For questions 1 -3 decode each message. The techniques used to encrypt the

messages are given in parentheses right before the cipher text. In your write-up, explain the process you used to decrypt and include any code you might have used as an aid. Please do not use websites that automatically solve ciphers as most of your grade will be based on your description of the decryption process and original code you include in your write up.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| P | Q | R | S | T | U | V | W | X | Y | Z |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

//SHIFT CIPHER

#include <stdio.h>

#include <string.h>

#include <stdlib.h>

#include <ctype.h>

int main()

{

char code[] = "hvwgwgxighhvstwfgheisghwcbrcbhpshvfckbcttpmhvsoddsofobqstoe";

char ans;

int i, key;

for(key = 0; key < 26 ; key++)

{

printf("Shift by %i: ", key);

for(i = 0; code[i] != '\0'; ++i)

{

ans = code[i];

ans = ans + key;

if(ans > 'z' || ans < 'a')

ans = ans - 'z' + 'a' - 1;

printf("%c", ans);

}

printf("\n");

}

return 0;

}

1) (shift)

hvwgwgxighhvstwfgheisghwcbrcbhpshvfckbcttpmhvsoddsofobqstoe

thisisjustthefirstquestiondontbethrownoffbytheappearancefaq

I used my code above to solve the shift cipher.

2) (shift)

padhzaolilzavmaptlzpadhzaoldvyzavmaptlz

itwasthebestoftimesitwastheworstoftimes

I used my code above to solve the shift cipher.

3) (affine)

xszvtekogmkveshysgtubvslssavtzsgitvtzmmtghbzmbuhbvcmlrmdskkeflmbmqedtmzwmhvktsdmysgbebhvimvqzskkmymb

forthisquestionyouhadtolookthroughthreehundredandtwelvepossibledeciphermentshopeyoudidntgetcrosseyed

I made a decrypt function in Java.

//AFFINE CIPHER

class Affine

{

static String decrypt(String encrypt)

{

String msg = "";

int inv = 0;

int flag = 0;

//a=1,3,5,7,9,11,15,17,19,21,23,25

//b=0-25

for(int a = 1; a < 26 && a != 13; a++)

{

for(int b = 0; b < 26; b++)

{

msg+="------------";

for (int i = 0; i < 26; i++)

{

flag = ((a \* i) % 26);

if (flag == 1)

inv = i;

}

for (int i = 0; i < encrypt.length(); i++)

msg = msg + (char)(((inv \* ((encrypt.charAt(i) + 'A' - b)) % 26)) + 'A');

}

}

return msg;

}

public static void main(String[] args)

{

String msg = "XSZVTEKOGMKVESHYSGTUBVSLSSAVTZSGITVTZMMTGHBZMBUHBVCMLRMDSKKEFLMBMQEDTMZWMHVKTSDMYSGBEBHVIMVQZSKKMYMB";

System.out.println(decrypt(msg));

}

}

4) Using the affine cipher with the encryption keys a = 15

and b = 19, encrypt the following plaintext:

packmyboxwithfivedozenliquorjugs

ktxnrpivaljsuqjwbmvebgcjzhvoyhfd

I just did this one by hand, not code, because it is easier to have the keys and to encrypt.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| X | E | L | S | Z | G | N | U | B | I | P | W | D | K | R |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| P | Q | R | S | T | U | V | W | X | Y | Z |
| Y | F | M | T | A | H | O | V | C | J | Q |