CS408
Cryptography & Internet Security

Lecture 5:
One-time pad

Reza Curtmola
Department of Computer Science
NJIT

The One-Time Pad (OTP)

- Basic Idea:
  - Use a key as long as the plaintext
  - The key is a random string
- Encryption: perform XOR between plaintext and key
- Decryption: perform XOR between ciphertext and key

The One-Time Pad (OTP)

- Use the binary representation (plaintext, key, ciphertext are sequences of 0s and 1s)
  - Plaintext is $x = (x_1, x_2, \ldots, x_n)$
  - Key is $k = (k_1, k_2, \ldots, k_n)$
  - Ciphertext is $y = (y_1, y_2, \ldots, y_n)$
- Encryption: $y = E_k(x) = (x_1 \oplus k_1, x_2 \oplus k_2, \ldots, x_n \oplus k_n)$
- Decryption: $x = D_k(y) = (y_1 \oplus k_1, y_2 \oplus k_2, \ldots, y_n \oplus k_n)$

- $\oplus$ means exclusive OR (XOR), it is a binary bitwise operator
  - $0 \oplus 0 = 0$; $0 \oplus 1 = 1$; $1 \oplus 0 = 1$; $1 \oplus 1 = 0$
  - $a \oplus b$ is equivalent with $(a+b) \bmod 2$

- For example:
  - Plaintext is 11011011
  - Key is 01101001
  - Then ciphertext is 10110010 (note, there is no carriage!)

Bit Operators

- Bitwise AND

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

- Bitwise OR

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

- Addition mod 2 (also known as Bitwise XOR)

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

How Secure is the One-Time Pad?

- Intuitively, it is secure …
- The key is random, so the ciphertext is completely random

Is one-time pad practical?

- Remember:
  - The key must be chosen at random
  - The key must be at least as long as the plaintext
  - The key must never be reused
- One-time pad is not practical because:
  - Keys can be very long: expensive to produce and expensive to transmit
  - A key cannot be reused (every encryption must use a different key, which should be established through a secure channel before the actual communication)

Is one-time pad practical?

- Distributing one-time pad keys is inconvenient and poses significant security risk
  - Large storage media can be used to carry a large one-time pad key (e.g., thumb drives, DVDs, etc.)
  - The large one-time pad key can then be used to encrypt many shorter messages
  - Still, it may be a challenge:
    - to securely transport the media device
    - to securely destroy the device

    A 4.7 GB DVD-R full of one-time-pad data, if shredded into particles 1 mm^2 in size, leaves over 100 kibibits of (admittedly hard to recover, but not impossibly so) data on each particle. (from Wikipedia)

Names connected with OTP

- Co-inventors of One-time-pad
  - **Joseph Mauborgne** (1881-1971) became a Major General in the United States Army
  - **Gilbert Vernam** (1890 - 1960), was AT&T Bell Labs engineer
- Security of OTP
  - **Claude Shannon** (1916 - 2001), American electronics engineer and mathematician, was "the father" of information theory.

Some historical facts

- VENONA project:
  - during WWII, the US and the UK intercepted encrypted messages sent by the intelligence agencies of the Soviet Union
  - The Soviets made the mistake of reusing one-time pads for encrypting messages
  - The encrypted messages were decrypted gradually between 1946 - 1980

Shannon (Information-Theoretic) Security

- Basic Idea: Ciphertext should provide no "information" about Plaintext
- We also say such a scheme has perfect secrecy.
  - No matter how powerful an adversary is, the scheme cannot be broken if it has perfect secrecy
- One-time pad has perfect secrecy
  - E.g., suppose that the ciphertext is "wpslq", can we say any plaintext is more likely than another plaintext?

- Result due to Shannon, 1949.

  C. E. Shannon, "Communication Theory of Secrecy Systems", Bell System Technical Journal, vol.28-4, pp 656--715, 1949.

Unconditional Security

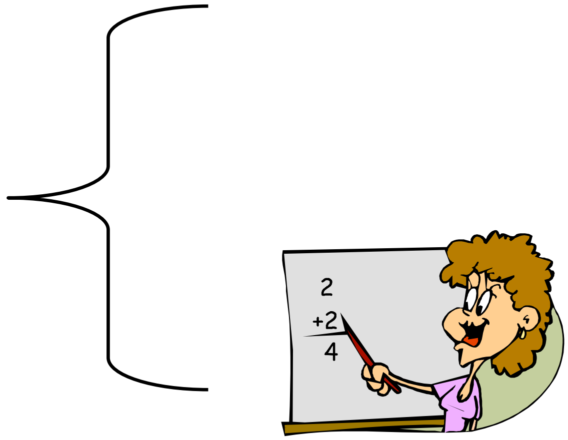
- The adversary has unlimited computational resources.
- Analysis is made by using probability theory.
- Perfect secrecy: observation of the ciphertext provides no information to an adversary.
- Result due to Shannon, 1949.

C. E. Shannon, "Communication Theory of Secrecy Systems", Bell System Technical Journal, vol.28-4, pp 656--715, 1949.

Security of one-time pad

- What happens if key is reused in one-time pad?
  - $y_1 = E_k(x_1) = x_1 \oplus k$
    $y_2 = E_k(x_2) = x_2 \oplus k$
  - Then, adversary can compute
    $y_1 \oplus y_2 = x_1 \oplus k \oplus x_2 \oplus k = x_1 \oplus x_2$
    If adversary knows x_1, it can find out x_2!

Begin Math



Random Variable

Definitions

- A random variable is a variable whose value is not known, and which can take different values
  - A probability distribution describes the probabilities of different values occurring
- A **discrete random variable**, **X,** consists of:
  - a countable set X of values it may take (e.g., a set of integers)
  - a probability distribution defined over X

The probability that the random variable **X** takes on the value x is denoted **Pr**[**X** =x]; sometimes, we will abbreviate this to **Pr**[x] if the random variable **X** is fixed.

It must be that:

$$0 \leq \Pr[x] \leq 1 \text{ for all } x \in X$$

$$\sum_{x \in X} \Pr[x] = 1$$

Relationships between Two Random Variables

Definitions

Assume X and Y are two random variables, we define:

- conditional probability: Pr[x|y] is the probability that X takes on the value x given that Y takes value y
-
- joint probability: Pr[x, y] = Pr[x|y] Pr[y] = Pr[y|x] Pr[x] is the probability that X takes value x and Y takes value y
- independent random variables: X and Y are said to be independent if Pr[x,y]=Pr[x] Pr[y], for all $x \in X$ and all $y \in Y$

Elements of Probability Theory

Find the conditional probability of event X given the conditional probability of event Y and the unconditional probabilities of events X and Y.

Bayes' Theorem

If Pr[y] > 0 then:

$$\Pr[x \mid y] = \frac{\Pr[x]\Pr[y \mid x]}{\Pr[y]}$$

Corollary

X and Y are independent random variables if and only if Pr[x|y] = Pr[x], for all $x \in X$ and all $y \in Y$.

End Math

}

Ciphers Modeled by Random Variables

Consider a cipher (P, C, K, E, D). We assume that:

1. there is a probability distribution on the plaintext (message) space
2. the key space also has a probability distribution. We assume:
   - the key is chosen before the message and
   - the key and the plaintext are independent random variables
3. the ciphertext is also a random variable

Perfect Secrecy

Definition

Informally, perfect secrecy means that an attacker can not obtain any information about the plaintext by observing the ciphertext.

What type of attack is this?

Definition

A cryptosystem has perfect secrecy if

Pr[x|y] = Pr[x], for all x ∈ P and y ∈ C,

where P is the set of plaintexts and C is the set of ciphertexts.

What can I say about Pr[x|y] and Pr[x], for all x ∈ P and y ∈ C,

Bayes:

$$\Pr[x \mid y] = \frac{\Pr[x]\Pr[y \mid x]}{\Pr[y]}$$

given: $\Pr[x]$

Don't know it, but can be computed: $\Pr[y \mid x]$

Don't know it, but can be computed: $\Pr[y]$

KNOWN: Pr[x], Pr[k]

C(k): the set of all possible ciphertexts if key is k.

$$\Pr[y] = \sum_{k: y \in C(k)} \Pr[k]\Pr[x] \qquad \Pr[y \mid x] = \sum_{k: x = D_k(y)} \Pr[k]$$

$$\Pr[x \mid y] = \frac{\Pr[x] \sum_{k: x = D_k(y)} \Pr[k]}{\sum_{k: y \in C(k)} \Pr[k]\Pr[x]}$$

One-time Pad has Perfect Secrecy

- P, C, K = $\{0,1\}^n$, key k is chosen at random and is used once per message
- We need to show that $\forall x \; \forall y$, $Pr[x \mid y] = Pr[x]$

  (for all plaintexts and ciphertexts, the prob. of finding information about the plaintext x given a ciphertext y is the same as the prob. of finding information about the plaintext given just x)

  $Pr[x|y] = Pr[x] \, Pr[y|x] / Pr[y]$ (cf. Bayes' theorem)

  $= Pr[x] \, Pr[k] / \sum_{x \in X} (Pr[x] \, Pr[k])$

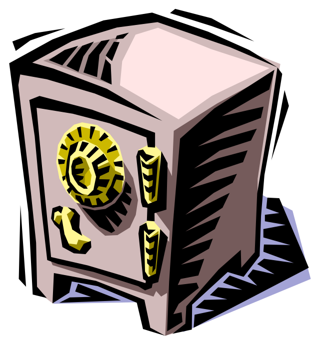
  $= Pr[x] \, 1/2^n / \sum_{x \in X} (Pr[x] \, 1/2^n)$

  $= Pr[x] / \sum_{x \in X} (Pr[x])$

  $= Pr[x]$

Modern Cryptography

- One-time pad requires the length of the key to be the length of the plaintext and the key to be used only once. Difficult to manage.
- Alternative: design cryptosystems, where a key is used more than once.
- What about the attacker? Resource constrained, make it infeasible for adversary to break the cipher.



Theoretically-motivated Principles

- Change frequently all cryptographic keys
- Make plaintext as random as possible (e.g., via compression)
- Use probabilistic encryption

Recommended Reading

- Chapter 2.9
- Chapter 15.4 (for Perfect Secrecy of OTP)