Cryptography

Langston Barrett

Fall 2017

Contents

- Instructor: Adam Groce
- Textbook:
  - Title: Introduction to Modern Cryptography, 2nd Edition
  - Author: Jonathan Katz and Yehuda Lindell
  - ISBN: 978-1-4665-7026-9

1 Probability

Lemma 1.1. If

a. A and B are random variables,

b. B is sampled from some finite set of outcomes $\mathcal{B}$,

then

$$\mathsf{Pr}(A) = \sum_{b \in \mathcal{B}} \mathsf{Pr}(A|B) \cdot \mathsf{Pr}(B = b)$$

Lemma 1.2 (Union Bound)**.** For events $E_0, \ldots, E_n$,

$$\mathsf{Pr}\left(\bigvee_{i=0}^{n} E_i\right) \leq \sum_{i=0}^{n} \mathsf{Pr}\, E_i$$

Theorem 1.3 (Bayes' Theorem)**.**

$$\mathsf{Pr}(A|B) = \frac{\mathsf{Pr}(B|A) \cdot \mathsf{Pr}\, A}{\mathsf{Pr}\, B}$$

2 Concepts

Note. What's wrong with having a small key space $\mathcal{K}$?
It makes your scheme vulnerable to brute-force attacks, especially when the distribution on the message space $\mathcal{M}$ is well-understood (as in all adversarial experiments).

Note. What are the four kinds of security experiments?

1. Ciphertext-only
2. Known-plaintext
3. Chosen-plaintext
4. Chosen-ciphertext

Note. How does a reduction work?
In it's most general form, reduction is a tool used to show that problem/language A is just as "hard" as problem/language B.

1. Assume that problem B "hard".
2. Assume $\mathcal{A}$ is an algorithm that solves A.
3. Using $\mathcal{A}$ as a subroutine, construct a solution $\mathcal{B}$ for B.
4. This contradicts the assumption that B couldn't be solved, conclude by contradiction that no such $\mathcal{A}$ exists.

Note. What is one piece of information that almost every encryption scheme leaks? Why might it be a problem? When can and when can't it be solved?
Plaintext length. It might be a problem if $\mathcal{M} = \{\text{"yes"}, \text{"no"}\}$. It can be solved when the maximum length of the encrypted messages is known in advance.

Note. Why is it necessary to use randomness in encryption?
No non-random scheme has indistinguishability for multiple encryptions.

3 Symmetric-key cryptography

Definition. A **private-key encryption scheme** consists of:

- a **message space** $\mathcal{M}$,
- a **key space** $\mathcal{K}$, and
- a trio of algorithms $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$.

A scheme is **correct** if

$$\mathsf{Dec}_k\left(\mathsf{Enc}_k\ m\right) = m$$

for all $m \in \mathcal{M}$ and $k \in \mathcal{K}$.

Definition. A private-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is **perfectly secret** if for all distributions on $\mathcal{M}$, $m \in \mathcal{M}$, and $c \in \mathcal{C}$ (with $\mathsf{Pr}(C = c) > 0)$,

$$\mathsf{Pr}(M = m | C = c) = \mathsf{Pr}(M = m)$$

Equivalently, for all $m, m' \in \mathcal{M}$, and $c \in \mathcal{C}$, a

$$\mathsf{Pr}(\mathsf{Enc}_K(m) = c) = \mathsf{Pr}(\mathsf{Enc}_K(m') = c)$$

Definition. The **perfect adversarial indistinguishability experiment** $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$ is:

1. The adversary $\mathcal{A}$ outputs $m_0, m_1 \in \mathcal{M}$.
2. (a) A key $k \leftarrow \mathsf{Gen}(1^n)$ is generated.
   (b) A bit $b \leftarrow \{0, 1\}$ is chosen.
   (c) A ciphertext $c \leftarrow \mathsf{Enc}_k\ m_b$ is fed to $\mathcal{A}$.
3. $\mathcal{A}$ outputs $b' \in \{0, 1\}$.

The experiment outputs 1 when $b = b'$.

Definition. A scheme Π has **perfectly indistinguishable encryptions in the presence of an eavesdropper** if

$$\mathsf{Pr}\big(\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1\big) = \frac{1}{2}$$

for all $\mathcal{A} \in \mathsf{PP}$.

Definition. The **adversarial indistinguishability experiment** $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n)$ is:

1. The adversary $\mathcal{A}$ is given 1^n and outputs $m_0, m_1 \in \mathcal{M}$ with $|m_0| = |m_1|$.
2. (a) A key $k \leftarrow \mathsf{Gen}(1^n)$ is generated.
   (b) A bit $b \leftarrow \{0, 1\}$ is chosen.
   (c) A ciphertext $c \leftarrow \mathsf{Enc}_k\ m_b$ is fed to $\mathcal{A}$.
3. $\mathcal{A}$ outputs $b' \in \{0, 1\}$.

The experiment outputs 1 when $b = b'$.

Definition. A scheme Π has **indistinguishable encryptions in the presence of an eavesdropper** if

$$\mathsf{Pr}\big(\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1\big) \leq \frac{1}{2} + \mathsf{negl}\ n$$

for all $\mathcal{A} \in \mathsf{PP}$ and $n \in \mathbb{N}$, where the probability is taken over randomness of $\mathcal{A}$ and that of the experiment.

Definition. The **multiple-message indistinguishability experiment** $\mathsf{PrivK}^{\mathsf{mult}}_{\mathcal{A},\Pi}(n)$ is:

1. The adversary $\mathcal{A}$ is given 1^n and outputs lists $(m_{0,0}, m_{1,0}, \ldots, m_{t,0})$ and $(m_{0,1}, m_{1,1}, \ldots, m_{t,1})$ such that $|m_{i,0}| = |m_{i,1}|$ for all $i \in \{1, \ldots, t\}$.
2. (a) A key $k \leftarrow \mathsf{Gen}(1^n)$ is generated.
   (b) A bit $b \leftarrow \{0, 1\}$ is chosen.
   (c) The ciphertexts $(\mathsf{Enc}_k\ m_{0,b}, \ldots, \mathsf{Enc}_k\ m_{t,b})$ are given to $\mathcal{A}$.
3. $\mathcal{A}$ outputs $b' \in \{0, 1\}$.

The experiment outputs 1 when $b = b'$.

3.1 Peseudorandomness

Definition 3.1. A *determinisitic* algorithm $G \in \mathsf{P}$ is a **pseudorandom generator** if there exists some real polynomial l such that $D : \{0,1\}^n \to \{0,1\}^{l\ n}$ and the following conditions hold:

1. **Expansion:** For all $n \in \mathbb{N}$, $l\ n > n$.
2. **Pseudorandomness:** For all distinguishers $D \in \mathsf{PP}$, there exists a negligible function negl such that

   $$|\mathsf{Pr}(D(r) = 1) - \mathsf{Pr}(D(G(s)) = 1)| \leq \mathsf{negl}\ n$$

   where the first probability is taken over the choice of a uniformly random string $r \leftarrow \{0,1\}^{l(n)}$ and the second over a choice of a uniformly random $s \leftarrow \{0,1\}^n$, and both over randomness of D.

Note. What is meant by the phrase “let s be a random string”?
Strictly speaking, this phrase doesn’t make sense. A given string (or function) can’t be *random*. What it means is “let s be a string drawn uniformly at random from the set of all strings”.

Note. Does the seed of a pseudorandom generator need to be kept secret? Why?
Yes. Consider the modified one-time pad scheme where a PRG is used to expand the key length. If the adversary knows the seed, they know the key.

Definition 3.2. A **stream cipher** is a pair of deterministic algorithms $(\mathsf{Init}, \mathsf{GetBits})$ where

- Init takes as input a seed s and an optional initialization vector IV, and outputs an initial state s_0.
- $\mathsf{GetBits}$ takes a state s_i and outputs a bit b and an updated state s_{i+1}.

3.2 CPA-security

Definition. The **CPA indistinguishability experiment** $\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n)$ is:

1. A key $k \leftarrow \mathsf{Gen}(1^n)$ is generated.
2. The adversary $\mathcal{A}$ is given 1^n and access to the oracle $\mathsf{Enc}_k(-)$. The adversary outputs $m_0, m_1 \in \mathcal{M}$ with $|m_0| = |m_1|$.
3. (a) A bit $b \leftarrow \{0, 1\}$ is chosen.
   (b) The ciphertext $c \leftarrow \mathsf{Enc}_k\ m_b$ is fed to $\mathcal{A}$.
4. $\mathcal{A}$ continues to have access to $\mathsf{Enc}_k(-)$ and outputs $b' \in \{0, 1\}$.

The experiment outputs 1 when $b = b'$.

3.3 Message authentication codes

Definition 3.3. A **message authentication code** consists of three PP algorithms $(\mathsf{Gen}, \mathsf{MAC}, \mathsf{Verify})$ such that:

- Gen takes input 1^n and outputs a key k with $|k| \geq n$,
- MAC takes a key $k \in \mathcal{K}$ and a message $m \in \mathcal{M}$ and outputs a tag t.
- Verify takes a key $k \in \mathcal{K}$, a message $m \in \mathcal{M}$, and a tag t, and outputs a bit b with $b = 1$ meaning valid and $b = 0$ meaning invalid.

A MAC is correct if for all $m \in \mathcal{M}$ and $k \in \mathcal{K}$,

$$\mathsf{Verify}_k\ (\mathsf{MAC}_k\ m) = 1$$