Block Ciphers

2.1) Write a C Program to implement one-time pad cipher.

Program:

#include<stdio.h>

#include<string.h>

#include<ctype.h>

main()

{

int i,j,len1,len2,numstr[100],numkey[100],numcipher[100];

char str[100],key[100],cipher[100];

printf("enter a string text to encrypt\n ");

gets(str);

for(i=0,j=0;i<strlen(str);i++)

{

if(str[i]!='\0')

{

str[j]=toupper(str[i]);

j++;

}

}

str[j]='\0';

for(i=0;i<strlen(str);i++)

{

numstr[i]=str[i]-'A';

}

printf("enter key string of random text:");

gets(key);

for(i=0,j=0;i<strlen(key);i++)

{

if(key[i]!='\0')

{

key[j]=toupper(key[i]);

j++;

}

}

key[j]='\0';

for(i=0;i<strlen(key);i++)

{

numkey[i]=key[i]-'A';

}

for(i=0;i<strlen(str);i++)

{

numcipher[i]=numstr[i]+numkey[i];

}

for(i=0;i<strlen(str);i++)

{

if(numcipher[i]>25)

{

numcipher[i]=numcipher[i]-26;

}

}

printf("one Time pad cipher text is \n");

for(i=0;i<strlen(str);i++)

{

printf("%c",(numcipher[i]+'A'));

}

printf("\n");

}

Output:

