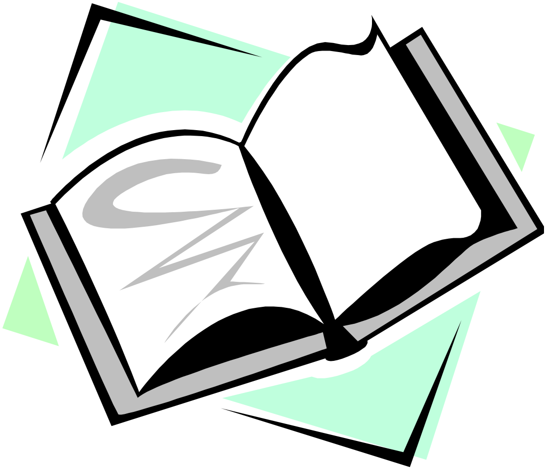
Cryptography
CS 555

Topic 3: One-time Pad and Perfect Secrecy

Outline and Readings

- Outline
  - One-time pad
  - Perfect secrecy
  - Limitation of perfect secrecy
  - Usages of one-time pad



- Readings:
  - Katz and Lindell: Chapter 2

One-Time Pad

- Fix the vulnerability of the Vigenere cipher by using very long keys

- Key is a random string that is at least as long as the plaintext
- Encryption is similar to shift cipher
- Invented by Vernam in the 1920s

One-Time Pad

Let Z_m ={0,1,…,m-1} be the alphabet.

Plaintext space = Ciphtertext space = Key space = $(Z_m)^n$

The key is chosen uniformly randomly

Plaintext $X = (x_1\ x_2\ \ldots\ x_n)$

Key $K = (k_1\ k_2\ \ldots\ k_n)$

Ciphertext $Y = (y_1\ y_2\ \ldots\ y_n)$

$e_k(X) = (x_1+k_1\ \ x_2+k_2\ \ldots\ x_n+k_n) \bmod m$

$d_k(Y) = (y_1-k_1\ \ y_2-k_2\ \ldots\ \ y_n-k_n) \bmod m$

The Binary Version of One-Time Pad

Plaintext space = Ciphtertext space =

Keyspace = $\{0,1\}^n$

Key is chosen randomly

For example:

- Plaintext is 11011011
- Key is 01101001
- Then ciphertext is 10110010

Bit Operators

- Bit AND

  $0 \wedge 0 = 0$ $0 \wedge 1 = 0$ $1 \wedge 0 = 0$ $1 \wedge 1 = 1$

- Bit OR

  $0 \vee 0 = 0$ $0 \vee 1 = 1$ $1 \vee 0 = 1$ $1 \vee 1 = 1$

- Addition mod 2 (also known as Bit XOR)

  $0 \oplus 0 = 0$ $0 \oplus 1 = 1$ $1 \oplus 0 = 1$ $1 \oplus 1 = 0$

- Can we use operators other than Bit XOR for binary version of One-Time Pad?

How Good is One-Time Pad?

- Intuitively, it is secure …
  - The key is random, so the ciphertext is completely random
- How to formalize the confidentiality requirement?
  - Want to say “certain thing” is not learnable by the adversary (who sees the ciphertext). But what is the “certain thing”?
- Which (if any) of the following is the correct answer?
  - The key.
  - The plaintext.
  - Any bit of the plaintext.
  - **Any information about the plaintext.**
    - E.g., the first bit is 1, the parity is 0, or that the plaintext is not “aaaa”, and so on

Perfect Secrecy: Shannon (Information-Theoretic) Security

- Basic Idea: Ciphertext should provide no "information" about Plaintext
- Have several equivalent formulations:
  - The two random variables **M** and **C** are independent
  - Observing what values **C** takes does not change what one believes the distribution **M** is
  - Knowing what is value of **M** does not change the distribution of **C**
  - Encrypting two different messages m_0 and m_1 results in exactly the same distribution.

Perfect Secrecy Definition 1

Definition 2.1 (From textbook). (**Gen,Enc,Dec)** over a message space $\mathcal{M}$ is perfectly secure if

$\forall$ probability distribution over $\mathcal{M}$

$\forall$ message $m \in \mathcal{M}$

$\forall$ ciphertext $c \in \mathcal{C}$ for which $\Pr[C=c] > 0$

We have

$$\Pr[\mathbf{M}=m \mid C=c] = \Pr[\mathbf{M} = m].$$

Perfect Secrecy Definition 0

Definition. (**Gen,Enc,Dec)** over a message space $\mathcal{M}$ is perfectly secure if

$\forall$ probability distribution over $\mathcal{M}$

The random variables **M** and **C** are independent.

That is,

$\forall$ message $m \in \mathcal{M}$

$\forall$ ciphertext $c \in \mathcal{C}$

$\Pr[\mathbf{M}=m \wedge C=c] = \Pr[\mathbf{M}=m]\Pr[\mathbf{C}=c]$

Definition 0 equiv. Definition 1

- Definition 0 implies Definition 1
  - Idea: Given Pr [**M=**m$\wedge$C=c] = Pr [**M** = m] Pr [**C** = c], for any c such that Pr [**C** = c] > 0, divide both sides of the above with Pr [**C** = c], we have Pr [**M=**m | C=c] = Pr [**M** = m].
- Definition 1 implies Definition 0
  - Idea: $\forall$ c$\in\mathcal{C}$ s.t. Pr[C=c] > 0

    Pr [**M=**m | C=c] = Pr [**M** = m], multiple both side by Pr[C=c], obtain Pr [**M=**m$\wedge$C=c] = Pr [**M** = m] Pr [**C** = c]

    $\forall$ c$\in\mathcal{C}$ s.t. Pr[C=c] = 0 we have

    Pr [**M=**m$\wedge$C=c] = 0 = Pr [**M=**m] Pr[C=c]

Perfect Secrecy. Definition 2.

Definition in Lemma 2.2. (**Gen,Enc,Dec)** over a message space $\mathcal{M}$ is perfectly secure if

$\forall$ probability distribution over $\mathcal{M}$

$\forall$ message $m \in \mathcal{M}$ (assuming Pr[**M**=m]>0)

$\forall$ ciphertext $c \in \mathcal{C}$

We have

$$\Pr[\mathbf{C}=c \mid \mathbf{M}=m] = \Pr[\mathbf{C} = c].$$

- Equivalence with Definition 0 straightforward.

Perfect Indistinguishability

Definition in Lemma 2.3. (**Gen,Enc,Dec)** over a message space $\mathcal{M}$ is perfectly secure if

$\forall$ probability distribution over $\mathcal{M}$

$\forall$ messages $m_0, m_1 \in \mathcal{M}$

$\forall$ ciphertext $c \in \mathcal{C}$

We have

$$\Pr[\mathbf{C}=c \mid \mathbf{M}=m_0] = \Pr[\mathbf{C}=c \mid \mathbf{M}=m_1]$$

To prove that this definition implies Definition 0, consider Pr [**C**=c].

Adversarial Indistinguishability

- Define an experiment called **PrivK$^{\mathbf{eav}}$**:
  - Involving an Adversary and a Challenger
  - Instantiated with an Adv algorithm A, and an encryption scheme Π = (Gen, Enc, Dec)

Challenger		Adversary
$k \leftarrow \text{Gen}()$	$\xleftarrow{m_0,\ m_1}$	chooses $m_0, m_1 \in \mathcal{M}$
$b \leftarrow_R \{0,1\}$	$\xrightarrow{C=\mathbf{E}_k[m_b]}$	
	$\xleftarrow{b' \in \{0,1\}}$	

PrivK$^{\mathbf{eav}}$ = 1 if b=b', and PrivK$^{\mathbf{eav}}$ = 0 if $b \neq b'$

Adversarial Indistinguishability (con'd)

Definition 2.4. (**Gen,Enc,Dec)** over a message space $\mathcal{M}$ is perfectly secure if

$\forall$ adversary A it holds that

$$\Pr[\mathbf{PrivK}^{\mathbf{eav}}_{\mathbf{A},\Pi}=1] = ½$$

Proposition 2.5. Definition 2.1 is equivalent to Definition 2.4.

Perfect Secrecy

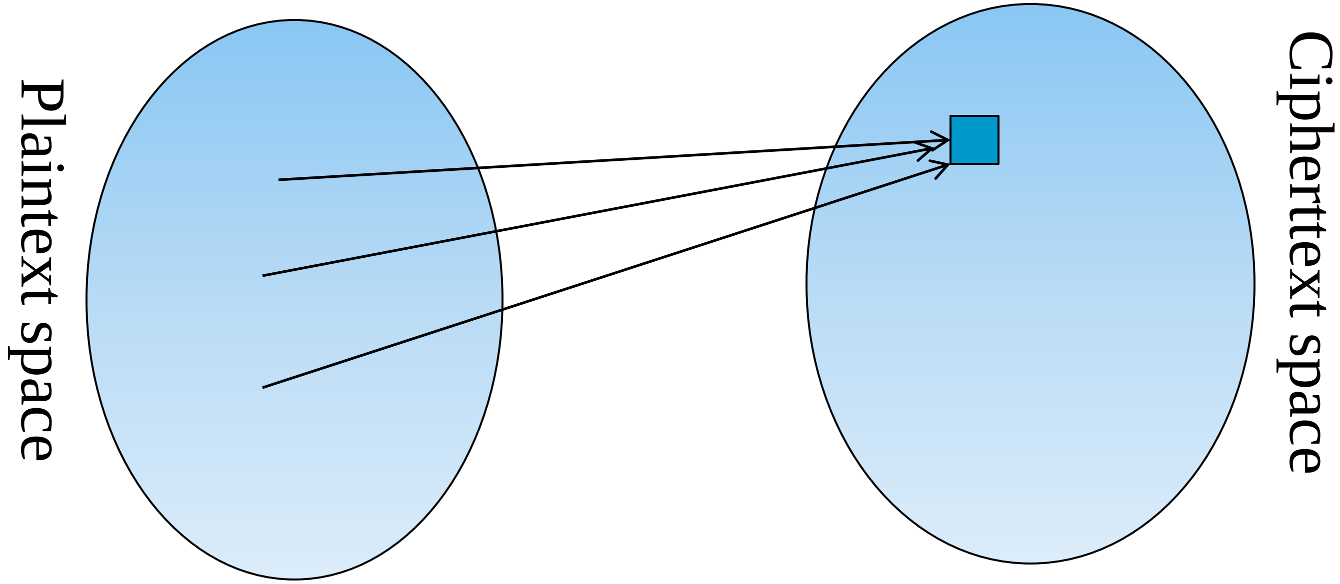
- Fact: When keys are uniformly chosen in a cipher, a deterministic cipher has Shannon security iff. the number of keys encrypting m to c is the same for any pair of (m,c)

- One-time pad has perfect secrecy (Proof?)
  - In textbook

The “Bad News” Theorem for Perfect Secrecy

- Question: OTP requires key as long as messages, is this an inherent requirement for achieving perfect secrecy?
- Answer. Yes. Perfect secrecy implies that
  key-length ≥ msg-length

Proof:



- Implication: Perfect secrecy difficult to achieve in practice

Key Randomness in One-Time Pad

- One-Time Pad uses a very long key, what if the key is not chosen randomly, instead, texts from, e.g., a book are used as keys.
  - this is not One-Time Pad anymore
  - this does not have perfect secrecy
  - this can be broken
  - How?
- The key in One-Time Pad should never be reused.
  - If it is reused, it is Two-Time Pad, and is insecure!
  - Why?

Usage of One-Time Pad

- To use one-time pad, one must have keys as long as the messages.
- To send messages totaling certain size, sender and receiver must agree on a shared secret key of that size.
  - typically by sending the key over a secure channel
- This is difficult to do in practice.
- Can’t one use the channel for send the key to send the messages instead?
- Why is OTP still useful, even though difficult to use?

Usage of One-Time Pad

- The channel for distributing keys may exist at a different time from when one has messages to send.

- The channel for distributing keys may have the property that keys can be leaked, but such leakage will be detected
  - Such as in Quantum cryptography

Coming Attractions …

- Cryptography: Block ciphers, encryption modes, cryptographic functions