Vietnam National University – Ho Chi Minh City
University of Information Technology - VNUHCM

3

Lab

FOR EDUCATIONAL PURPOSE ONLY

Classical Cryptography

Introduction to Information Assurance and Security

March 2023

Internal circulation only

<Strictly prohibited from posting on the internet in any form>

All feedback on the documents, please send to the email inseclab@uit.edu.vn

A. OVERVIEW

1. Introduction and learning objectives

- **Cryptography** plays a vital role in modern digital communication systems. The Oxford Dictionary[1] defines *cryptography* as "*the art of writing or solving codes*" with "*codes*" elsewhere defined as "*a system of pre-arranged signals, especially used to ensure secrecy in transmitting messages*". Historically, cryptography focused exclusively on ensuring private communication between two parties sharing secret information in advance using "code". It was used primarily for military, government applications, plus a few niche applications in industry for centuries.

  But cryptography nowadays is much more of a science. We would say that **modern cryptography** involved *"the study of mathematical techniques for securing information, systems, and distributed computations against adversarial attack*". Cryptography has gone from "*an **art** form that dealt with secret communication for the military*" to "*a **science** to secure systems for ordinary people all across the globe*". It deals with mechanisms for ensuring integrity, techniques for exchanging secret keys, protocols for authenticating users, electronic auctions and elections, digital currency, and more.
- The **learning objective** of this lab is for students to get familiar with the concepts in secret-key encryption, particularly in classical cryptography. After finishing the lab, students should gain first-hand experience with encryption algorithms. Moreover, students may use crypto tools and write simple programs to encrypt/decrypt messages. This lab will cover the following topics regarding classical ciphers:
  - **Monoalphabetic substitution ciphers - Frequency analysis.**
  - **Polyalphabetic ciphers.**
  - **Permutation ciphers.**

2. Backgrounds and Prerequisites

- To ensure everything goes smoothly and you achieve better results in this lab, you are expected to be familiar with cryptography concepts and gain enough background knowledge about symmetric cryptography, particularly in classical ciphers. Besides, programming skill (with your preferred language, e.g., Python, C/C++, Golang) is also necessary.

[1] https://www.oxfordlearnersdictionaries.com/

- The following section summarizes some of the key aspects to help you review the knowledge that you may already have obtained before getting started. You can also read the textbooks and related references that I listed in section 1.4 for more details.

Concept

Before beginning, we define some terms. When we're encrypting a message,

- **The plaintext (p)** refers to the original or unencrypted message.
- **The ciphertext (C)** refers to the coded or encrypted message.

A cipher is therefore composed of two functions:

- Encryption or Enciphering (E) turns plaintext into ciphertext.
- Decryption or Deciphering (D) turns a ciphertext back into plaintext.
  Written as functions:
- C = E(K_e,p)
- p = D(K_d, C)

where K_e and K_d are encryption key and decryption key, respectively

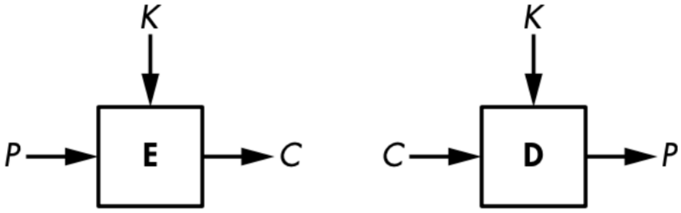


Figure 1. Basic encryption and decryption.

Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of **cryptanalysis** (breaking the code). The areas of cryptography and cryptanalysis together are called **cryptology**.

Taxonomy

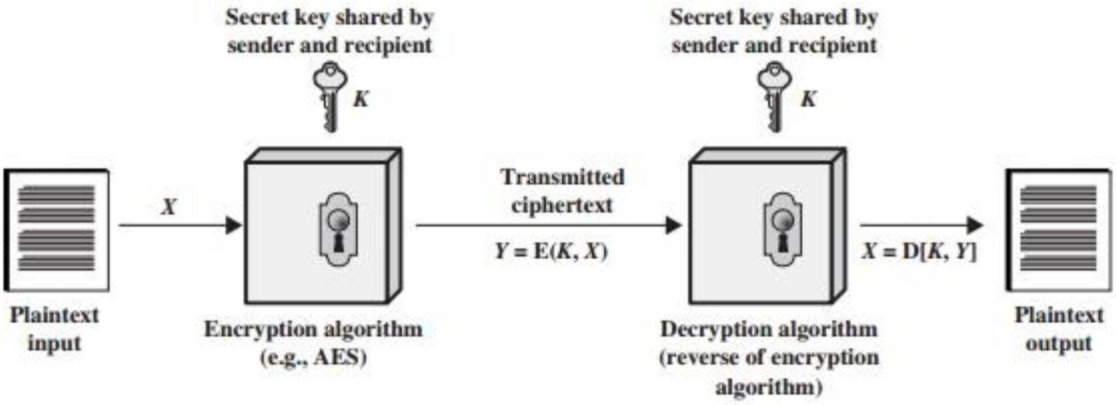

Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 2. Symmetric Encryption model.

Concerning encryption methodologies, there are two types of ciphers:

1. **Symmetric ciphers** (or *Secret-key ciphers*): Using single key for encryption and decryption. It was the only type of encryption in use prior to the development of public-key encryption in the 1970s (Figure 2).
2. **Asymmetric ciphers** (or *Public-key ciphers*): Use 2 related keys, a public key and a private key, which are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.

Classical ciphers are ciphers that predate computers, therefore work on letters rather than on bits and almost are symmetric ciphers.

The two basic building blocks of all encryption techniques are *substitution* and *transposition* (Figure 3).

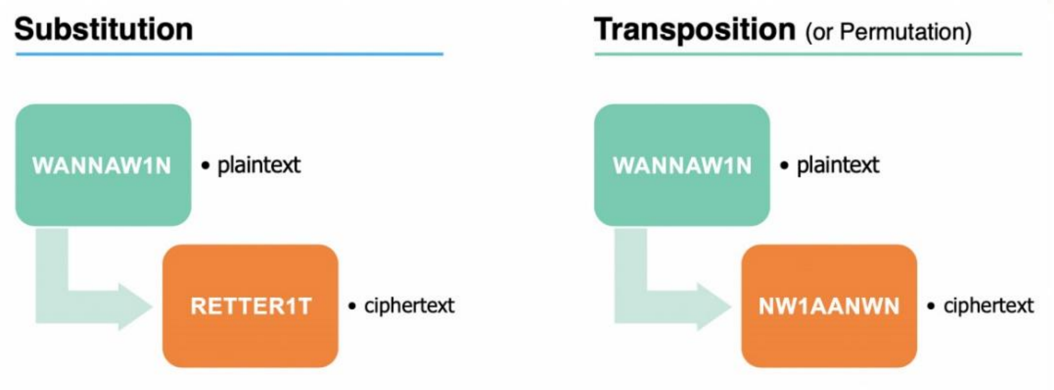


Figure 3. Substitution and Transposition example.

1. **Substitution ciphers**: replacing the letters of plaintext by other letters or by numbers or symbols.
2. **Transposition** (or **Permutation**) **ciphers**: performing some sort of permutation (or changing the order) on the plaintext letters.

B. LAB TASKS

1. Kickoff: Crack the code

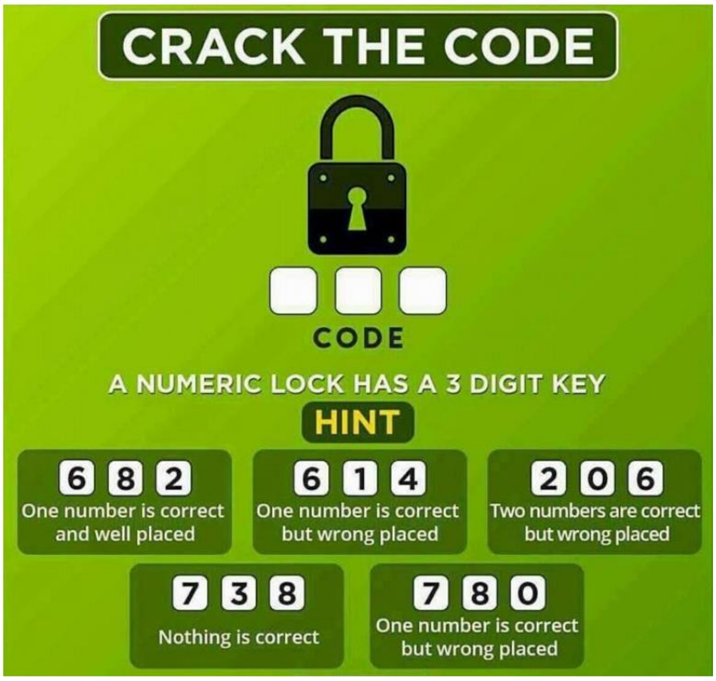
Task 1: Let's begin with a straightforward task that does not use any cipher algorithm. Try to solve the following codes:

1. We need to find the code to open the lock in figure 4. The lock has 3 digit pin which satisfies 5 conditions (hints) that are given . Can you crack this code? If it's possible, explain how.

2. Find the corresponding encoding for the numbers 1 to 9 according to the clues provided in table 1.2.1

- Each symbol in the set (△◁ ▷◯ ♡ ♠ ♢ ♣ ●) unique encoding for one of the number from 1 to 9.
- The rightmost column is the sum of the numbers in each row.
- The bottom row is the sum of the numbers in each column.

- Each ? can represent any one-digit or two-digit number and could be same or different from each other.



CRACK THE CODE

CODE

A NUMERIC LOCK HAS A 3 DIGIT KEY

HINT

6 8 2 One number is correct and well placed

6 1 4 One number is correct but wrong placed

2 0 6 Two numbers are correct but wrong placed

7 3 8 Nothing is correct

7 8 0 One number is correct but wrong placed

Figure 4. Crack the code to open the lock.

Table 1. Find the corresponding encoding for each number.

△	△	◁	○	?
♡	♡	♠	♡	◇◇
?	?	◁	♣	●●
?	♡	♠	♡	●▷
●♡	◇◇	●●	●◇	

2. Caesar cipher

Task 2: In this task, you must create an application in your chosen programming language that performs encryption and decryption using the **Caesar** cipher. The application should meet the following criteria:

- Enable user input for a key and either plaintext for encryption or ciphertext for decryption.

Provide the ability to perform a brute-force attack by trying all possible keys to decrypt a given ciphertext without knowing the key.

- To validate your program, test it with a message of at least 100 words and compare the results with other cryptography online tool, such as dcode (https://www.dcode.fr), CrypTool 2 online. Additionally, use your program to crack the following ciphertext:

Mfwzpn Rzwfpfrn bfx gtws ns Pdtyt ns 1949 fsi stb qnajx sjfw Ytpdt. Mj nx ymj fzymtw tk rfsd stajqx fx bjqq fx xmtwy xytwnjx fsi sts-knhynts. Mnx btwpx nshqzij Stwbjlnfs Btti, Ymj Bnsi-Zu Gnwi Hmwtsnhqj, Pfkpf ts ymj Xmtwj, Fkyjw Ifwp fsi Bmfy N Yfqp Fgtzy Bmjs N Yfqp Fgtzy Wzssnsl. Mnx btwp mfx gjjs ywfsxqfyji nsyt rtwj ymfs ktwyd qfslzfljx, fsi ymj rtxy wjhjsy tk mnx rfsd nsyjwsfyntsfq mtstzwx nx ymj Ojwzxfqjr Uwnej, bmtxj uwjantzx wjhnunjsyx nshqzij O.R. Htjyejj, Rnqfs Pzsijwf, fsi A.X. Sfnufzq.

Do you find any special concerning the key used to encrypt this ciphertext?

Tips: *Using the Caesar algorithm*

Encryption : C = E(k, p) = (p + k) mod 26

Decryption : p = D(k,C) = (C- k) mod 26

where C = Ciphertext, p = plaintext, k is key

3. Mono-alphabetic substitution cipher and frequency analysis

(This task is based on a lab in SEED Labs materials by Wenliang Du, Syracuse University.)

It is well-known that monoalphabetic substitution cipher (also known as the monoalphabetic cipher) is not secure because it can be subjected to frequency analysis. You are given a ciphertext encrypted using a monoalphabetic cipher in this lab. Each letter in the original text is replaced by another letter, where the replacement does not vary (i.e., a letter is always replaced by the same letter during the encryption.

Task 3: Click **here** to download the ciphertext file [2].

Your job is to find out the original text using frequency analysis. It is known that the original text is an English article.

Describe how to find the plain-text in detail (step-by-step).

Notice that you are not allowed to use the automatic mode of any tools (like CrypTool 2, dCode, quipqiup) to decrypt.

Tips: *Using the frequency analysis, you can find out the plain-text for some of the characters quite easily. For those characters, you may want to change them back to its plain-text, as you may be able to get more clues. It is better to use capital letters for plain-text, so for the same letter, we know which is plain-text and which is cipher-text*

If you are using Linux or MacOS, you can use the tr command to do this. For example, in the following, we replace letters a,e, and t in in.txt with letters X,G,E, respectively; the results are saved in out.txt.

```
$ tr ’aet’ ’XGE’ < in.txt > out.txt
```

[2] https://seedsecuritylabs.org/Labs_16.04/Crypto/Crypto_Encryption/files/ciphertext.txt

You can also use Cryptool or dCode to decrypt it manually by analyzing and replacing letters. There are many online resources that you can use. Two valuable links as the following:

- ***Cryptool Online N-gram analysis**: This website can produce the statistics from sequence), trigram frequencies (3-letter sequence), etc.*
- *http://norvig.com/mayzner.html: This web page provides frequencies for a typical English plaintext, including unigram, bigram, and trigram frequency.*

Advanced Task 3.1: Decrypt a cipher-text from Edgar Allan Poe's - The Gold-Bug and explain how to do:

53‡‡†305))6*;4826)4‡.)4‡);806*;48†8¶60))85;;]8*;:‡*8†83(88)5*†;46(;88*96
?;8)‡(;485);5*†2:*‡(;4956*2(5*—4)8¶8*;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡
1;48†85;4)485†528806*81(‡9;48;(88;4(‡?34;48)4‡;161;:188;‡?;

It is known that:

- The original text is an English article.
- The cipher-text does not include punctuation and spaces.
- Each symbol corresponds to a letter in the English alphabet.

4. Playfair cipher

Task 4: Write an application with your own programming language to encrypt and decrypt a message using **Playfair cipher**. Your application should satisfy the following requirements:

- Allow you to input a key and a plain-text to encrypt or a cipher-text to decrypt using the given key.
- Display the Playfair matrix (5x5) corresponding with the given key.

1. Test your program with an message of at least 100 words and compare the result with other cryptography tools (like Cryptool 2) to verify.
2. Using the Playfair matrix below (Table 1.2) to encrypt the following message.

Message: ***I only regret that I have but one life to give for my country.***

This message is by Nathan Hale, a soldier in the American Revolutionary War.

Table 2. Playfair Grid for Task 4 - Part 2.

J/K	C	D	E	F
U	N	P	Q	S
Z	V	W	X	Y
R	A	L	G	O
B	I	T	H	M

5. Polyalphabetic cipher – Vigenère

Task 5: Write an application using your chosen programming language to encrypt and decrypt a message using Vigenère cipher.

Test your application by a message with at least 100 words and a key of about 10-20 letters. Then verify the result with other cryptography tools (e.g., Cryptool 2, dCode, etc.)

6. Other ciphers – Capture The Flag

Task 6: Decode the following text to find the flag. It is known that the message was encoded with ASCII code:

87 101 108 99 111 109 101 32 116 111 32 67 114 121 112 116 111 32 73 115 108 97 110 100 33 33 33 32

Tips: You can refer to ASCII table at http://www.ascii-code.com

Task 7: The file crypto01.jpg can be downloaded from **here**, and it contains a flag. Knowing that this image was encrypted with XOR cipher by a 6-letter key. Let's find the flag and describe how to do

Tips: You can refer to https://www.dcode.fr/xor-cipher to learn how XOR cipher work.

Advanced Task 7.1: Describe another classical cipher that was not mentioned in this lab. Write an application and and give an demonstration to illustrate how it work.

C. REQUIREMENTS & EVALUATION

- Students are required to study and practice according to the instructions, carrying out the tasks in their assigned groups.
- Submission of the result report including the code, exported database, and details of the tasks (report) that the group has completed. Include observations and, if applicable, screenshots of the results; provide explanations for observations (if any).
- Report Format:
  - PDF file focusing on content, avoiding theoretical descriptions.
  - Naming convention: [Class Code]-LabX_StudentID1.
  - Example: [NT219.K11.ANTN.1]-Lab1_1852xxxx-.
  - If the report consists of multiple files, compress all files into a ZIP file with the same report name.
  - Submit the report within the agreed-upon timeframe on courses.uit.edu.vn.

Instances of plagiarism, delays, etc., will be handled based on the severity of the violation.

D. REFERENCES

[1] William Stallings, Cryptography and network security: Principles and practice, 7th ed, Pearson Education, 2017. Chapter 3. Classical Encryption Techniques

[2] Wenliang Du (Syracuse University), SEED Cryptography Labs https://seedsecuritylabs.org/Labs_16.04/Crypto/

[3] Bernhard Esslinger et al., The CrypTool Book: Learning and Experiencing Cryptography with CrypTool and SageMath, 12th ed, 2018. Available: https://www.cryptool.org/en/ctp-documentation

Training platforms and related materials:

- ASecuritySite - https://asecuritysite.com/
- Cryptopals - https://cryptopals.com/

THE END

Wishing you all the best in successfully completing the tasks!