Introduction to Modern Cryptography

Michele Ciampi

(Slides courtesy of Prof. Jonathan Katz)

Lecture 03, part 2

Perfect Secrecy

Probability Review

Random variable (*RV*)

Variable that takes on (discrete) values with certain probabilities

Probability distribution (*PD*)

A *PD* for a *RV* specifies the probabilities with which the variable takes on each possible value

- Each probability must be between **0** and **1**
- The probabilities must sum to **1**

Probability Review

Event

A particular occurrence in some experiment:

- $\mathbf{Pr}[\boldsymbol{E}]$: probability of event $\boldsymbol{E}$

Conditional probability

Probability that one event occurs, given that some other event occurred:

- $\mathbf{Pr}[\boldsymbol{A}|\boldsymbol{B}] = \mathbf{Pr}[\boldsymbol{A} \textbf{ and } \boldsymbol{B}]/\mathbf{Pr}[\boldsymbol{B}] \equiv \mathbf{Pr}[\boldsymbol{AB}]/\mathbf{Pr}[\boldsymbol{B}]$

Independence

Two *RV* $\boldsymbol{X}, \boldsymbol{Y}$ are **independent** if:

- $\forall\, \boldsymbol{x}, \boldsymbol{y}: \ \mathbf{Pr}[\boldsymbol{X} = \boldsymbol{x} | \boldsymbol{Y} = \boldsymbol{y}] = \mathbf{Pr}[\boldsymbol{X} = \boldsymbol{x}]$

Probability Review

Law of total probability

Let $\boldsymbol{E_1 \dots E_n}$ are a partition of all possibilities. Then $\forall \boldsymbol{A}$:

$$\begin{aligned} \mathbf{Pr}[A] &= \sum_i \mathbf{Pr}[AE_i] \\ &= \sum_i \mathbf{Pr}[A|E_i]\ \mathbf{Pr}[E_i] \end{aligned}$$

Note

$\mathbf{Pr}[A|B] = \mathbf{Pr}[AB]/\mathbf{Pr}[B] \implies \mathbf{Pr}[AB] = \mathbf{Pr}[A|B]\mathbf{Pr}[B]$

Notation (recall)

- $\mathcal{K}$ (key space): set of all possible keys
- $\mathcal{M}$ (message space): set of all possible messages
- $\mathcal{C}$ (ciphertext space): set of all possible ciphertexts

Probability Distributions

The random variable $\boldsymbol{M}$

- $\boldsymbol{M}$ is the *RV* denoting the value of the message
- $\boldsymbol{M}$ ranges over $\boldsymbol{\mathcal{M}}$; context dependent
- Reflects the likelihood of different messages being sent, given the attacker's **prior knowledge**

Example

$$\mathbf{Pr}[\boldsymbol{M} = \textbf{attack today}] = \mathbf{0.7}$$
$$\mathbf{Pr}[\boldsymbol{M} = \textbf{don't attack}] = \mathbf{0.3}$$

Probability Distributions

The random variable $\boldsymbol{K}$

- $\boldsymbol{K}$ is the *RV* denoting the key
- $\boldsymbol{K}$ ranges over $\mathcal{K}$
- Fix some encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$
- Gen defines a probability distribution for $\boldsymbol{K}$:

$$\mathbf{Pr}[\boldsymbol{K} = \boldsymbol{k}] = \mathbf{Pr}[\mathsf{Gen} \text{ } \mathbf{outputs\ key} \text{ } \boldsymbol{k}]$$

Probability Distributions

RV $\boldsymbol{M}$ and $\boldsymbol{K}$ are independent

Require that parties don't pick the key based on the message, or the message based on the key

Probability distributions

The random variable $\boldsymbol{C}$

- Fix some encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, and some *PD* for $\boldsymbol{M}$
- Consider the following (randomized) experiment:
  - Generate a key $\boldsymbol{k}$ using Gen
  - Choose a message $\boldsymbol{m}$, according to the given *PD*
  - Compute $\boldsymbol{c} \leftarrow \mathsf{Enc}_{\boldsymbol{k}}(\boldsymbol{m})$
- **This defines a distribution on the ciphertext**
- Let $\boldsymbol{C}$ be a *RV* denoting the value of the ciphertext in this experiment

Example 1: the PD of $\boldsymbol{C}$ (Shift Cipher)

- $\forall\ \boldsymbol{k} \in \{\mathbf{0} \ldots \mathbf{25}\} \implies \mathbf{Pr}[\boldsymbol{K} = \boldsymbol{k}] = \mathbf{1/26}$
- Let $|\boldsymbol{M}| = \mathbf{2}$, $\boldsymbol{m} \in \{\boldsymbol{a}, \boldsymbol{z}\}$ and

$$\mathbf{Pr}[\boldsymbol{M} = \boldsymbol{a}] = \mathbf{0.7}$$
$$\mathbf{Pr}[\boldsymbol{M} = \boldsymbol{z}] = \mathbf{0.3}$$

- What is $\mathbf{Pr}[\boldsymbol{C} = \boldsymbol{b}]$?

Example 1: the PD of $\boldsymbol{C}$ (Shift Cipher)

What is $\mathbf{Pr}[\boldsymbol{C} = \boldsymbol{b}]$?

Either $\boldsymbol{M} = \boldsymbol{a}$ and $\boldsymbol{K} = \mathbf{1}$ or $\boldsymbol{M} = \boldsymbol{z}$ and $\boldsymbol{K} = \mathbf{2}$

$$
\begin{aligned}
&\mathbf{Pr}[\boldsymbol{C} = \boldsymbol{b}] = \\
&= \mathbf{Pr}[\boldsymbol{M} = \boldsymbol{a}]\ \mathbf{Pr}[\boldsymbol{K} = \mathbf{1}] + \mathbf{Pr}[\boldsymbol{M} = \boldsymbol{z}]\ \mathbf{Pr}[\boldsymbol{K} = \mathbf{2}] \\
&= \mathbf{0.7}\ \frac{\mathbf{1}}{\mathbf{26}} + \mathbf{0.3}\ \frac{\mathbf{1}}{\mathbf{26}} = \frac{\mathbf{1}}{\mathbf{26}}
\end{aligned}
$$

Example 2: the PD of $\boldsymbol{C}$ (Shift Cipher)

Let $|\boldsymbol{M}| = \mathbf{2}$, $\boldsymbol{m} \in \{\mathbf{one}, \mathbf{ten}\}$ and

$$\mathbf{Pr}[M = \mathbf{one}] = \mathbf{Pr}[M = \mathbf{ten}] = \mathbf{1/2}$$

What is $\mathbf{Pr}[\boldsymbol{C} = \mathbf{rqh}]$?

$$\begin{aligned}
&\mathbf{Pr}[C = \mathbf{rqh}] = \\
&= \mathbf{Pr}[C = \mathbf{rqh} | M = \mathbf{one}]\ \mathbf{Pr}[M = \mathbf{one}] \\
&+ \mathbf{Pr}[C = \mathbf{rqh} | M = \mathbf{ten}]\ \mathbf{Pr}[M = \mathbf{ten}] \\
&= \frac{\mathbf{1}}{\mathbf{26}}\ \frac{\mathbf{1}}{\mathbf{2}} + \mathbf{0}\ \frac{\mathbf{1}}{\mathbf{2}} = \frac{\mathbf{1}}{\mathbf{52}}
\end{aligned}$$

Perfect Secrecy (informal)

Regardless of any **prior** information the attacker has about the plaintext, the ciphertext should leak no **additional** information about the plaintext

- Attacker's information about the plaintext = attacker-known distribution of $\boldsymbol{M}$
- Perfect secrecy means that **observing the ciphertext should not change the attacker's knowledge about the distribution of $\boldsymbol{M}$**

Perfect Secrecy (formal)

Definition

Encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\boldsymbol{\mathcal{M}}$ and ciphertext space $\boldsymbol{\mathcal{C}}$ is **perfectly secret** if $\forall PD$ over $\boldsymbol{\mathcal{M}}$, $\forall \boldsymbol{m} \in \boldsymbol{\mathcal{M}}$, and $\forall \boldsymbol{c} \in \boldsymbol{\mathcal{C}}$ with $\mathbf{Pr}[\boldsymbol{C} = \boldsymbol{c}] > \mathbf{0}$, it holds that

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

i.e. the distribution of $\boldsymbol{M}$ does not change conditioned on observing the ciphertext

Example 3: Perfect Secrecy (Shift Cipher)

- Let
$$\mathbf{Pr}[\boldsymbol{M} = \mathbf{one}] = \mathbf{Pr}[\boldsymbol{M} = \mathbf{ten}] = \mathbf{1/2}$$

- Take $\boldsymbol{m} = \mathbf{ten}$ and $\boldsymbol{c} = \mathbf{rqh}$. Then
$$\mathbf{Pr}[\boldsymbol{M} = \mathbf{ten} | \boldsymbol{C} = \mathbf{rqh}] = \mathbf{0} \neq \mathbf{Pr}[\boldsymbol{M} = \mathbf{ten}]$$

- The *PD* of $\boldsymbol{M}$ changes upon observing the ciphertext

Bayes's theorem

$$\mathbf{Pr}[A|B] = \frac{\mathbf{Pr}[B|A]\ \mathbf{Pr}[A]}{\mathbf{Pr}[B]}$$

$$\begin{aligned} \mathbf{Pr}[A|B] &= \mathbf{Pr}[AB]/\mathbf{Pr}[B]\ , \\ \mathbf{Pr}[B|A] &= \mathbf{Pr}[AB]/\mathbf{Pr}[A] \\ \implies \mathbf{Pr}[AB] &= \mathbf{Pr}[B|A]\mathbf{Pr}[A]\ , \\ \implies \mathbf{Pr}[A|B] &= \frac{\mathbf{Pr}[B|A]\ \mathbf{Pr}[A]}{\mathbf{Pr}[B]}\ . \end{aligned}$$

Example 4: Perfect Secrecy and Shift Cipher

Let $|\boldsymbol{M}| = \mathbf{3}$, $\boldsymbol{m} \in \{\mathbf{hi}, \mathbf{no}, \mathbf{in}\}$ and

$$\mathbf{Pr}[M = \mathbf{hi}] = \mathbf{0.3}$$
$$\mathbf{Pr}[M = \mathbf{no}] = \mathbf{0.2}$$
$$\mathbf{Pr}[M = \mathbf{in}] = \mathbf{0.5}$$

What is $\mathbf{Pr}$ of $(\boldsymbol{M} = \mathbf{hi})$ given $(\boldsymbol{C} = \mathbf{xy})$?

$$\mathbf{Pr}[M = \mathbf{hi}|C = \mathbf{xy}] =$$
$$= \frac{\mathbf{Pr}[C = \mathbf{xy}|M = \mathbf{hi}]\ \mathbf{Pr}[M = \mathbf{hi}]}{\mathbf{Pr}[C = \mathbf{xy}]}$$

Example 4: Perfect Secrecy and Shift Cipher

$$\mathbf{Pr}[C = \mathbf{xy} | M = \mathbf{hi}] = \mathbf{1/26}$$

By the law of total probability:

$$\begin{aligned}
&\mathbf{Pr}[C = \mathbf{xy}] = \\
&\mathbf{Pr}[C = \mathbf{xy} | M = \mathbf{hi}]\ \mathbf{0.3} + \\
&\mathbf{Pr}[C = \mathbf{xy} | M = \mathbf{no}]\ \mathbf{0.2} + \\
&\mathbf{Pr}[C = \mathbf{xy} | M = \mathbf{in}]\ \mathbf{0.5} \\
&= \mathbf{(1/26)\ 0.3 + (1/26)\ 0.2 + 0\ 0.5 = 1/52}
\end{aligned}$$

Example 4: Perfect Secrecy and Shift Cipher

$$\begin{aligned}
&\mathbf{Pr}[M = \mathbf{hi} | C = \mathbf{xy}] = \\
&= \frac{\mathbf{Pr}[C = \mathbf{xy} | M = \mathbf{hi}]\ \mathbf{Pr}[M = \mathbf{hi}]}{\mathbf{Pr}[C = \mathbf{xy}]} \\
&= \frac{\mathbf{(1/26)\ 0.3}}{\mathbf{(1/52)}} = \mathbf{0.6} \\
&\neq \mathbf{Pr}[M = \mathbf{hi}] = \mathbf{0.3}
\end{aligned}$$

Conclusion

- The Shift Cipher is not perfectly secret!
- How to construct a perfectly secret scheme?
- $\implies$ next lecture!

End

Reference: From Chapter 2 until (included) Pag. 30 of the book.