CENG 374E - INTRODUCTION TO COMPUTER SECURITY

Prof. Dr. Şeref SAĞIROĞLU
Gazi University
Engineering Faculty
Computer Engineering Department
Maltepe/Ankara

SS@gazi.edu.tr
https://avesis.gazi.edu.tr/ss

Basic Cryptography

Cryptography

Studies techniques for secure communication in the presence of malicious third parties (adversaries)

Cryptography: Basic Definitions

Encryption: making messages unreadable to unauthorized parties

Decryption: converting encrypted message to the original

Cipher: algorithm for performing encryption or decryption

Plaintext: original meaningful message

Ciphertext: unreadable encrypted message

Key: parameter determining the output of cipher

Types of Ciphers

Classical ciphers:

- Transposition ciphers
- Substitution ciphers

Modern ciphers:

- Next lecture

Transposition Ciphers

Rearrange characters of plaintext to obtain ciphertext

Substitution Ciphers

Replace characters (or blocks of characters) with other characters

- Simple
- Homophonic: One plaintext symbol maps to multiple ciphertext symbols.
- Polyalphabetic: Multiple ciphertext alphabets
- Polygram: Substituting groups of letters

Caesar Cipher

- Substitution cipher
- One of the oldest and simplest ciphers known

Homophonic Ciphers

Replace each character by a group of characters

- Ciphertext alphabet is larger than the plaintext alphabet.

Polyalphabetic Ciphers

Use multiple mappings from plaintext alphabet to ciphertext alphabet.

Example: Vigenere cipher

Breaking Ciphers

Cryptanalysis

It is possible to break substitution ciphers using one of various methods.

- Frequency Analysis
- Kasiski Method
- Index of Coincidence Method

Frequency Analysis

Look at the frequencies of different letters to guess substitution rule.

Kasiski Method

Published by Friedrich Kasiski in 1863.

Idea: Repeating words might be encrypted using the same key letters.

Plaintext	GAZIUNIVERSITYISALARGEPUBLICUNIVERSITY
Key	GAZIGAZIGAZIGAZIGAZIGAZIGAZIGAZIGAZIGA
Ciphertext	MAYQANHDKRRQZYHAGLZZMEOCHLHKANHDKRRQZY

Kasiski Method

Published by Friedrich Kasiski in 1863.

Idea: Repeating words might be encrypted using the same key letters.

Use this to find the key length.

Plaintext	GAZIUNIVERSITYISALARGEPUBLICUNIVERSITY
Key	GAZIGAZIGAZIGAZIGAZIGAZIGAZIGAZIGAZIGA
Ciphertext	MAYQANHDKRRQZYHAGLZZMEOCHLHKANHDKRRQZY

Index of Coincidence Method

Friedman Test: **Invented in the 1920s by William Friedman**

Let the length of the text be N

Let the size of the alphabet be n.

$$\frac{F_i(F_i-1)}{N(N-1)}$$

$$\sum_{i=1}^{n}\frac{F_i(F_i-1)}{N(N-1)}=\frac{1}{N(N-1)}\sum_{i=1}^{n}F_i(F_i-1)$$

Consider the i-th letter a_i in the alphabet. Suppose a_i appears in the given text F_i times. Since the number of a_i's in the text is F_i, picking the first a_i has F_i different choices and picking the second a_i has only F_i-1 different choices because one a_i has been selected. Since there are $N(N$-1) different ways of picking two characters from the text, the probability of having two a_is is

Since the alphabet has n different letters and the above applies to each of them, the probability of having two identical letters from the text is

The *index of coincidence IC* or *IOC*, is the probability of two randomly selected letters being equal. The use of index of coincidence was first proposed by William F. Friedman in 1922

$$\mathrm{IC}=\frac{1}{N(N-1)}\sum_{i=1}^{n}F_i(F_i-1)$$

Index of Coincidence Method

Note that English has ***n*** = 26 letters.

Example 1

THERE ARETW OWAYS OFCON STRUC TINGA SOFTW AREDE SIGNO NEWAY
ISTOM AKEIT SOSIM PLETH ATTHE REARE OBVIO USLYN ODEFI CIENC
IESAN DTHEO THERW AYIST OMAKE ITSOC OMPLI CATED THATT HEREA
REN00 BVIOU SDEFI CIENC IESTH EFIRS TMETH ODISF ARMOR EDIFF
ICULT

The frequency count is as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
15	2	9	7	27	8	2	9	20	0	2	4	5	10	19	2	0	12	15	22	4	2	5	0	4	0

- The index of coincidence is 0.068101.
- The five highest frequency letters are **E**, **T**, **I**, **O** and **A** and **S** with 27, 22, 20, 19 and 15 occurrences, respectively.

Index of Coincidence Method

- The five most frequently used letters are **E** (13.11%), **T** (10.47%), **A** (8.15%), **O** (8.00%) and **N** (7.10%).
- The five least frequently used letters are **Z** (0.08%), **Q** (0.12%), **J** (0.13%), **X** (0.17%) and **K** (0.42%).
- Note that this table is generated from a sample of long English texts.
- Different samples yield slightly different results.

Frequency (%) of Letters in English Text

A	B	C	D	E	F	G	H	I	J	K	L	M
8.15	1.44	2.76	3.79	13.11	2.92	1.99	5.26	6.35	0.13	0.42	3.39	2.54
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
7.10	8.00	1.98	0.12	6.83	6.10	10.47	2.46	0.92	1.54	0.17	1.98	0.08

Perfect Secrecy

One-time pad

- Key length >= Plaintext length
- Key is never reused.
- Vernam cipher
- A table used

Plaintext	GAZIUNIVERSITYISALARGEPUBLICUNIVERSITY
Key	THISISALONGSECRETKEYANDITISUSEDONLYONCE
Ciphertext	ZHHACFIGSEYAXAZWTVEPGRSCUTAWMRLJRCQWGA

Crypto Approach and Algorithms

- Symmetric key cryptography vs. Asymmetric key cryptography
- Block ciphers vs. Stream ciphers
- DES, AES
- Types of attacks on ciphers

Disadvantages of One Time Pad

If OTP provides perfect secrecy, why do we need other ciphers?

- Secure key generation and key exchange are difficult.
- Generating truly random keys is difficult.
- Destroying one-time keys is impractical in digital environments.

Hence, we use other cryptographic tools and techniques.

Symmetric vs Asymmetric Key Cryptography

Symmetric key cryptography: Encryption key = Decryption key

- Shared secret key
- Also called "Private key cryptography"

Asymmetric key cryptography: Encryption key ≠ Decryption key

- Two keys, one secret, one public
- Also called "Public key cryptography"

Symmetric Key Cryptography

Block ciphers vs. Stream ciphers

- Block ciphers encrypt plaintext in blocks (groups of bits).
- Stream ciphers encrypt plaintext bit-by-bit.

Block Ciphers

Block size: n bits

Key size: k bits

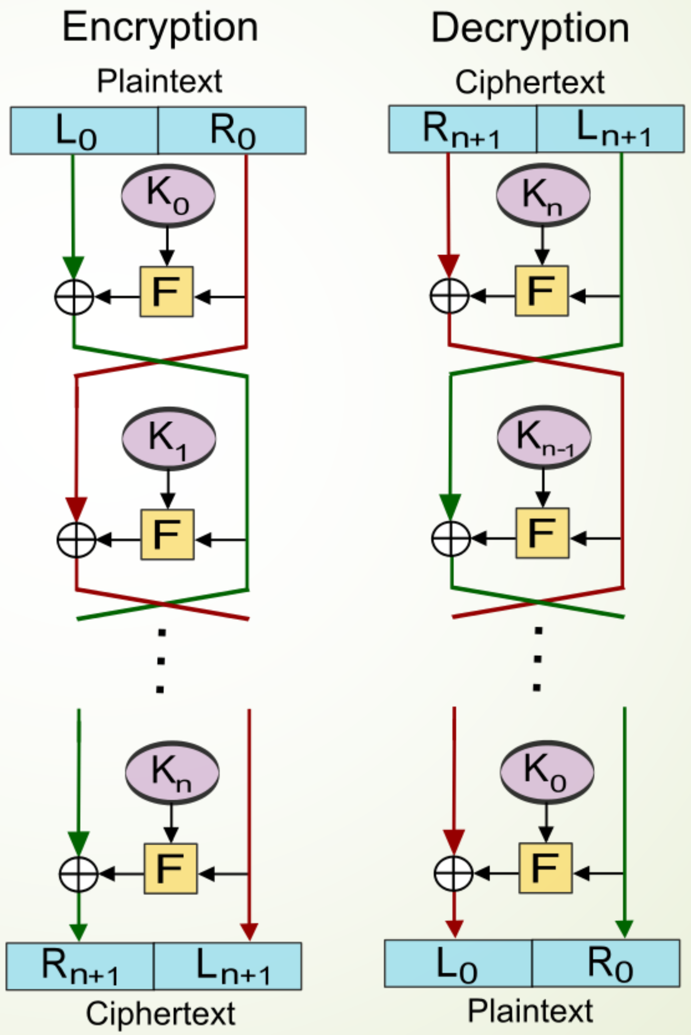
Iterated Block Ciphers

IBC’s consist of many rounds.

Feistel Ciphers

1. Split plaintext in two halves.
2. Apply the round function to one half.
3. XOR the output with the other half.
4. Swap the two halves.

Feistel Ciphers



Block Cipher Modes of Operation

- Block cipher encrypts only one block.
- How do we encrypt messages consisting of many blocks?
- There are several ways to do this.

Block Cipher Modes of Operation

Simple idea: Encrypt and decrypt each block independently.

- This is called **Electronic Codebook (ECB) mode.**
- **Problem:** Same plaintext ⊕ Same key = Same ciphertext
  - Attacker will know if two blocks are the same.
- **Problem:** Order of blocks can be changed by attacker.
  - Recipient will not know this, integrity will be lost.

Block Cipher Modes of Operation

Most modes use an initialization vector (IV).

- IV makes sure that the same (plaintext, key) pair produces different ciphertexts.
- Does not need to be secret, but should not be reused with the same key.

Block Cipher Modes of Operation

Cipher Block Chaining (CBC)

- Invented by IBM in 1976.

Block Cipher Modes of Operation

Output Feedback (OFB)

Some other modes:

- Propagating cipher block chaining (PCBC)
- Cipher feedback (CFB)
- Counter (CTR)

Data Encryption Standard (DES)

- Developed by IBM in the late 1970’s.
- Adopted as standard in the USA.
- Block size: 64 bits
- Key size: 56 bits
- Rounds: 16

Now considered not secure for most applications. Why?

Data Encryption Standard (DES) Security

- DES key size of 56 bits is too small.
- It is vulnerable to *brute-force attacks.*
- Can be broken in hours using distributed cloud computing.
- DES is no longer a standard.

- Triple DES is sometimes used: applying DES three times with different keys. This is still relatively secure.

Advanced Encryption Standard (AES)

- Developed in the late 1990’s, adopted as a standard in 2001.
- Based on the Rijndael (pr. “Rein-daal”) cipher by Vincent Rijmen and Joan Daemen.
- Block size: 128 bits
- Key size: 128, 192 or 256 bits
- Cycles: 10, 12 or 14
- Substitution-permutation network: series of substitutions and permutations

Advanced Encryption Standard (AES) Security

- Attacks have been described for versions of AES using fewer cycles.
- Full versions of AES are considered cryptographically secure.

Attacks on Ciphers

Attack Models: What does the attacker know?

We always assume the attacker knows how encryption and decryption are done.

- Algorithms are not (and should not be) secret!
- Key is secret.
- Goal: Discover a specific plaintext, or the key!
  - If the key is known, all plaintexts encrypted using that key can be discovered.

Attacks on Ciphers

Attack Models: What does the attacker know?

- Ciphertext-only attack (COA): Only ciphertexts are available.
  - Brute-force: Try all keys. Complexity depends on key length.
- Known-plaintext attack (KPA): Both plaintexts and corresponding ciphertexts are available.
  - Many different pairs may be known.

Attacks on Ciphers

Attack Models: What does the attacker know?

- **Chosen-plaintext attack (CPA) :** Attacker can choose plaintexts to be encrypted. *Customizable KPA*.

- **Chosen-ciphertext attack (CCA) :** Attacker can decrypt desired ciphertexts.

Attacks on Ciphers

Attack Models: What does the attacker know?

- **Related-key attack:** Attacker can encrypt the same plaintext with different but *related* keys.
- **Side-channel attack:** Attacker knows other types of information such as the time it takes to perform encryption steps or key sounds from typing the plaintext.

Attacks on Ciphers

- Differential cryptanalysis
  - Usually a chosen-plaintext attack by using *related* plaintexts.
  - Analyzes how a difference in the plaintext translates into a difference in the ciphertext.
- Linear cryptanalysis

Attacks on Ciphers

Meet-in-the-middle attack

- Type of known plaintext attack
- Targets cases where encryption is repeated with two or more keys.
- Example: Double encryption

Summary

- *Symmetric vs. Asymmetric Key Cryptography*
  - *Symmetric: Block ciphers vs. Stream ciphers*
    - *Block: Modes of operation, DES, AES*
- *Types of Attacks on Ciphers*
  - *Attack models: COA, KPA, CPA, CCA, RKA*

Q&A