CS171: Cryptography

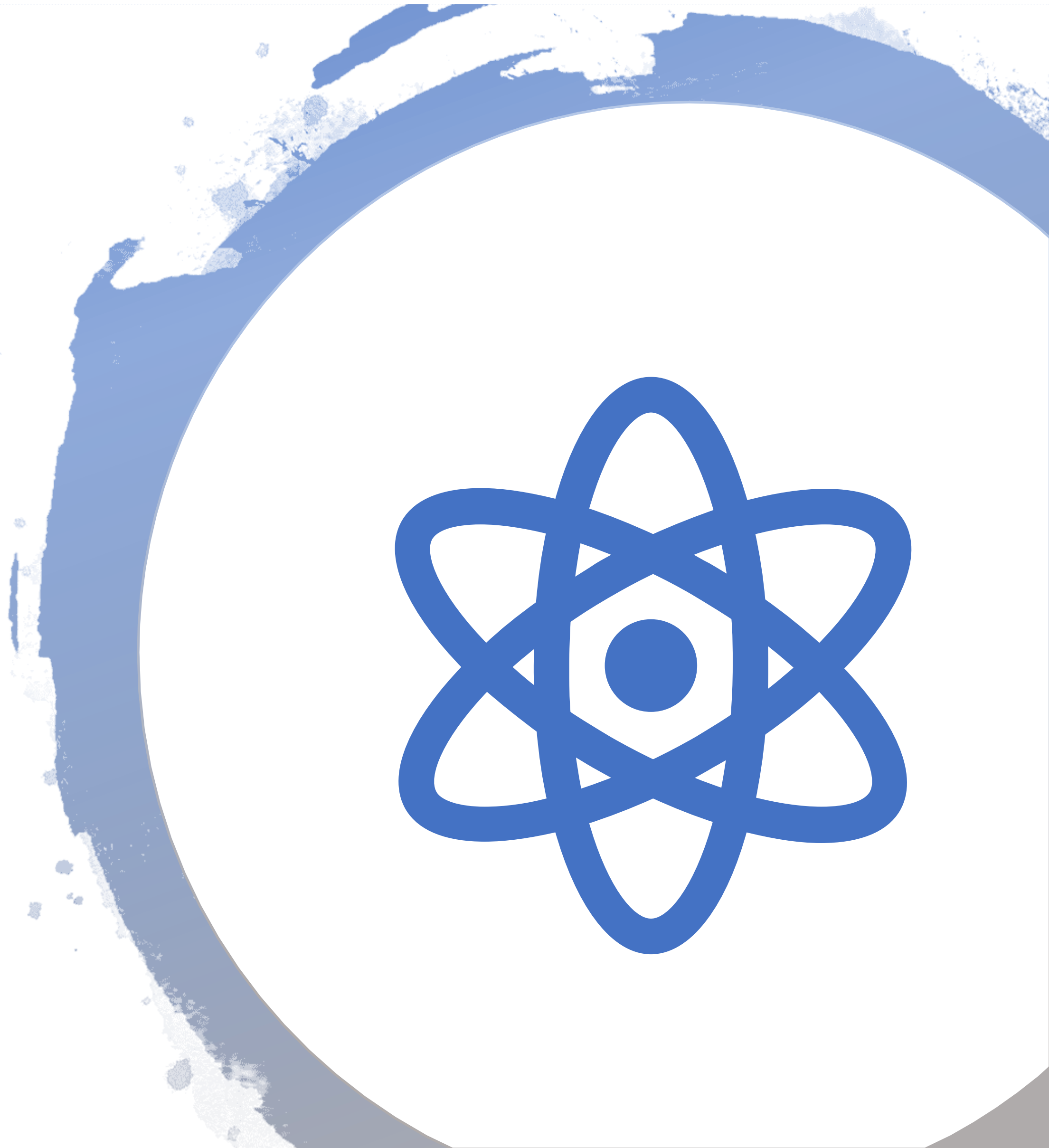
Lecture 2

Sanjam Garg

Recap from previous lecture

- Kerckhoff's principle (Security shouldn't rely on secrecy of the cipher)
- Any secure encryption scheme must have a *sufficiently large* key space
- Security must hold independent of the plaintext distribution
- Ad hoc fixes are likely to break

Cryptography has developed from an art to a science.



Design Principles

- Rigorous and precise definitions
- Precise assumptions
- Rigorous proof of security

Importance of Definitions

What is the ``right'' definition for a setting? Does a scheme satisfy this definition?

Communicate security properties, useful in larger system

DESIGN

ANALYSIS

USAGE

If you don't understand what you want to achieve, how can you possibly know when (or if) you have achieved it?

Assumptions

- Unconditional security, howsoever desirable, is not always achievable
  - We need $P \neq NP$, and in fact more!

- Assumption should be clearly stated
  - Can validate/invalidate them
  - Compare schemes based on different assumptions

Proofs of Security

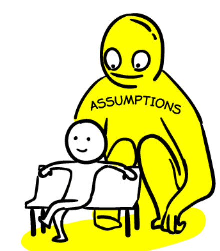
Very strong guarantee!

Limitation: Definition may not capture the real-world attack space!

A construction satisfies the considered security definition under the specified assumptions

Limitation: Implementation might be buggy!

Limitation: Assumption might be invalid!



Crypto remains a bit of an art!

Yet, definitions and security proofs are immensely valuable (reduce the attack space).

Illustrate, definitions and proofs.
But, not assumptions for now.

Perfect

Defining Secure Encryption

Private-key Encryption (syntax)

- A *private-key encryption scheme* is defined by a message space $\mathcal{M}$, a key space $\mathcal{K}$, and algorithms (Gen, Enc, Dec):
  - Gen (key-generation algorithm): outputs $k \in \mathcal{K}$
  - Enc (encryption algorithm): takes key k and message $m \in \mathcal{M}$ as input; outputs ciphertext c

    $$c \leftarrow \mathrm{Enc}_k(m)$$

  - Dec (decryption algorithm): takes key k and ciphertext c as input; outputs m or "error"

    $$m := \mathrm{Dec}_k(c)$$

k must be kept secret

Correctness: For all $m \in \mathcal{M}$ and k output by Gen,

$$\mathrm{Dec}_k(\mathrm{Enc}_k(m)) = m$$

Attempt at security?

Is it enough to keep your key secret?

Attempt at security?

Is it enough if the attacker cannot recover the entire message?

Attempt at security?

Is it enough if every character/bit in the message is hidden?

Attempt at security?

Can we require that the attacker doesn’t learns anything about the message?

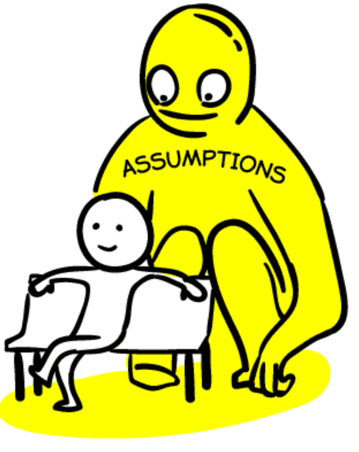
The right definition

Regardless of any information an attacker already has, a ciphertext should leak no *additional* information about the plaintext.

What about the length of the message?

No assumptions!

Perfect Security: Formally



Notation

variable that takes on (discrete) values with certain probabilities

- Given $\mathcal{K}$ and (Gen, Enc, Dec)
  - K be a random variable denoting the output of Gen()

$$\Pr[K = k] = \Pr[Gen()\ outputs\ k]$$

- M be a random variable denoting the value of the message (M ranges over $\mathcal{M}$)
  - If $\Pr[M = m] > 0$ then m must have been in $\mathcal{M}$
  - Application specific, example:

$$\Pr[M = \text{“}Attack!\text{”}] = .6$$
$$\Pr[M = \text{“}Retreat\text{”}] = .4$$

M and K are independent!

- C be a random variable denoting the value of the ciphertext $\Pr[C = c] = \Pr[Enc_K(M) = c]$ (Randomness of Enc as well)

Shift Cipher: Example 1

- $k \in \{0, \ldots, 25\}$, $\Pr[K = k] = ?$
  $1/26$
- Pr[M = ‘a’] = 0.6, Pr[M = ‘b’] = 0.4
- What is $\Pr[C = \text{‘}z\text{’}]?$

$= \Pr[Enc_K(M) = \text{‘}z\text{’}]$

$= .6 \times \Pr[Enc_K(\text{‘}a\text{’}) = \text{‘}z\text{’}] + .4 \times \Pr[Enc_K(\text{‘}b\text{’}) = \text{‘}z\text{’}]$

$= .6 \times \frac{1}{26} + .4 \times \frac{1}{26}$

$= \frac{1}{26}$

Shift Cipher: Example 2

- Pr[M = ‘aa’] = 0.6, Pr[M = ‘ab’] = 0.4
- C = ‘zz’
- Can you guess what m is?

Shift cipher is insecure even for messages of length two.

The right definition: Formally

Informal: Regardless of any information an attacker already has, a ciphertext should leak no *additional* information about the plaintext.

Definition 1: An encryption scheme (Gen, Enc, 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 for which $\Pr[C = c] > 0$:

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

Example

Baye's Theorem:

$$\Pr[A \mid B] = \Pr[B \mid A] \cdot \Pr[A]/\Pr[B]$$

- $k \in \{0, \ldots, 25\}, \Pr[K = k] = 1/26$
- Pr[M = 'a'] = 0.6, Pr[M = 'b'] = 0.4
- $\Pr[C = \text{'}z\text{'}] = 1/26$

- Pr[M = 'a'$|C = \text{'}z\text{'}$]

= Pr[$C = \text{'}z\text{'}$| M = 'a'] · Pr[M = 'a'] / Pr[$C = \text{'}z\text{'}$]

$= \frac{1}{26} \cdot \frac{0.6}{\frac{1}{26}}$

= 0.6

= Pr[M = 'a']

Definition 2

Definition 2: An encryption scheme (Gen, Enc, Dec) with message space $\mathcal{M}$ is *perfectly secret* if for every two messages , $m, m' \in \mathcal{M}$, and every ciphertext c (in ciphertext space):

$$\Pr[Enc_K(m) = c] = \Pr[Enc_K(m') = c],$$

where probability is only over K and random coins of Enc.

Definition 1 is equivalent to Definition 2.

Definition 2 => Definition 1.

Given: $\forall m, m', c \ \Pr[Enc_K(m) = c] = \Pr[Enc_K(m') = c]$

To prove: $\forall$ distribution on $\mathcal{M}$, m, and c for which $\Pr[C = c] > 0$,

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

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

$$= \frac{\Pr[Enc_K(m)=c] \cdot \Pr[M=m]}{\sum_{m'} \Pr\left[C = c \mid M = m'\right] \cdot \Pr[M=m']}$$

$$= \frac{\Pr[Enc_K(m)=c] \cdot \Pr[M=m]}{\sum_{m'} \Pr[Enc_K(m)=c] \cdot \Pr[M=m']} = \frac{\Pr[M=m]}{\sum_{m'} \Pr[M=m']}$$

$$= \Pr[M = m]$$

Try on your own: Definition 1 => Definition 2

Definition 3 (Game Style)

eav is for Eavesdropper

$\mathrm{PrivK}^{\mathrm{eav}}_{A,\Pi}$

1. A outputs $m_0, m_1 \in \mathcal{M}$.
2. $\mathrm{b} \leftarrow \{0,1\}$, $k \leftarrow \mathrm{Gen}()$, $c \leftarrow Enc_k(m_b)$
3. c is given to A
4. A output b'
5. Output 1 if $b = b'$ and 0 otherwise

Challenge ciphertext

Encryption scheme $\Pi = (Gen, Enc, Dec)$ with message space $\mathcal{M}$

is perfectly indistinguishable if

$\forall A$ it holds that:

$$\Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{A,\Pi} = 1\right] = \frac{1}{2}$$

A can always succeed with probability ½. How?

Lemma (Prove on your own): Encryption scheme Π is *perfectly secret* if and only if it is *perfectly indistinguishable*.

The One-Time Pad

Fix and integer ℓ, $\mathcal{M}, \mathcal{K}, \mathcal{C} = \{0,1\}^{\ell}$

- Gen: output a uniform value from $\mathcal{K}$
- $Enc_k(m)$: where $m \in \{0,1\}^{\ell}$, output $c := k \oplus m$
- $Dec_k(c)$: output $m := k \oplus c$
- Correctness: $Dec_k\big(Enc_k(m)\big) = k \oplus k \oplus m = m$
- Security: $\forall\, m, c, \Pr[Enc_K(m) = c] = 2^{-\ell}$. Or, $\forall\, m, m', c, \Pr[Enc_K(m) = c] = \Pr[Enc_K(m') = c]$

Thank You!