University of Colorado
Denver

Department of Computer Science & Engineering

CSCI/CSCY 4407:: Security Cryptography
Lab 1 Assignment: Cryptography by Hand (Cracking Classical Ciphers)
Instructor: Dr. Victor Kebande
Teaching Assistant : Celest Kester
Spring 2026

---

1 Assignment Instructions

This is a **group assignment**. Each group is required to complete and submit its own original work. You may discuss general cryptography concepts with classmates; however, **you are not permitted to share, reuse, or copy** solutions, calculations, code, written explanations, or final answers. Each group has been assigned a unique task, and therefore the outputs are expected to be different across groups. The cryptographic key(s) required for this assignment have been uploaded to Canvas. Each group is responsible for identifying and using the correct key assigned to them when completing the tasks.

1.1 Academic Integrity and Collaboration

- **Allowed:** Discussing lecture content and general concepts at a high level.
- **Not allowed:** Sharing written answers, screenshots, solution files.
- **Not allowed:** Copying from the internet, friends, previous students, or public repositories.
- **Submission:** Only one file should be submitted for each group, that means only one member should submit the completed assignment on or before the deadline

2 Introduction

The purpose of this assignment is to provide practical, hands-on experience with a set of fundamental encryption algorithms commonly used in cryptography. Through this exercise, you will explore how these algorithms function and evaluate their role in achieving secure communication. The outcomes of the experiments, together with a clear description of the methods employed, must be presented in a comprehensive written report and submitted via It's Canvas. All submissions will be subject to plagiarism detection, and students are expected to adhere strictly to academic integrity guidelines.

2.1 Objectives

The main objective of this assignment is to introduce you to the fundamental cryptographic encryption techniques and to understand how simple ciphers are used to protect information. You should be able to:

- Understand the basic principles of cryptography, including plaintext, ciphertext, keys, and encryption.
- Implement and apply classical encryption algorithms such as the Caesar cipher, substitution ciphers and Vigenère Cipher.
- Perform encryption and decryption operations using given keys and parameters.
- Analyze the security properties and limitations of simple cryptographic algorithms.
- Compare different encryption methods in terms of strength, usability, and vulnerability to attacks.
- Gain experience in documenting cryptographic processes and results in a clear and structured manner.
- Develop reasoning skills by explaining each step of the encryption and decryption process.

By the end of this assignment, you should be able to demonstrate a fundamental understanding of how encryption algorithms work and critically reflect on their role in securing information systems.

2.2 Requirements

To complete this assignment, you are expected to meet the following requirements:

- You must work as a **group**. Each group must submit their own original work.
- You must produce a **written report in PDF format**.
- Your report must include:

  - A clear description of the methods used for each task.
  - The plaintexts, ciphertexts, keys, and intermediate results.
  - Short explanations and reasoning for each step.
  - Screenshots for each step if you are not required to use pen and paper.

- All calculations and cryptographic operations must be shown or explained, the instructor will not figure out what you mean without an explanation.
- You must answer all questions in complete sentences and use appropriate technical terminology.
- Any external tools or resources used (e.g., online simulators, textbooks, websites, or AI tools) must be properly cited how they have been used.
- The final report must be submitted as a **single PDF file** on Canvas before the deadline.
- Feedback will be given to submissions handed in on or before the deadline if necessary. No submissions will be graded/or no feedback will be given if they are handed in after the deadline

Failure to meet these requirements may result in a reduction of marks, even if the technical answers are correct.

3 Enigma

Enigma machine that is shown in Figure 1 is the name of both the encryption machine and the cryptographic algorithm used by the German military during the Second World War. It is widely believed that if the Allied forces (notably the Americans, British, and Russians) had not co-operated to understand and break the complexity of the Enigma system, the outcome of the war and consequently the world today, might have been very different.

The Enigma machine was an entirely mechanical device consisting of a set of rotating wheels (rotors), gears, and electrical circuits that together performed encryption. In many ways, it can be compared to an advanced typewriter, where each key press produces a different encrypted character depending on the internal rotor settings.

Read more here: German Cipher Machines of World War II

Your first task is to experiment with an Enigma encryption machine available online at the link above based on the link below at:

`https://cryptii.com/pipes/enigma-decoder`

Instructions:

In this task, you are required to interact with the online Enigma machine simulator. You must adjust the *rotor order*, *rotor starting positions*, and *ring settings* according to the given configuration. For each configuration:

Figure 1: Enigma Machine

- Set the specified rotors.
- Adjust the initial rotor positions.
- Configure the ring settings accordingly.
- Encrypt the given plaintext.

You must take clear screenshots showing:

- The rotor order.
- The rotor positions.
- The ring settings.
- The resulting ciphertext.

These screenshots must be included in your submission as evidence of correct configuration and execution.

3.1 Task 1: Enigma Encryption

1. Start by encrypting a message. The plaintext you should use can be found in the column next to your (Column 2) in the attached file. This column is labeled *"Plain text (encrypt)"*. Use the corresponding key provided in Column 3, labeled *"Enigma Key"*. The key represents the initial rotor settings for the Enigma machine.

2. Encrypt the plaintext and record the resulting ciphertext, and take screenshots to show the outcome.

3. Next, encrypt the ciphertext again using the same key and observe the result. Explain what happens and why this behavior occurs in the Enigma system.

4 Caesar Cipher

The Caesar cipher is one of the simplest and oldest encryption techniques that uses substitution as is shown in Figure 2. It is a type of substitution cipher in which each letter in the plaintext is replaced by another letter located a fixed number of positions further down the alphabet.

For example, with a shift of 3, the letter A is replaced by D, B becomes E, and so on. After reaching the end of the alphabet, the substitution wraps around to the beginning.

The method is named after Julius Caesar, who is known to have used this cipher in his private correspondence to protect sensitive military messages. **Read more here:** Caesar Cipher – GeeksforGeeks

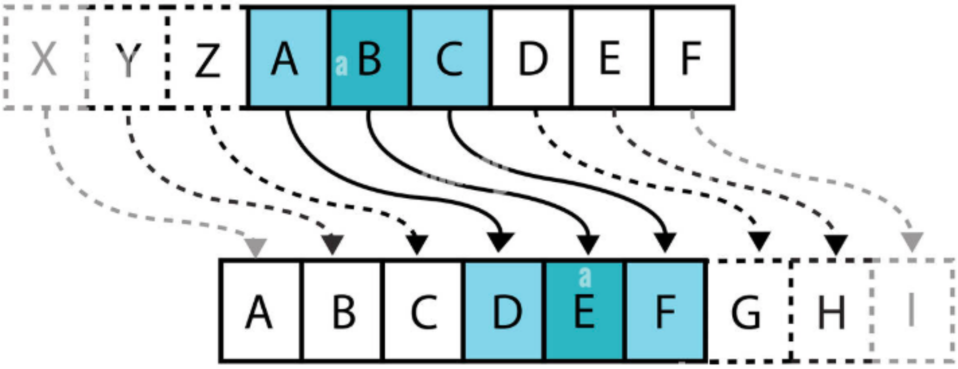


Figure 2: Illustration of the Caesar cipher with a shift of 3

Use online resources and relevant literature to find out more about how the Caesar cipher works. Based on your understanding, you are required to encrypt, decrypt, and manually crack a message.

4.1 Tasks

1. Encrypt the plaintext found in Column 2, labeled *"Plain text (encrypt)"*, using the key provided in Column 4, labeled *"Caesar key"*.

2. Decrypt the ciphertext found in Column 5, labeled *"Caesar cipher text (decrypt)"*, using the same key as in the previous step.

3. Crack the ciphertext found in Column 6, labeled *"Caesar cipher text (crack)"*, using only pen and paper. The use of automated cracking tools or software is strictly prohibited. You must clearly explain, step by step, the method you used to break the cipher. After decrypting scan or take a photo of your workings and append as part of the solution to this task. No grade will be awareded if this is not done manually using the traditional pen and paper.

5 Vigenère Cipher

The Vigenère cipher is a more sophisticated encryption technique than the Caesar cipher. It can be viewed as an extension of the Caesar cipher that supports a longer and more complex key. In the Caesar cipher, a single number is used to represent a fixed shift in the alphabet (for example, with a shift of 3, A becomes D). In contrast, the Vigenère cipher uses a word or a sequence of letters as the key, where each letter represents a different shift value. This results in a polyalphabetic substitution cipher, making the Vigenère cipher significantly more resistant to simple frequency analysis compared to the Caesar cipher.

For example, from Figure 3, using the Vigenère cipher with the keyword `KEY` to encrypt the plaintext `HELLO`, the key is repeated to match the length of the message, giving `KEYKE`. To encrypt the first letter, `H`, we select the row corresponding to `K` in the Vigenère table and the column corresponding to `H`; the intersection gives the ciphertext letter `R`. Repeating this process for each character produces the final ciphertext `RIJVS`.

5.1 Tasks

1. You are required to use pen and paper in the task below

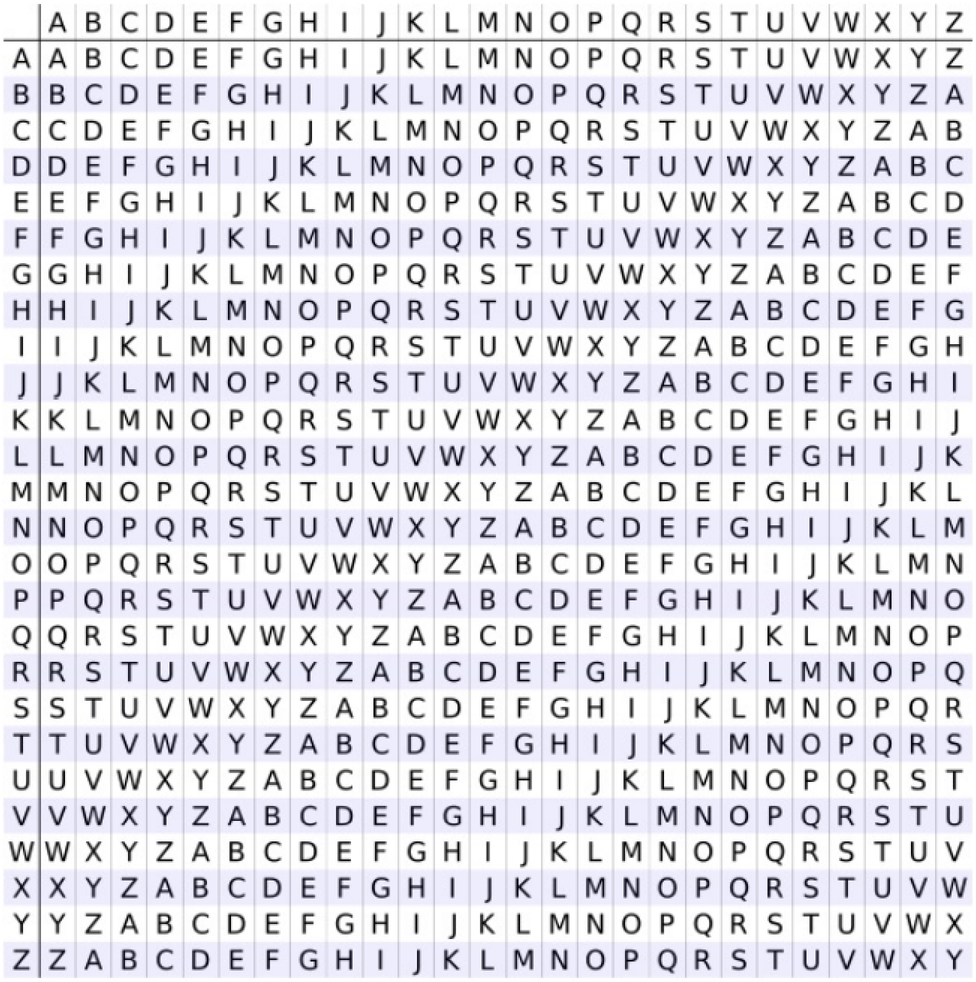
2. Encrypt the plaintext found in Column 2, labeled *"Plain text (encrypt)"*, using the key provided in Column 7, labeled *"Vigenère key"*, and the Vigenère cipher.

3. Decrypt the ciphertext found in Column 8, labeled *"Vigenère cipher text (decrypt)"*, using the same key as in the previous step.

6 Report

1. This is a group assignment.

2. All submitted solutions will be subject to plagiarism detection. Therefore, all material must be entirely your own work.



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

Figure 3: Illustration of Vigenère Table (Tabula Recta)

3. Any work performed using pen and paper (e.g., calculations, tables, or manual cracking steps) must be scanned and included in your final report. These pages must clearly show your group number and your names

6.1 Submission

Submit your completed assignment via Canvas. While submitting your report, please follow the submission rules outlined below:

1. The completed assignment must be submitted on the course Canvas page before the stated deadline. The submission must include scanned copies of any handwritten work (you may use a smartphone camera for scanning).

2. The submitted document must be in **PDF format**.

3. Assignments submitted via email or any other communication channel will **not** be accepted or graded.

examination opportunity to submit the assignment.

4. Your first page must include your full name(s) (as registered in Canvas), and your email addresses.

5. The due date for this assignment is 1/13/2026, observe deadlines

Grading Rubric (Total: 100 points)

Task	**Assessment Criteria**	**Points**
Enigma Cipher (Task 1)	Correct encryption	10
	Double encryption and explanation	10
	Clarity of method and reasoning	10
	Subtotal	**30**
Caesar Cipher (Task 2)	Correct encryption	10
	Correct decryption	10
	Manual cracking (no tools)	15
	Explanation of cracking method	5
	Subtotal	**40**
Vigenère Cipher (Task 3)	Correct encryption	10
	Correct decryption	10
	Subtotal	**20**
Report Quality	Structure, clarity, scanned work, formatting	10
	Total	**100**