Secure Communications

Lecture 2: Perfect Secrecy, One Time Pad

Melek Önen

Fall 2022

EURECOM
Sophia Antipolis

Review

- Security Services
  - Authentication, Access Control, Confidentiality, Non-repudiation, Integrity, Privacy
- Cryptography
  - Historical ciphers and their Cryptanalysis

Outline

- Principles of Modern Cryptography
  - Formal Definitions, Precise Assumptions, Security Proofs
- Discrete Probability
  - Definitions, Probability Distributions, Conditional Probability
- Perfect secrecy
  - Perfect secrecy, One-time Pad

Outline

- Principles of Modern Cryptography
  - Formal Definitions, Precise Assumptions, Security Proofs
- Discrete Probability
  - Definitions, Probability Distributions, Conditional Probability
- Perfect secrecy
  - Perfect secrecy, One-time Pad

Principles of Modern Cryptography

- Principle 1
  - Precise and formal definition of security
- Principle 2
  - Clearly stated and unambiguous assumptions
- Principle 3
  - Rigorous proof of security

Principle 1- Security Definition

- *"If you do not understand what you want to achieve how can you possibly know when you have achieved it?" (J. Katz)*
  - Easier knowledge transfer
  - Easier comparative study
  - Easier to evaluate

- Methodology
  - Define threat model
    - What actions can the attacker carry out?
  - Define security guarantee
    - What to prevent the attacker from doing it?

Principle 2 - Precise Assumptions

- Cryptography requires explicit computational assumptions
  - Easier to validate
  - Easier to compare schemes based on the same assumption
  - Easier to react when assumptions turn out to be wrong
  - Easier to prove

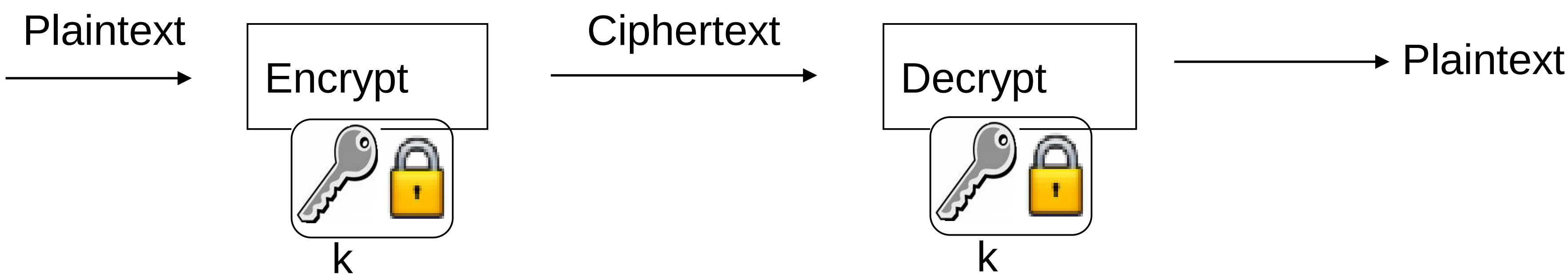
Principle 3 – Proofs of Security

- Rigorous proof that a construction satisfies the *given definition under the specified assumptions.*

- Provably secure schemes can be broken!
  - If reality is different than definition
  - If assumption is invalid.

Secure Encryption

- (Private-key) Encryption scheme defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$
  - Key generation: KeyGen(κ)$\rightarrow k$
  - Encryption: Enc(k, m) $\rightarrow$ c
  - Decryption: Dec(k,c) = m



- Security Guarantees
  - Correctness: Dec(k,Enc(k,m)) = m

Principle 1 - Security Definition

- *"If you do not understand what you want to achieve how can you possibly know when you have achieved it?" (J. Katz)*
  - Easier knowledge transfer
  - Easier comparative study
  - Easier to evaluate

- Methodology
  - **Define threat model**
    - What actions can the attacker carry out?
  - **Define security guarantee**
    - What to prevent the attacker from doing it?

Principle 1 – Threat Models for Encryption

- **Brute force attack**
  - **Most simple attack: simply try every key**
  - **Success rate = inversely proportional to the key size**

Key Size (bits)	Number of Alternative Keys	Time required at 1 encryption/μs	Time required at 10^6 encryptions/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} years	6.4×10^6 years

Principle 1 – Threat Models for Encryption

- **Ciphertext-only attack**
  - Attacker knows ciphertext *C*
  - one or many ciphertexts.
- **Known plaintext attack**
  - Attacker knows ciphertext *C* of plaintext *M*
  - Attacker knows (M_i, C_i)
- **Chosen plaintext attack**
  - Attacker can get ciphertext *C* for a chosen plaintext *M*
  - Attacker can *adaptively* choose *M*
- **Chosen ciphertext attack**
  - Attacker can get plaintext *M* for a chosen ciphertext *C*
  - Attacker can *adaptively* choose *C*

Reminder Kerckhoff's principle

- Kerckhoff's principle:

  " *The cipher method must not be required to be secret and it must be able to fall into the hands of the enemy without inconvenience"*

- Only the key should remain secret
  - The key must be chosen at random
  - The key must be kept secret

- Consequences
  - Short information to keep secret (key instead of algorithm)
  - Easy to update if problem (key instead of algorithm)

Principle 1 – Security Guarantee for Encryption

- What is considered as break?

- Example – Secure encryption
  - Key recovery?
    - The aim of encryption is to protect the message
    - The key is a means for achieving this but not sufficient
  - Entire plaintext recovery?
    - What if the attacker learns % of the message?

Principle 1 – Security Guarantee for Encryption

- Right notion!
  - Regardless of any ***prior*** information the attacker has about the plaintext, the ciphertext should leak no ***additional*** information about the plaintext.

Outline

- Principle of Modern Cryptography
  - Formal Definitions, Precise Assumptions, Security Proofs
- Discrete Probability
  - Definitions, Probability Distributions, Conditional Probability
- Perfect secrecy
  - Perfect secrecy, One-time Pad

Definitions – Sample Space

- **Random experiment**

Process for which the outcome cannot be predicted with certainty

  - *Ex: c=Encryption of 2-bit message m, (|c|=2)*

- **Sample space**

Set of all possible outcomes- All possible occurrences in some experiment

  - *S={00, 01, 10, 11}*

- **Event**

Subset of the sample space – Particular occurrence in some experiment

  - *"c=10"*
  - *"c=0*"*

Probabilities and Set Operations

- **Probability**:

measures the likelihood that some event will occur
  - *P(A)* denotes the probability that event A occurs
- Axioms of Probability
  - Axiom 1: $0 \leq P(A) \leq 1$
  - Axiom 2: $P(S) = 1$
  - Axiom 3: If $\{A_1, A_2, ..\}$ is a set of disjoint events then $P(\bigcup_{i=1}^{n} A_i) = \sum_{i=1}^{n} P(A_i)$
- Consequences
  - $P(\bar{A}) = 1 - \mathrm{P(A)}$
  - $P(A \cup B) = P(A) + P(B) - P(A \cap B)$

$\Rightarrow$ Union bound: $P(A \cup B) \leq P(A) + P(B)$

Random Variable - Definition

- Discrete Random Variable

Variable that takes on values in a finite set within an experiment with some probabilities

  - *Ex: X=Encryption of 2 bits ab*

- Probability Distribution

Probabilities with which the variable takes on each possible value

  - *Ex: P[00]=1/2, P[01]=1/8, p[10]=1/4, p[11]=1/8*
  - $\sum_{x \in U} p(X) = ?$
  - $\sum_{x \in U} p(X) = 1$

- Distribution vector
  - Ex: (P[00],P[01],P[10],P[11])

Probability Distributions - Example

- **Point Distribution at $\boldsymbol{x_0}$**

$$P[x_0] = 1, \forall x \neq x_0 P[x] = 0$$

- **Uniform Distribution**

For all $x \in U$: $P[X] = \frac{1}{|U|}$

  - **Ex:** $\boldsymbol{U = \{0,1\}^2}$

P[00]=P[01]=P[10]=P[11]=1/4

  - **Ex:** A=$\{ \, all \; x \; in \; \{0{,}1\}^2, such \; that \; lsb(x) = 1\}$

P[01]+P[11] = 1/2

Conditional probability

- P(A|B) : Probability of A given B

Probability that A occurs assuming that some other event B occurred

- $P(A|B) = \frac{P(A \cap B)}{P(B)}$ with $P(B) \neq 0$
- *A* and *B* are independent if

$$P(A \cap B) = P(A)P(B)$$

$$P(A|B) = P(A)$$

- Law of total probability

  Let $B_1, B_2, .., B_n$, a set of disjoint events where $\cup_{i=1}^{n} B_i = S$

$$P(A) = \sum_{i=1}^{n} P(A|B_i)P(B_i)$$

Bayes formula

- $P(B|A) = \frac{P(A|B)P(B)}{P(A)}$
- $P[M = m|C = c] = \frac{P[C = c|M = m].P[M=m]}{P[C=c]}$

- *Ex:Shift cipher with*

P[m='hi']=0.3, P[m='no']=0.2, P[m='in']=0.5

- *P[M='hi'|C='xy']=?*

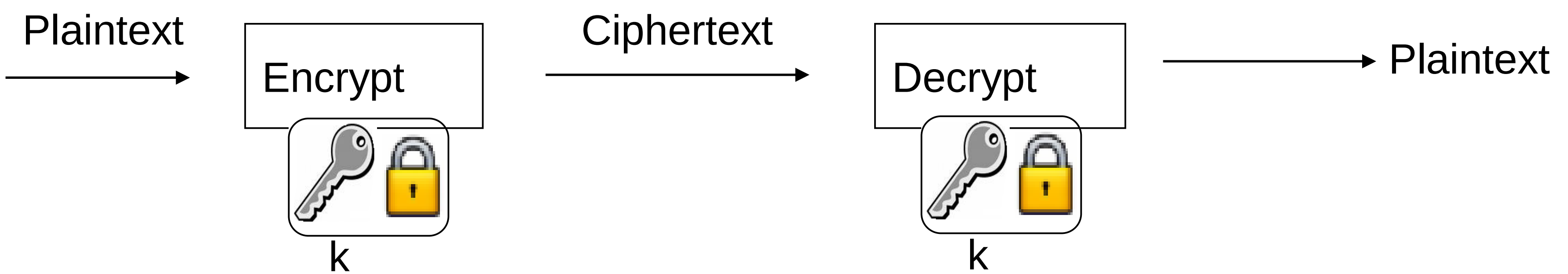
$$= \frac{P[C = ' xy'|M =' hi'].P[M =' hi']}{P[C = 'xy']}$$

Outline

- Principle of Modern Cryptography
  - Formal Definitions, Precise Assumptions, Security Proofs
- Discrete Probability
  - Definitions, Probability Distributions, Conditional Probability
- Perfect secrecy
  - Perfect secrecy, One-time Pad

Private Key Encryption – Security Evaluation

- Let $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ be the key space, message space and ciphertext space
  - Key generation: KeyGen(κ)=k
  - Encryption: Enc(k, m) = c
  - Decryption: Dec(k,c) = m



- Security Guarantees
  - Correctness: Dec(k,Enc(k,m)) = m

Probability distributions

- Fix some encryption scheme (KeyGen, Enc, Dec) and some distribution for M

- Consider the following randomized experiment
  - Choose a message m, according to the given distribution
  - Generate a key k using KeyGen
  - Compute c = Enc(k,m)
- This defines a distribution on the ciphertext
  - C is the r.v. on the ciphertext in this experiment

Perfect secrecy

- Regardless of any ***prior*** information the attacker has about the plaintext, the ciphertext should leak no ***additional*** information about the plaintext.

- Attacker's information about plaintext after= Attacker's information about plaintext before

- An Encryption scheme (KeyGen, Enc,Dec) with message space $\mathcal{M}$ is **perfectly secure** if for every probability distribution over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which Pr[C=c]>0:

$$\boldsymbol{P[M = m|C = c] = P[M = m]}$$

Example (*Katz,Lindell, Modern Cryptography)*

- Consider the shift cipher and the distribution

$$P[M = one] = \frac{1}{2}, P[M = ten] = \frac{1}{2}$$

- Take m=‘ten’ and c=‘rqh’

- $P[M =' ten'|C =' rqh'] =?$

$= 0$

$\neq P[M =' ten']$

⇒The shift cipher is not perfectly secret!

Example (*Katz,Lindell, Modern Cryptography)*

- Consider the shift cipher and the distribution
$$P[M =' hi'] = 0.3, P[M =' no'] = 0.2\ P[M =' in'] = 0.5$$
- $P[M =' hi'|C =' xy'] =?$

$$P[C =' xy'|M =' hi'] = \frac{1}{26}$$

$$P[C =' xy'] \\ = P[C =' xy'|M = 'hi'].P[M =' hi] \\ + P[C =' xy'|M =' no'].P[M =' no'] \\ + P[C =' xy'|M =' in'].P[M =' in']$$

$$= \frac{1}{26.} * 0.3 + \frac{1}{26} * 0.2 + 0 = 1/52$$

$$P[M =' hi'|C =' xy'] = \frac{1}{26} * 0.3 * \frac{52}{1} = 0.6$$
$$\neq P[M =' hi']$$

$\Rightarrow$**The shift cipher is not perfectly secret!**

One-time pad

- Let $\mathcal{M} = \{0,1\}^n$
- KeyGen: Choose a uniform key $k \in \{0,1\}^n$
- Enc(k,m): c = $k \oplus m$ (bit-wise XOR)
- Dec(k,c): m = $k \oplus c$

- Correctness

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

One-time pad

Vernam Cipher

E { M 01001011100 …..

$\oplus$

K 10011101010 ….

$\downarrow$

C 11010110110 ….

D { $\oplus$

K 10011101010 ….

$\downarrow$

M 01001011100 ….

Perfect secrecy of one-time pad (Shannon)

- $\boldsymbol{P[M = m|C = c] = ?}$

$$= \frac{P[C = c|M = m] * P[M = m]}{P[C = c]}$$

$$P[C = c] = \sum_{m'} P[C = c|M = m'] * P[M = m']$$

$$= \sum_{m'} P[K = m' \oplus c] * P[M = m']$$

$$= \sum_{m'} (1/2)^n * P[M = m']$$

$$= \boldsymbol{2^{-n}}$$

$$\boldsymbol{P[M = m|C = c] = ?}$$

$$= \frac{\boldsymbol{2^{-n} * P[M = m]}}{\boldsymbol{2^{-n}}}$$

$$\boldsymbol{P[M = m|C = c] = P[M = m] \Rightarrow \textit{Perfect secrecy}}$$

More visual proof with message size=1

M : cleartext
C : ciphertext (1 bit)
K : key

	P[M=m]	p	1-p
P[K=k]	K \ M	1	0
1/2	1	0	1
1/2	0	1	0

P[M=m|C=c] = P[C=c|M=m]*P[M=m]/P[C=c]
=P[M=m]
$\Rightarrow$ Perfect secrecy

Distribution of M:
P[M=0]=p, p[M=1]=1-p

Distribution of K: Uniform
P[K=k]=1/2

P[C=0|M=0] = P[K=0]=1/2

P[C=0|M=1] = P[K=1]=1/2

P[C=1|M=0] = P[K=0]=1/2

P[C=1|M=1] = P[K=0]=1/2

$\Rightarrow$ P[C=c|M=m]=1/2

P[C=0] = ½.p+1/2(1-p)=1/2
P[C=1] = ½(1-p)+1/2(p)=1/2
$\Rightarrow$ p[C=c] = 1/2

One-Time Pad – Usage

- Achieves perfect secrecy
- Red phone between DC and Moscow

One-Time Pad - Limitations

- Key size = Message size
  - Parties need to share keys as long as the message
- Each key is used to encrypt a single message
  - Key needs to be re-generated for each new message

What happens if the same key is used twice?

- Let $c_1 = k \oplus m_1$ and $c_2 = k \oplus m_2$

- Attacker can compute $c_1 \oplus c_2 = m_1 \oplus m_2$

$\Rightarrow$ Leakage on m_1, m_2

- $m_1 \oplus m_2$=0 $\Rightarrow m_1 = m_2$, $m_1 \oplus m_2$=1 $\Rightarrow m_1 \neq m_2$

- Real-world examples
  - Project Venona (‘40s), MS-PPTP (windows NT)

One-time Pad

- Advantages
  - Perfect secrecy

- Drawbacks
  - Key as long as the message
  - Only secure if each key is used to encrypt once

  - Valid for all perfectly secret schemes (Shannon)

Optimality of the one-time pad

- Theorem If (KeyGen, Enc, Dec) with message space $\mathcal{M}$ is perfectly secret then $|\mathcal{K}| \geq |\mathcal{M}|$

- Proof
  - Assume $|\mathcal{K}| < |\mathcal{M}|$
  - Take any ciphertext c
  - Define M(c)={Dec(k,c)} with $k \in \mathcal{K}$

$$\Rightarrow |M(c)| \leq |\mathcal{K}| < |\mathcal{M}|$$

  which means that there exists m that is not M(c)
  - **P[M=m|C=c]=0 $\Rightarrow$ no perfect secrecy**

Secure Communications

Lecture 2: Perfect Secrecy, One-time Pad

Melek Önen

Fall 2022