Name: Sohel Momin

Roll No:1513126/a4

CSS EXPERIMENT 4

**Program:**

%% CRYPTANALYSIS OF AFFINE CIPHER using KNOWN PLAINTEXT

% C1 = (P1\*k1 + k2)mod26

% C2 = (P2\*k1 + k2)mod26

% programs asks no. of algorithms and checks plaintext,ciphertext for each

% one. If the algorithm used was affine, it decrypts a user-entered encrypted string

clc;clear variables;close all;

%%

alg = input('Enter the no. of algorithms to check -> ');

for i=1:alg

%% Get corresponding plaintext,ciphertext pairs

p = double(input('Enter Plaintext pair -> ','s'));

c = double(input('Enter Ciphertext pair -> ','s'));

p = p - 65\*ismember(p,65:90) - 97\*ismember(p,97:122); % so that upper/lower case doesn't matter

c = c - 65\*ismember(c,65:90) - 97\*ismember(c,97:122); % so that upper/lower case doesn't matter

%% Calculate keys

D = p(1)-p(2);

[D\_inv,gcd] = mulinv(D,26);

if gcd ~= 1

fprintf('Calculation of keys not possible for this plaintext pair\n');

continue

end

k1 = mod(D\_inv\*(c(1)-c(2)),26);

k2 = mod(D\_inv\*(p(1)\*c(2)-p(2)\*c(1)),26);

[k1\_inv,gcd] = mulinv(k1,26);

if gcd ~= 1

fprintf('The key obtained for this algorithm is not valid\n');

continue

end

%% DECRYPTION ( if the keys are valid )

fprintf('This algorithm if an affine cipher and keys are k1=%d, k2=%d\n',k1,k2);

enc\_msg = double(input('Enter the encrypted message -> ','s'));

enc\_msg = enc\_msg - 65\*ismember(enc\_msg,65:90) - 97\*ismember(enc\_msg,97:122); % so that upper/lower case doesn't matter

dec\_num = mod((enc\_msg-k2)\*k1\_inv,26);

dec\_msg = char(dec\_num + 97);

fprintf('The decrypted message is -> "%s"',dec\_msg);

end

**OUTPUT**

Enter the no. of algorithms to check -> 2

Enter Plaintext pair -> et

Enter Ciphertext pair -> wc

The key obtained for this algorithm is not valid

Enter Plaintext pair -> et

Enter Ciphertext pair -> wf

This algorithm if an affine cipher and keys are k1=11, k2=4

Enter the encrypted message -> wvwafjcroauerlfwvwacg

The decrypted message is -> "electronicsandtelecom"