

INDEX

S.NO	TITLE	SIGN
1	<p>Alice and Bob wish to share private message using a shift cipher algorithm to ensure confidentiality. Both can work as a sender and receiver so individual function should be implemented for encryption, decryption and brute force with the following conditions:</p> <ul style="list-style-type: none"> • Plain text should be in lowercase. (not accept any number and special symbol) • Cipher text should be in uppercase. (not accept any number and special symbol) • Brute force attack. (Find the key value) 	
2	<p>Alice and Bob wish to share private message using a multiplicative cipher algorithm to ensure confidentiality. The key value taken by both parties should be co prime with modulo 26. Both can work as a sender and receiver so individual function should be implemented for encryption, decryption and brute force with the following conditions must be satisfy:</p> <ul style="list-style-type: none"> • Plain text should be in lowercase. (Not accept any number and special symbol) • Cipher text should be uppercase. (Not accept any number and special symbol) 	
3	<p>To enhance the security Amit and Anil are agreed to use the affine cipher algorithm with two keys. So that the first key must be co prime with modulo 26 and second key varies from 1 to 26. Both can work as a sender and receiver so individual function should be implemented for encryption, decryption and brute force with the following conditions must be satisfy:</p> <ul style="list-style-type: none"> • Plain text should be in lowercase. (Not accept any number and special symbol) • Cipher-text should be uppercase. (Not accept any number and special symbol) 	
4	<p>Rust-om wants to send a confidential message "meet me after toga party" to kelvin. So both are ready to share the initial key and other keys are generated automatically then individual function should be implemented for encryption, decryption and brute force with the following conditions must be satisfy:</p> <ul style="list-style-type: none"> • Plain text should be in lowercase. (Not accept any number and special symbol) • Cipher text should be uppercase. (Not accept any number and special symbol) • Brute force attack. (Find) (Find the key value) 	
5	<p>The project investigates a cipher that is somewhat more complicated than the simple substitution cipher. In the Play fair cipher, there is not a single translation of each letter of the alphabet, that is, you don't just decide that every B will be turned into an F. Instead, pairs of letters are translated into other pairs of letters. Here is how it works. To start, pick a keyword that does not contain any letter more than once. For example, I'll pick the word keyword. Now write the letters of that word in the first squares of a 5*5 matrix. Then finish filling up the remaining squares of the matrix with the remaining letters of the alphabet, in alphabetical order. Since there are 26 letters and only 25 squares, we assign I and l to the same square. So implement Play fair Cipher to encrypt & decrypt the given message where the key matrix can be formed by using a given keyword.</p>	
6	<p>Write a program to implement Hill Cipher to encrypt & decrypt the given message by using a given key matrix. Show the values for key and its corresponding key inverse values</p>	
7	<p>ElGamal cryptosystem can be defined as the cryptography algorithm that uses the public and private key concepts to secure communication between two systems. It can be considered the asymmetric algorithm where the encryption and decryption happen by using public and private keys. In order to encrypt the message, the public key is used by the client, while the message could be decrypt-ed using the private key on the server end. This is considered an efficient algorithm to perform encryption and decryption as the keys are extremely tough to predict. The sole purpose of introducing the message transaction's signature is to protect it against MITM, which this algorithm could very effectively achieve. Write a program to implement Elgamal Cryptosystem to generate the pair of keys and then show the encryption & decryption of a given message</p>	
8	<p>Write a program to implement Rabin Miller Primality Test to check whether given number is prime or composite.</p>	
9	<p>User A and B want to communicate with each other by shared key so both parties decided that using Asymmetric key cryptography to generate a shared key and exchange with the help of Diffie-Hellman key exchange Algorithm. Perform exchange encryption & decryption using key exchange algorithm</p>	
10	<p>Alice uses a Bob's public key for sending a confidential message. Alice select a two large prime numbers to generate a private and public key so that eve could not break the cipher text. So as a developer implement this Algorithm to generate a pair of keys and each message should be encrypted by different key pairs.</p>	
11	<p>Alice is of one of the employee of company XYZ. He wants to ensure that whatever data he is sending to Bob should be checked for accuracy. Implement the RSA digital signature for the message "This is an example" for showing the Digital Signature in such a scenario.</p>	
12	<p>Alice is of one of the employee of company XYZ. He wants to ensure that whatever data he is sending to Bob should be checked for accuracy. Implement the Elgamal digital signature for the message "Hello how are you" for showing the Digital Signature in such a scenario</p>	