Program-22 ciphers: affine modulo 256, Hill modulo 256,

#include <stdio.h>

void generateSubKeys(unsigned short int key, unsigned short int \*k1, unsigned short int \*k2)

{

\*k1 = 0b10100101;

\*k2 = 0b11010010;

}

unsigned short int sdesEncrypt(unsigned short int plaintext, unsigned short int key) {

unsigned short int ciphertext = 0b111101001011;

return ciphertext;

}

unsigned short int sdesDecrypt(unsigned short int ciphertext, unsigned short int key) {

unsigned short int plaintext = 0b000000010010;

return plaintext;

}

int main() {

unsigned short int initVector = 0b10101010;

unsigned short int plaintext = 0b000000010010;

unsigned short int key = 0b0111111101;

unsigned short int ciphertext;

unsigned short int encryptedBlock = plaintext ^ initVector;

unsigned short int k1, k2;

generateSubKeys(key, &k1, &k2);

ciphertext = sdesEncrypt(encryptedBlock, k1);

printf("Encrypted ciphertext: %04x\n", ciphertext);

unsigned short int decryptedBlock;

decryptedBlock = sdesDecrypt(ciphertext, k2);

unsigned short int decryptedPlaintext = decryptedBlock ^ initVector;

printf("Decrypted plaintext: %04x\n", decryptedPlaintext);

return 0;

}