Project: Hybrid Cryptosystem using Rotor Machine and DES Encryption

Objective: The objective of the project is to understand the significance of encryption, and effect of multi-layers of encryption on the overall security of the system. The other pertinent objectives pertaining to this project includes but not limited to:

1. Understand the operations of rotor machine, and data encryption standard (DES).
2. Practical implementations of rotor machine, DES, and a hybrid system that combines both.
3. Compare the security advantages and potential weaknesses of using a hybrid cryptographic system.
4. Gain practical experience in implementing encryption algorithms and managing encryption keys.

Overview of the project: In this project you will be working on constructing a hybrid cryptosystem that comprises of a Rotor Machine, and DES. This two layer encryption will add on to the security of the information being transmitted. As shown in the Fig. 1 the hybrid cryptosystem comprises of two stages namely rotor machine, and DES. The information to be transmitted, referred to as M, is first encrypted using Rotor machine, this encrypted text (also known as E_1) is once encrypted using DES, the resultant encrypted text is known as E_2. E_2 is the double encrypted ciphertext. Similarly, the decryption process is performed in the reverse direction. E_2 is decrypted using DES, the result deciphered text is referred to as D_1 which is once again decrypted using rotor machine to get a final decrypted text D_2. You need to test if the M and D_2 are same. Table 1 summarizes all the mathematical notations used in this project.

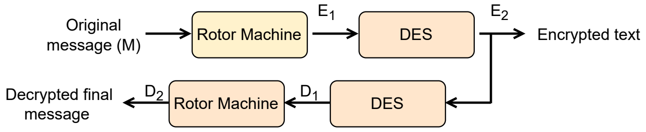

Figure 1: Hybrid Cryptosystem.

Table 1: Notations used in this project

Notation	**Description**
M	Original message to be transmitted
E_1	First encryption using rotor machine
E_2	Second encryption using DES
D_1	First decryption using DES
D_2	Second decryption using rotor machine

Description of the tasks: There are three main tasks to be performed in this project. These tasks are outlined as follows:

Task-1: Implement rotor machine - In this task a classic rotor machine should be implemented subject to the following conditions:

- Rotor machine should have 3 rotors
- Develop a code that simulates the working of rotor machine in such a way that each rotor should rotate after character is encrypted.
- The developed system should include provisions for decryption process too.
- Test your rotor machine design using the following messages: 'HELLO', 'HOPE', and 'NEW YEAR'. Document your results in the format shown in Table 2.

Table 2: Documenting the results of rotor machine

Initial Information	**Encrypted Text**	**Decrypted Text**
HOPE		
HELLO		
NEW YEAR		

Task-2: Implementing DES - In this task DES scheme should be implemented. Test the operation of the developed DES scheme using the same three original messages given in Task-1, and document the results once again similar to Table 1.

Task-3: Implement hybrid Cryptographic system - In this task two layer encryption will be done. First, M will be passed through rotor machine to get E_1, which then should be passed through DES to get E_2. In the similar manner decryption process should be done. Test the developed hybrid system on the following messages, and document the results as shown in Table 3

Table 3: Documenting the results of hybrid cryptosystem

Original Information (M)	E_1	E_2	D_1	D_2
HOW ARE YOU				
HAPPY NEW YEAR				
WELCOME TO PUERTO RICO				

Discussion Questions: Based on the hybrid cryptosystem answer the following questions:

1. How does the initial rotor position affect the encryption process? Provide examples to demonstrate how different initial rotor settings produce different ciphertexts for the same plaintext.

2. Discuss the process of decryption in a rotor machine. How does the structure of the machine ensure that decryption with the same rotor settings as encryption will return the original message?

3. Consider two scenarios: (1) Using the same initial rotor positions for multiple messages and (2) Using different initial rotor positions for each message. How do these scenarios impact the overall security of the rotor machine encryption?

4. Discuss the key schedule in DES. How are the 56-bit keys generated for each round of the encryption process? What effect does this have on the strength of the encryption?

5. DES uses 16 Feistel rounds. Explain why multiple rounds of encryption (in this case, 16) are necessary to create a secure cipher. What would happen if fewer rounds were used? Justify your response by considering few examples.

6. What is the role of padding in DES encryption? Why is padding necessary, and what padding schemes can be used? What are the potential issues that could arise if padding is not handled correctly?

7. Consider the computational performance of the hybrid cryptosystem with standalone rotor machine, and DES using the evaluation metrics such as computational complexity, resource utilized, and the total time taken and document the results in Table 4. Analyze the results by explaining the benefits, and limitations of hybrid cryptographic systems.

Table 4: Comparing the performances of three different cryptographic systems

Metric	**Rotor Machine**	**DES**	**Hybrid Cryptosystem**
Computational Complexity			
Computation time			
Resource utilized			

8. Discuss the practicality of using a hybrid cryptosystem like Rotor Machine + DES in modern encryption applications. Could this approach be applied in real-world situations? If so, suggest few potential places where it can be applied.

Instructions for completing and submitting the project: Please read through the instructions carefully before starting to work on the hybrid Cryptosystem.

1. You are free to use any programming language. However, Python is recommended to complete this work due to its relatively simpler usage.

2. Students are encouraged to reduce the dependence on in-built functions, try to develop functions on your own from scratch for the implementations.

3. All the codes that were used in implementing your tasks must be submitted separately as text (txt) files. Sufficient explanations for the codes must be provided within the code. You can submit it as a one zip file comprising of the solutions for this project, and codes developed. Label the zip file in the following manner: "<group-number>_<project-1>". For instance, "Group-X_project-1". One per group need to submit their work.

4. For every task, the screenshot generated from your code for the questions asked must be pasted and explained sufficiently.

5. Follow the flow provided in this project, and respond to the questions in the same order (using the same headings). The responses to the descriptive questions must be as detailed as possible with sufficient information.

6. The entire project response must be typed on computer, and it must be submitted in PDF format only. Any format will not be accepted.

7. Additional points or bonus points will be provided for doing tasks that are salient, and beyond the ambit of the project.

8. The project must be done in groups of two only. If you don't a project partner, the instructor must be approached as soon as possible.

9. If there are two students say A and B. A has special accommodation, while B does not. In this case deadline will be the deadline of the student with accommodation (A in this case).

10. One per group will submit the project with names of all the members in the group.

11. **Points will be deducted for not following the instructions and guidelines provided in this project.** For instance, demonstrating this Hybrid cryptography system on any standard applications or adding another layer of encryption and decryption or anything that you think would be ideal but provide strong justification for your efforts. Final decision to award the bonus points will be at the discretion of the Instructor.

Grading and Evaluations: The bifurcation of points for this project is discussed in Table 5. This project is for 100 points excluding the Bonus.

Table 5: Evaluation rubric

Criteria	**Points**
Task-1	20
Task-2	20
Task-3	30
Discussion Questions	30
Bonus	10

Deadlines: The following deadlines must be followed strictly. [1]

Start Date	November 7, 2025
End Date*	November 21, 2025

[1] *Deadline for groups with students without any special accommodations. For those groups with students having accommodation, the deadline is November 30, 2025.