1. plaintext space and ciphertext space is {A…Z}, key space is

define cryptosystem:

bb

1. The encryption functions of a block cipher are permutations. So, the maximum number of encryption function is (|Σ|n)! = 2n!

3.

a) Cipher text for “TEXAS”:

T: 19 E: 4 X: 23 A: 0 S: 18

11p+5(mod 26):

7: G 23: X 24: Y 5: F 21:V

So the result is: GXYFV

b) Plaintext for “OKLAHOMA”:

O: 14 K:10 L:11 A:0 H:7 O:14 M:12 A:0

To solve this, assuming 11x=1 mod 26

Using Extended Euclidean Algorithm, we have:

26=2\*11+4

11=2\*4+3

4=1\*3+1

So: 1=4-1\*3=4-1\*(11-2\*4)=3\*4-1\*11=3(26-2\*11)-1\*11=3\*26-7\*11

So x=-7 mod 26 = 19

Thus: 19\*11\*p = 19(c-5)

19\*11\*p mod 26 =p mod 26 = 19(c-5) mod 26

Then the corresponding p:

15: P 17: R 10:K 9:J 12:M 15:P 3:D 9:J

So plaintext is PRKJMPDJ

4.

93 can be represented in binary as: 10010011

Using extended Euclidean Algorithm:

x^8+x^4+x^3+x+1=x\*(x^7+x^4+x+1)+(x^5+x^4+x^3+x^2+1)

x^7+x^4+x+1=(x+x^2)\*(x^5+x^4+x^3+x^2+1)+(x^4+x^3+x^2+1)

x^5+x^4+x^3+x^2+1=x\*(x^4+x^3+x^2+1)+(x^2+x+1)

x^4+x^3+x^2+1=x^2\*(x^2+x+1)+1

And we have:

1=(x^6+x^5+x^3+x^2+1)(x^7+x^4+x+1)+(x^5+x^4+)( x^8+x^4+x^3+x+1)

Now, calculate the inverse of x^7+x^4+x+1, using sage:

F2.<x>=GF(2)[]

F2\_8.<x>=GF(2^8,modulus=x^8+x^4+x^3+x+1)

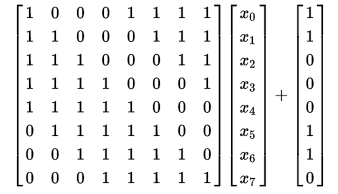
1/(x^7+x^4+x+1)

Out:

x^6 + x^5 + x^3 + x^2 + 1

The result above is the multiplicative inverse of x^7+x^4+x+1

Then using the multiplicative inverse is transformed using the following affine transformation:



where [x7, ..., x0] is the multiplicative inverse as a vector.

Then the result is:

[0 0 1 1 1 0 1 1]’, hence in hexadecimal is 0xdc

5.

Assuming we

W=[a1 b1 c1

a2 b2 c2

a3 b3 c3]

C=[1 1 0

0 1 0

1 0 1]

We have equations as following:

W\*[1 0 0]’=[1 0 1]

W\*[1 1 0]’=[1 1 0]

W\*[1 1 0]’=[0 0 1]

So a1=1, b1=0, c1=1, a2=0, b2=1,c2=1;a3=1,b3=1,c3=1

A=[1 0 1

0 1 1

1 1 1]

6.

If C = MP+S(where c is the ciphertext and p is the plaintext), then we know that for Vigenere cipher, m=I. And we have:

M:12 T:19 Y:24 G: 6 H:7

If plaintext is ALICE, then

A: 0 L: 11 I: 8 C: 2 E: 4

So S = [12 8 16 4 3]’=”M I Q E D”

If the plaintext is TEXAS:

T: 19 E: 4 X: 23 A: 0 S: 18

So S=[19 15 1 6 15]’=”T P B G P”