Cryptography

Important Information:

Exam: January 2020
Lectures: 14:15-17:00, 106 HG
Exercises: 10 points each, required 70%
Trivia: NONE

Chapter 1

Introduction

Difference between **Cryptology** and **Cryptography**:
Cryptology is the combination of Cryptography and Cryptoanalysis
Cryptology concerns the protection of informstion in an adverserial context.

1.0.1 Classical Goals of Cryptography (CIA)

- Confidentiality
- Integrity
- Availability

1.0.2 Techniques

- encryption
- digital signatures
- hash functions
- MACs

1.0.3 Modern goals

- Anonymity
- Zero-knowledge proofs

1.1 A model for a cryptosystem (Shannon, 48)

KeyGen() (outputs secret key k)

$\downarrow$k $\qquad\qquad\qquad\qquad\qquad\qquad$ $\downarrow$k

(Alice) $\overset{m}{\rightarrow}$ [Enc] $\xrightarrow{c}$ [Dec] $\overset{\hat{m}}{\rightarrow}$ (Bob)

$\downarrow$c

(Eve)

plaintext m, ciphertext c, decoded text $\hat{m}$

1.1.1 Key genereaton algorithm

KeyGen() $\rightarrow$ k

1.1.2 Encryption algorithm

Enc(k,m) $\rightarrow$ c

1.1.3 Decription algorithm

Dec(k,c) $\rightarrow$ $\hat{m}$

1.1.4 Goals

1. *Completeness*:
   Bob obtains the message from Alice:
   m $\overset{?}{=}$ $\hat{m}$

2. *Security*:
   "Eve obtains no useful information about the message m"

1.2 Hystoric cryptography

- *Scytale* (ancient Greece, 3rd. cent. BC)
- *Ceasar cipher* (Roman empire, 50 BC) (shift cipher)
  - KeyGen(): k $\overset{R}{\leftarrow}$ {0,1,...,25}
  - Enc(k,l): return l+k
  - Dec(k,c): return c-k
- *Monoalphabetic substitution* (uniform distributed permutation of the input)
  - Enc(k,l): return K[l]
  - Dec(k,c): return K^{-1}[c]

Chapter 2

Mathematical preliminories

2.1 Probability theory

⋆ A probability distribution P[ ] over a sample space Ω assigns a value in [0,1] to each $S \subseteq \Omega$ ("events") such that:

(a) P[Ω] = 1

(b) P[A $\cup$ B] = P[A] + P[B]
for any $A, B \subseteq \Omega$ s.t. $A \cap B \neq \emptyset$

⋆ Random variable $X \in \chi$ (χ-alphabet) is defined by an alphabet χ and a prob. distribution P_X over χ, s.t.:

$$P_X(x) = P[X = x] \text{ s.t. } \sum_{x \in \chi} P_X(x) = 1$$

⋆ A uniform random variable U over an alphabet $\mho$ satisfies:

$$P_U(u) = 1/\mid \mho \mid \text{ for } u \in \mho$$

Example:
P[Adversary A outputs a value k] $\leq 2^{-\lambda}, \lambda \in \{0,1\}^\lambda$

Warning!!!! "random" $\neq$ arbitrary

2.2 Notation

⋆ **$\leftarrow$ or $\overset{R}{\leftarrow}$**

For set S the notation:

$$x \leftarrow S$$

denotes that the value x ios chosen uniformly at random from set S

$$\forall s \in S : P[x \leftarrow S : x = s] = 1/ \mid S \mid$$

For a randomized algorithm R(y):

$$x \leftarrow R(y)$$

denotes the experiment of running R on input y and assigning its output to x

⋆ **:=** (assignment operator)

$$\text{x := 1}$$

⋆ $\overset{?}{=}$

$$\underline{\text{if}}\ x \overset{?}{=} \underline{\text{then}}\ ...$$

2.3 Kerckhoff's principle

Design cryptosystem s.t. its security does not rely on the secrecy of the algrithm itself

2.3.1 One-time-pad (Vernam's cipher)

- Vernam ($\sim$ 1916)
- Security proof by Shannon (1948)

Syntax: keys, messages are λ-bit strings Σ = {0,1} $m \in \Sigma^\lambda$

KeyGen(): $k \leftarrow \Sigma^\lambda$

Enc(k,m): return $k \oplus m$

Dec(k,c): return $k \oplus c$

2.3.2 Completeness

Theorem

$$\forall m \in \Sigma^\lambda, \forall k \in \Sigma^\lambda,$$

$$Dec(k, Enc(k, m)) = m$$

Proof

$$k \oplus Enc(k, m)$$

$$= k \oplus (k \oplus m)$$

$$= (k \oplus k) \oplus m$$

$$= 0^\lambda \oplus m$$

$$= m$$

2.3.3 Security

Consider experiment that produces exactly the distribution seen by Eve.
Eavesdrop(m)

$$k \leftarrow \Sigma^{\lambda}$$

$$c \leftarrow m \oplus k$$

$$\textit{return } c$$

Theorem

$$\forall m \in \Sigma^{\lambda},\ \textit{Eavesdrop(m) is a uniform random variable over } \Sigma^{\lambda}$$

$$\Rightarrow m \neq m' :\ \textit{Eavesdrop(m) has same distribution as Eavesdrop(m')}$$

Proof

$$\forall m \in \Sigma^{\lambda}$$

$$\forall c \in \Sigma^{\lambda}$$

$$P[\textit{Eavesdrop(m)=c}] = ?$$

$$\underline{\textit{We know:}}\ c = m \oplus k \Leftrightarrow k = m \oplus c$$

$$P[\textit{Eavesdrop(m)=c}] = P[m \oplus k = c] = P[k = \underbrace{m \oplus c}_{s}] = P[k = s] = 2^{-\lambda}$$