Fundamentals of Information & Network Security ECE 471/571

Lecture #8-9: Definitions of Security/Secrecy

Instructor: Ming Li
Dept of Electrical and Computer Engineering
University of Arizona

Do There Exist “**Unbreakable**” Ciphers?

Security Notions

- <u>Unconditionally (perfect) secure</u>: A cryptosystem is said to be unconditionally secure if it cannot be broken even if Eve has an unbounded amount of computational resources at her disposal.

- <u>Provably secure</u>: Prove security by means of reduction to a well known mathematical problem that is thought to be difficult to solve, e.g., factoring large numbers, discrete logarithm problem

- <u>Computationally secure</u>: if cost of breaking the cipher exceeds the value of the encrypted information, or time required to break the cipher exceeds the useful lifetime of the information, practical security

How to define “Perfect Secrecy”?

consider the following experiment

(**x** – a message)

1. the key **K** is chosen uniformly at random
2. **y := Enc_K(x)** is given to the adversary

how to
define
security

?

Idea 1

(**x** – a message)

1. the key **K** is chosen uniformly at random
2. $y := \mathrm{Enc}_K(x)$ is given to the adversary

An idea

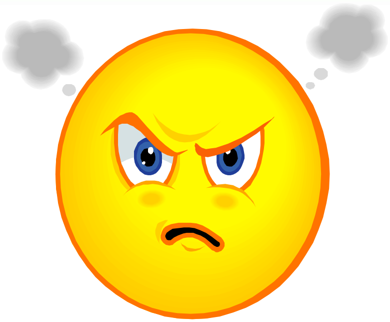
"The adversary should not be able to compute **K**."

A problem

the encryption scheme that "doesn't encrypt":

$$\mathrm{Enc}_K(x) = x$$

satisfies this definition!



Idea 2

(**x** – a message)

1. the key **K** is chosen uniformly at random
2. **$y := Enc_K(x)$** is given to the adversary

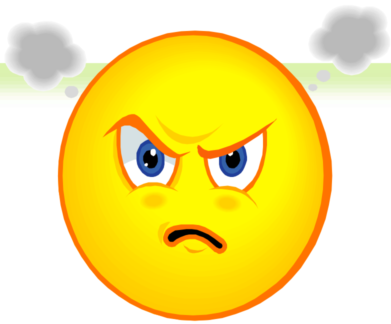
An idea

"The adversary should not be able to compute **x**."

A problem

What if the adversary can compute, e.g., the first half of **x**?

x_1	…	$x_{\|x\|/2}$	?	…	?



Idea 3

(**x** – a message)

1. the key K is chosen uniformly at random
2. **y := Enc$_k$(x)** is given to the adversary

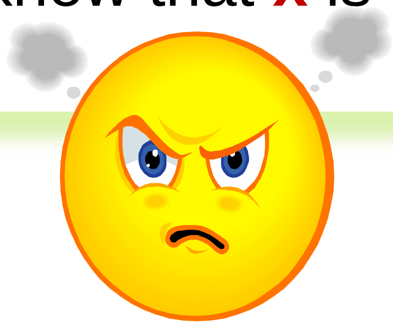
An idea

"The adversary should not learn any information about **x**."

A problem

But he may already have some a priori information about **x**!

For example he may know that **x** is a sentence in English...



Idea 4

(**x** – a message)

1. the key **K** is chosen randomly
2. **$y := Enc_K(x)$** is given to the adversary

An idea

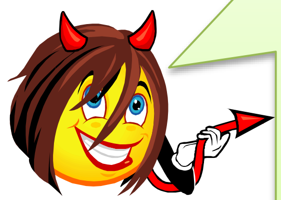
"The adversary should not learn any **additional** information about **x**."

This makes much more sense.

But how to formalize it?

Example

x

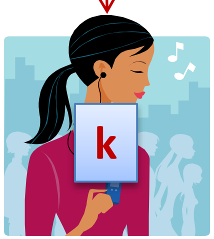


Eve knows that

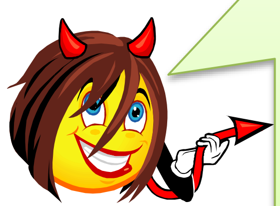
$$\mathbf{x} := \begin{cases} \textit{“I love you”} & \text{with prob. } \mathbf{0.1} \\ \textit{“I don't love you”} & \text{with prob. } \mathbf{0.7} \\ \textit{“I hate you”} & \text{with prob. } \mathbf{0.2} \end{cases}$$

---

x



$y := Enc_K(x)$



Eve **still** knows that

$$\mathbf{x} := \begin{cases} \textit{“I love you”} & \text{with prob. } \mathbf{0.1} \\ \textit{“I don't love you”} & \text{with prob. } \mathbf{0.7} \\ \textit{“I hate you”} & \text{with prob. } \mathbf{0.2} \end{cases}$$

How to formalize the “Idea 4”?

“The adversary should not learn any **additional** information about **x**.”

also called: **information-theoretically** secret

An encryption scheme is **perfectly secret** if

for every random variable **X**

and every $x \in \mathcal{P}$ and $y \in \mathcal{C}$

such that
P(Y = y) > 0

$$P(X = x) = P(X = x \mid (E_K(X)) = y)$$

equivalently: **X** and **E(K,X)** are independent

Probability Calculation

- For a cryptosystem: $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$,where key is randomly generated:

$$\mathbf{Pr}[\mathbf{y} = y] = \sum_{\{K : y \in \mathcal{C}\}} \mathbf{Pr}[\mathbf{K} = K]\mathbf{Pr}[\mathbf{x} = d_K(y)].$$

$$\mathbf{Pr}[\mathbf{y} = y|\mathbf{x} = x] = \sum_{\{K : x = d_k(y)\}} \mathbf{Pr}[\mathbf{K} = K].$$

$$\mathbf{Pr}[\mathbf{x} = x|\mathbf{y} = y] = \frac{\mathbf{Pr}[\mathbf{x} = x] \times \sum_{\{K : x = d_k(y)\}} \mathbf{Pr}[\mathbf{K} = K]}{\mathbf{Pr}[\mathbf{y} = y] = \sum_{\{K : y \in \mathcal{C}\}} \mathbf{Pr}[\mathbf{K} = K]\mathbf{Pr}[\mathbf{x} = d_K(y)]}.$$

Example

- Let's look at an example first…
  - Let $\mathcal{P}$ = {a, b}, with Pr[a] = 0.25 and Pr[b] = 0.75: Let also $\mathcal{K}$ = {K_1,K_2,K_3} having probability distribution of 0.5, 0.25, 0.25, respectively. Let the ciphertext be $\mathcal{C}$ = {1, 2, 3, 4} with the encryption function be given by the following matrix

	a	b
K_1	1	2
K_2	2	3
K_3	3	4

Table 1. The encryption matrix.

Activity: Calculate Pr[x|y] for all x $\in \mathcal{P}$ and y $\in \mathcal{C}$

Is this perfectly secret?

Perfect Secrecy Definition

An encryption scheme is **perfectly secret** if

for every random variable $\mathbf{X}$

and every $x \in \mathcal{P}$ and $y \in \mathcal{C}$

such that $P(Y = y) > 0$

$$P(X = x) = P(X = x \mid E_K(X) = y)$$

equivalently: $\mathbf{X}$ and $E_K(X)$ are independent

Perfect Secrecy Definitions

When $|\mathcal{P}|=|\mathcal{K}|=|\mathcal{C}|$, **K** is uniform chosen, and for every $x \in \mathcal{P}$ and $y \in \mathcal{C}$, there exists a unique key K such that $E_K(x) = y$

⇕

for every **X** we have that: **X** and $E_K(X)$ are independent

⇕

"the distribution of $E_K(X)$ does not depend on **X**"

⇕

for every x_0 and x_1 we have that
$E_K(x_0)$ and $E_K(x_1)$ have the same distribution:
For every y, $Pr[y \mid x_0] = Pr[y \mid x_1]$

A perfectly secret scheme: one-time pad

n – a parameter

$\mathcal{K} = \mathcal{P} = \{0,1\}^n$

component-wise **xor**

Vernam's cipher:

$$E_k(x) = k \text{ xor } x$$
$$D_k(y) = k \text{ xor } y$$

Gilbert Vernam (1890 –1960)

Correctness is trivial:

$$D_k(E_k(x)) = k \text{ xor } (k \text{ xor } x)$$
$$= x$$

Perfect secrecy of the one-time pad

Why perfectly secret?

This is because for every **x**
the distribution of $\mathbf{E_K(x)}$ is uniform
(and hence does not depend on **x**).

for every **y:**
$\mathbf{P(E_K(x) = y) = P(K = x \text{ xor } y) = 2^{-n}}$

Another More Familiar Example…

- Shift cipher with 26 keys uniformly generated with equal probability: is it a perfect secret cryptosystem?

Theorem 1. Let 26 keys be used in the Shift Cipher with equal probability 1/26. For any plaintext probability distribution, the Shift Cipher is perfectly secret.

Observation

One time pad can be **generalized** as follows.

Let **(G,+)** be a group. Let $\mathcal{K} = \mathcal{P} = \mathcal{C} = \mathbf{G}$.

The following is a perfectly secret encryption scheme:

- **Enc(k,x) = x + k**
- **Dec(k,x) = x – k**

Is the one-time pad practical?

1. **The key has to be as long as the message.**
2. **The key cannot be reused**

This is because:

$$E_k(x_0) \text{ xor } E_k(x_1) = (k \text{ xor } x_0) \text{ xor } (k \text{ xor } x_1)$$
$$= x_0 \text{ xor } x_1$$

Practicality?

Generally, the **one-time pad** is **not very practical**, since:
• the key has to be as long as the **total** length of the encrypted messages,
• it is hard to generate truly random strings.

However, it is sometimes used (e.g. in the **military applications**), because of the following advantages:
• **perfect secrecy**,
• short messages can be encrypted using **pencil and paper** .

In the 1960s the Americans and the Soviets established a hotline that was encrypted using the one-time pad.(**additional advantage**: they didn't need to share their secret encryption methods)

Venona project (1946 – 1980)

American **National Security Agency** decrypted **Soviet** messages that were transmitted in the 1940s.

That was possible because the Soviets reused the keys in the one-time pad scheme.