1, 2 or 3 (uniformly chosen)
- Complete the steps for adversary A in the game

1. Adversary $\mathcal{A}$ chooses $m_0 = aaa$ and $m_1 = aab$
2. Challenger flips a coin, obtains b and $c_b \leftarrow \mathsf{Enc}_k(m_b)$
3. Given $c_b = c_{b1}c_{b2}c_{b3}$, Adversary $\mathcal{A}$ guesses $b' = 0$ if $c_{b2} = c_{b3}$; otherwise $b' = 1$
4. $\mathcal{A}$ wins iff $b' = b$

Analysis on Vigenere Cipher

- Choose m_0=`aaa`, m_1=`aab`
- Given $c_b = c_{b1}c_{b2}c_{b3}$, guess b'=0 if $c_{b2} = c_{b3}$

- Adversary A wins if b'=0|b=0 or b'=1|b=1
- <u>Practice:</u> Prove A can win <u>greater than1/2</u>

$$
\begin{aligned}
& \Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\mathsf{VC}} = 1] \\
= \quad & \Pr[b=0] \cdot \Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\mathsf{VC}} = 1 | b = 0] \\
& + \quad \Pr[b=1] \cdot \Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\mathsf{VC}} = 1 | b = 1] \\
= \quad & \frac{1}{2} \cdot \Pr[b' = 0 | b = 0] + \frac{1}{2} \cdot \Pr[b' = 1 | b = 1]
\end{aligned}
$$

Analysis on Vigenere Cipher

- $b'=0|b=0$ ($c_b=c_{b1}c_{b2}c_{b3}$, $c_{b2}=c_{b3}|m_0=$ **aaa**) has 3 cases:
  - Key length is 1 (k_1)
    - E.g., **aaa** + $k_1k_1k_1$ = **xxx**
  - Key length is 2 (k_1k_2), and <u>k_1,k_2 are same</u>
    - E.g., **aaa** + $k_1k_2k_1$ = $k_1k_1k_1$ = **xxx**
  - Key length is 3 ($k_1k_2k_3$), and <u>k_2,k_3 are same</u>
    - E.g., **aaa** + $k_1k_2k_3$ = $k_1k_2k_2$ = **#xx**

$$\Pr[b'=0|b=0] = \frac{1}{3} + \frac{1}{3}\cdot\frac{1}{26} + \frac{1}{3}\cdot\frac{1}{26} \approx 0.359$$

Analysis on Vigenere Cipher

- $b'=1|b=1$ ($c_b=c_{b1}c_{b2}c_{b3}$, $c_{b2}!=c_{b3}|m_1=$**aab**) has 3 cases:
  - Key length is 1 (k_1)
    - E.g., **aab** + $k_1k_1k_1$ = **XXY**
  - Key length is 2 (k_1k_2), and k_2 is not k_1+1
    - E.g., **aab** + $k_1k_2k_1$ = $k_1(k_1+1)k_1$ = **WXX**
  - Key length is 3 ($k_1k_2k_3$), and k_3 is not k_2-1
    - E.g., **aab** + $k_1k_2k_3$ = $k_1k_2(k_2-1)$ = **#XX**

$$\Pr[b'=1|b=1] = \frac{1}{3} + \frac{1}{3}\cdot(1-\frac{1}{26}) + \frac{1}{3}\cdot(1-\frac{1}{26}) \approx 0.974$$

Analysis on Vigenere Cipher

- Put everything together

$$
\begin{aligned}
& \Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\mathsf{VC}} = 1] \\
= \quad & \frac{1}{2} \cdot \Pr[b' = 0 | b = 0] + \frac{1}{2} \cdot \Pr[b' = 1 | b = 1] \\
\approx \quad & \frac{1}{2} \cdot 0.359 + \frac{1}{2} \cdot 0.974 \\
= \quad & 0.667 \quad > \quad \frac{1}{2}
\end{aligned}
$$

Perfect Secrecy of OTP

Theorem An encryption scheme $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ is **perfectly secret** if for every probability distribution over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$:

$$\Pr[M = m | C = c] = \Pr[M = m]$$

Bayes' Theorem

$$\Pr[M = m | C = c] = \frac{\Pr[C = c | M = m] \cdot \Pr[M = m]}{\Pr[C = c]}$$

Perfect Secrecy of OTP

- We need to prove

$$\frac{\Pr[C = c | M = m]}{\Pr[C = c]} = 1$$

- For an arbitrary c in space $\mathcal{C}$ and m in space $\mathcal{M}$

$$\begin{aligned} \Pr[C = c | M = m] &= \Pr[\mathsf{Enc}_K(m) = c] \\ &= \Pr[m \oplus K = c] \\ &= \Pr[K = m \oplus c] \\ &= 2^{-l} \end{aligned}$$

key is uniformly distributed

Perfect Secrecy of OTP

- Total probability: for any c in space C

$$\begin{aligned}\Pr[C=c] &= \sum_{m'\in\mathcal{M}} \Pr[C=c \cap M=m'] \\ &= \sum_{m'\in\mathcal{M}} \Pr[C=c|M=m'] \cdot \Pr[M=m'] \\ &= 2^{-l} \cdot \sum_{m'\in\mathcal{M}} \Pr[M=m'] = 2^{-l}\cdot 1 = 2^{-l}\end{aligned}$$

- Finally, we have

$$\Pr[M=m|C=c] = \frac{2^{-l}\cdot \Pr[M=m]}{2^{-l}} = \Pr[M=m]$$

Limitations of OTP

- Key is as long as message
    - Cannot decide message size in advance
    - Why not share the message directly while sharing the key

- Use each key only once

$$
\begin{aligned}
c \oplus c' &= (m \oplus k) \oplus (m' \oplus k) = m \oplus (k \oplus k) \oplus m' \\
&= m \oplus \{0\}^\lambda \oplus m' = m \oplus m'
\end{aligned}
$$

$$k = m \oplus c$$

OTP is Optimal

- OTP is optimal for perfect secrecy
  - Key size is the <u>smallest</u> we can get

- If perfectly secret, then key space size $|\mathcal{K}|$ must be greater than or equal to message space size $|\mathcal{M}|$

- Prove $|\mathcal{K}| < |\mathcal{M}|$ cannot be perfectly secret
  - Uniformly distribution over message space $\mathcal{M}$
  - A ciphertext c occurs with non-zero probability

OTP is Optimal

- $\mathcal{M}$(c): the set of messages that are possible decryption of ciphertext c

$$\mathcal{M}(c) = \{m | m = \mathsf{Dec}_k(c) \text{ for some } k \in \mathcal{K}\}$$

- Decryption algorithm is deterministic, each m in $\mathcal{M}$(c) should be decrypted by a different key, therefore $|\mathcal{M}(c)| <= |\mathcal{K}|$

OTP is Optimal

- Learn $|\mathcal{M}(c)| \le |\mathcal{K}|$, assume $|\mathcal{K}| < |\mathcal{M}|$,

  —> $|\mathcal{M}(c)| < |\mathcal{M}|$

  —> some m' in $\mathcal{M}$ but not in $\mathcal{M}(c)$

  - m' in $\mathcal{M}$ and uniformly distribution over $\mathcal{M}$:

$$\Pr[M = m'] > 0$$

  - m' not in $\mathcal{M}(c)$

$$\Pr[M = m' | C = c] = 0$$

- However, perfect secrecy needs

$$\Pr[M = m' | C = c] = \Pr[M = m']$$

Additional Reading

Chapter 2, *Introduction to Modern Cryptography, Drs. J. Katz and Y. Lindell, 2nd edition*