1

Security 2

2022

C Schürmann

Lecture 1

SECURITY 2

- Labs
- 6 Quizes
- Honor system
- Project work.
  - BOUNCY CASTLE

Teacher: CARSTEN SCHÜRMANN (CARSTEN)

ASSISTANTS: ASK HARUP SEJSBO (ASSE)

IN SECURITY 1: BASIC UNDERSTANDING OF CYBERSECURITY.

- ATTACKERMODEL / TRUST ASSUMPTIONS
- NETWORK SECURITY
- HACKING
- USABILITY
- A LITTLE CRYPTO.

QUESTIONS: MATH BACKGROUND, PROGRAMMING?

IN SECURITY 2:

components

Bancy castles

HOW TO DESIGN AND IMPLEMENT

perfect secrecy

SECURE SYSTEMS

USING CRYPTOGRAPHY.

THIS CLASS : FOUNDATIONS OF CRYPTOGRAPHY

- WHAT IS SECURITY?
- WHAT ARE THE UNDERLYING ALGORITHMS
- HOW DO WE PROVE THINGS
- HOW DO WE USE THINGS.

Table of Contents.

- History of ciphers
- Primer on probabilty theory
- Perfect secret Encryption

SYMMETRIC CRYPTO k

ASYMMETRIC CRYPTO pk sk

KERCKHOFF'S PRINCIPLE

[1883, NOTE ON CIPHERS used in the military]

A CRYPTOSYSTEM SHOULD BE SECURE
EVEN IF EVERYTHING ABOUT THE SYSTEM

EXCEPT THE KEY

IS PUBLIC KNOWLEDGE.

NOTE: This principle does not define what security is.

NOTE: We have to trust that the key is secret.

NOTE: Trust is central to all of this.

HISTORY OF CIPHERS:

SHIFT CEASAR'S CIPHER

$m = m_1 \dots m_n$ key k

$c = c_1 \dots c_n$ $k \leftarrow \{a \dots z\}$

$ENC_k(m) = c$ $\quad c_i = m_i + k \mod 26$

$DEC_k(c) = m$ $\quad m_i = c_i - k \mod 26$

$ENC_3(\text{house}) = KRXVH$

$DEC_3(KRXVH) = \text{house}$

$\mathcal{M} = \{a \dots z\}^*$

$\mathcal{K} = \{a \dots z\}$

$\mathcal{C} = \{A \dots Z\}$

LARGER KEY SPACES

Key space: $\sigma \in S_{26}$ (↑ permutation)

MONOALPHABETIC CIPHER

A → C
B → E
C → D
D → W
E → A
⋮

$ENC_\sigma(m) = c$ $\quad c_i = m_i[\sigma]$

$DEC_\sigma(c) = m$ $\quad m_i = c_i[\sigma^{-1}]$

Example homework

$\sigma = \{h \to a, o \to x, u \to c, s \to t, e \to r\}$

VIGENÈRE CIPHER (POLY-ALPHABETIC SHIFT CIPHER)

Key space : $K = k_1 \dots k_n$ $\quad |K| = 26^n$

Example: $m =$ tellhimaboutme

$k =$ cafecafecafeca

$C =$ VEQPJIREDOZXOE

VJDO "c"

EIOE "a"

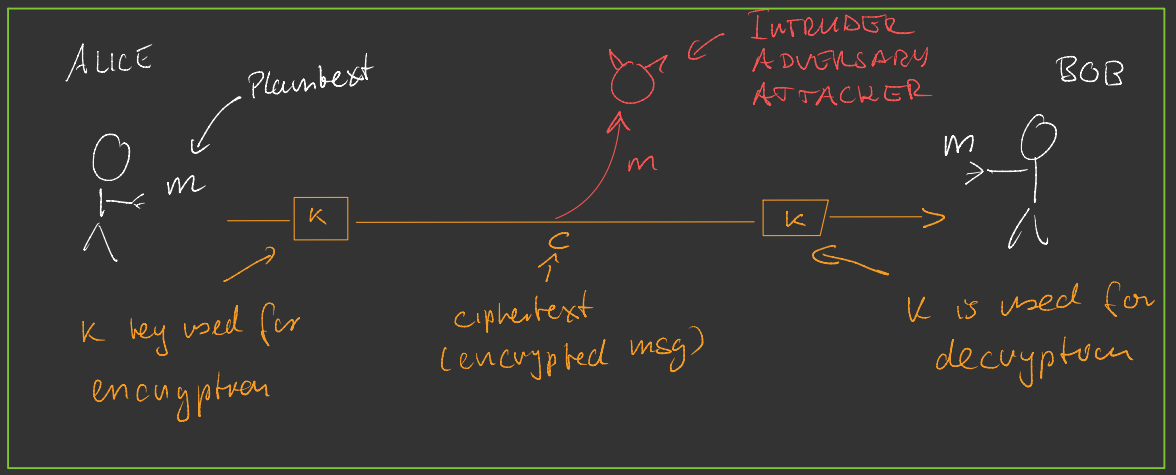
QRZ "f"

PEX "e"

$ENC_K(m) = c$ $\quad c_i = m_i + k_i \mod 26$

$DEC_K(c) = m$ $\quad m_i = c_i - k_i \mod 26$

THREAT MODEL



Possible attacks: (attacker doesn't know the key)

1) CIPHERTEXT ONLY ATTACK: OBSERVE c GUESS m

2) KNOWN PLAINTEXT ATTACK: OBSERVE (p_i, c_i) for a $c \neq c_i$ guess m

3) CHOSEN PLAINTEXT ATTACK: ACCESS TO ENCRYPTION ORACLE $\mathcal{O}(p) = c$ for a fresh c guess m.

4) CHOSEN CIPHERTEXT ATTACK: ACCESS TO DECRYPTION ORACLE $\mathcal{O}(c) = p$

SUMMARY

CRYPTOGRAPHY IS ALL ABOUT PROBABILITIES
RANDOMNESS

PRINCIPLE 1: FORMAL DEFINITIONS

PRINCIPLE 2: PRECISE ASSUMPTIONS

PRINCIPLE 3: PROOFS OF SECURITY

A PRIMER ON PROBABILITY THEORY

BASICS

DEF: EVENT E

DEF: $0 \leq P(E) \leq 1$

$$P(E) = \frac{\#\text{ event } E \text{ observed}}{\#\text{ events } E \text{ possible}}$$

DEF: COMPLEMENT $P(\bar{E}) = 1 - P(E)$

DEF: CONJUNCTION $P(E_1 \wedge E_2) = P(E_1) \cdot P(E_2)$ E_1, E_2 indep

DEF: DISJUNCTION $P(E_1 \vee E_2) = P(E_1) + P(E_2)$ [ ]

DEF: CONDITIONAL PROBABILITY

$$P(E_1 \mid E_2) = \frac{P(E_1 \wedge E_2)}{P(E_2)}$$

BAYES THEOREM

Lemma: $P(E_2 \wedge E_1) = P(E_2 \mid E_1) \cdot P(E_1)$ $\quad 1 : P(E_2)$

Proof

$$\frac{P(E_2 \wedge E_1)}{P(E_1)} = P(E_2 \mid E_1) \quad \text{by def of cond. probab.}$$

Theorem : [Bayes]

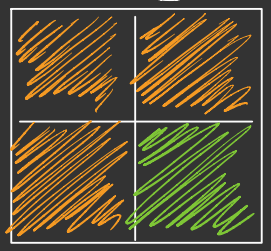
$$P(E_2 \mid E_1) = \frac{P(E_1 \mid E_2) \cdot P(E_2)}{P(E_1)}$$

Proof

$$P(E_2 \mid E_1) \overset{\text{def}}{=} \frac{P(E_2 \wedge E_1)}{P(E_1)} \overset{\text{reorder}}{=} \frac{P(E_1 \wedge E_2)}{P(E_1)}$$

$$\overset{\text{lemma}}{=} \frac{P(E_1 \mid E_2) \cdot P(E_2)}{P(E_1)}$$

Example



Box of cookies

/// chocolate cookies (CC)

/// peanut cookies (PC)

Question 1: If we draw a chocolate cookie what is the propability that it comes from box A?

Intuitively: $P(A|CC) \overset{?}{=} \frac{2}{3}$ $P(A|PC) \overset{?}{=} 0$ ✓

WITH MATH:

$P(CC) = \frac{3}{4}$ $P(PC) = \frac{1}{4}$

$P(A) = \frac{1}{2}$ $P(B) = \frac{1}{2}$

$P(CC|A) = 1$ $P(PC|A) = 0$ ✓

$P(CC|B) = \frac{1}{2}$ $P(CC|B) = \frac{1}{2}$

$P(A|CC)$

Bayes $\frac{P(CC|A) \cdot P(A)}{P(CC)}$

$= \frac{1 \cdot \frac{1}{2}}{\frac{3}{4}}$

$= \frac{2}{3}$ ✓

Perfect Secret Encryption

Information theoretically secure

Formal Definitions

Message space : $\mathcal{M}$

Key space : $\mathcal{K}$

Ciphertext Space: $\mathcal{C}$

Cryptosystem: $\Pi = (Gen, Enc, Dec)$

$Gen : K \leftarrow \mathcal{K}$

$Enc : c \leftarrow Enc_K(m)$ non-det.

$Dec : m := Dec_K(c)$

Def: We write $P(\underbrace{K=k}_{\text{Event}})$ for the probability that Gen produces k (random variable, given)

$P(C=c)$ $P(M=m)$

Def: [Perfect Secrecy] Π has perfect secrecy iff

$$P(M=m) = P(M=m \mid C=c)$$

Is the shift cipher perfectly secret?

$\mathcal{K} = \{0..25\}$ $\quad P(K=k) = \frac{1}{26}$

Example 1 $\quad \mathcal{M} = \{a, z\}$ $\quad P(M=a) = 0.7$ $\quad P(M=z) = 0.3$

1) What is the probability, that we observe ciphertext B?

$$P(C=B) = P(M=a \wedge K=1) + P(M=z \wedge K=2)$$
$$= P(M=a) \cdot P(K=1) + P(M=z) \cdot P(K=2)$$
$$= 0.7 \cdot \frac{1}{26} + 0.3 \cdot \frac{1}{26} = \frac{1}{26}$$

2) $$P(M=a \mid C=B) = \frac{P(C=B \mid M=a) \cdot P(M=a)}{P(C=B)} = \frac{\frac{1}{26} 0.7}{\frac{1}{26}} = 0.7$$

$$= P(M=a)$$

3) $P(M=z \mid C=B) =$ HW.

Is the Shift cipher perfectly secret?

Looks pretty good

$$P(M = a \mid C = B) = 0.7 = P(M = a)$$

$$P(M = z \mid C = B) = 0.3 = P(M = z)$$

Example 2. $M = \{kim, ann, boo\}$ OBSERVED CIPHERTEXT: DQQ.

$P(M = kim) = \frac{1}{2}$ $P(M = ann) = 0.2$ $P(M = boo) = 0.3$

$$P(C = DQQ) = P(M = ann \wedge k = 3) + P(M = boo \wedge k = 2)$$
$$= P(M = ann) \cdot P(k = 3) + P(M = boo) \cdot P(k = 2)$$
$$= 0.2 \cdot \frac{1}{26} + 0.3 \cdot \frac{1}{26} = 0.5 \frac{1}{26}$$
$$= \frac{1}{52}.$$

$$P(M = ann \mid C = DQQ) = \frac{P(C = DQQ \mid M = ann) \cdot P(M = ann)}{P(C = DQQ)} = \frac{\frac{1}{26} \cdot 0.2}{\frac{1}{52}}$$

$$= 0.4$$

$$\neq P(M = ann).$$