Guidelines for Assignment Execution

1) *Affine Cipher*

.Consists of two files:

- *Affine_cipher_encryption.cpp for encrypting any text specified in plain_input_affine.txt and the encrypted output generated is stored in encrypted_output_affine.txt*

- *Affine_cipher_decryption.cpp for decrypting the text stored in encrypted_output_affine.txt into plain text. The output of this cpp file is stored in plain_output_decrypted.txt*

. Example files are generated by using a = 17 and b = 3 in the following equations:

// for encryption

*y (cipher_value) = (a * x (plain_text_value) + b) % 26*

// for decryption

*x (plain_text_value) = ((a ^ -1) * ((y (cipher_value) - b + 26) % 26)) % 26*

.However the files can generate encrypted and decrypted output for any values of a and b

2) *Playfair Cipher*

.Consists of two files:

- *Playfair_cipher_encryption.cpp for encrypting any text specified in plain_input_playfair.txt and the encrypted output generated is stored in encrypted_output_playfair.txt*

- *Playfair_cipher_decryption.cpp for decrypting the text stored in encrypted_output_playfair.txt into plain text. The output of this cpp file is stored in decrypted_output_playfair.txt*

. Example files are generated by using Keyword: - PLAYFAIR EXAMPLE

.However the files can generate encrypted and decrypted output for any input keyword string

3) *Hill Cipher*

.Consists of two files:

- *Hill_cipher_encryption.cpp for encrypting any text specified in plain_input_hill.txt and the encrypted output generated is stored in encrypted_output_hill.txt*

- *Hill_cipher_decryption.cpp for decrypting the text stored in encrypted_output_hill.txt into plain text. The output of this cpp file is stored in decrypted_output_hill.txt*

. Example files are generated by using Keyword: - GYBNQKURP

The associated Keyword matrix is as follows:

6, 24, 1

13, 16, 10

20, 17, 15

The associated inverse Keyword matrix is as follows:

8, 5, 10

21, 8, 21

21, 12, 8

4) *Diffie Hellman*

.Consists of three files:

- *Diffie_Hellman.cpp is used for demonstrating key exchange protocol using Diffie Hellman, between Alice and Bob. The files associated with it are Alice.txt and Bob.txt*

- *Diffie_Hellman_Attack.cpp is used for demonstrating man in middle attack during key exchange protocol between Alice and Bob. The files associated with it are Alice_attacked.txt, Bob_attacked.txt and Attacker.txt*

- *Delay.cpp is used for calculating the communication delay between Alice and Bob when key sizes are 128, 256, 512 and 1024 bits. The output file for it is Diffie_Hellman_Delays.txt*

. Example files are generated by using g = 7 and n = 11 (publicly known) in the following equation:
(g ^ (xy)) mod n

.Values of x and y are randomly chosen by Alice and Bob who are exchanging data

.However the files can generate shared secret key for any values of g and n