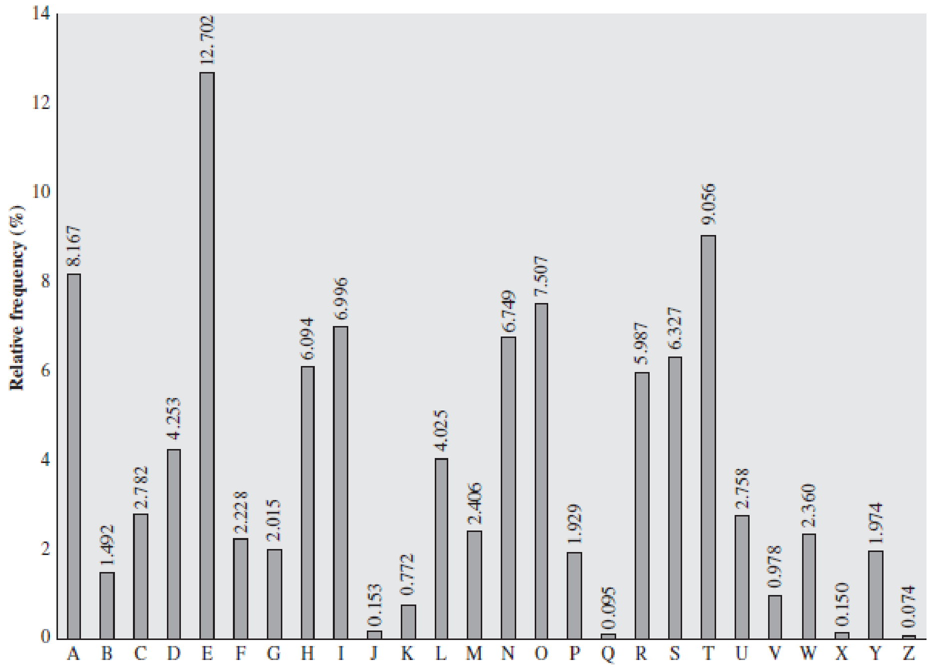
Cryptography Exam 1

Name ______________________ Date 2/8/16 (Closed note, computer, book)

Problem 1. A ciphertext has been generated with an affine cipher.The most frequent letter of the ciphertext is ‘B’, and the second most frequent letter of the ciphertext is ‘U’. Break this code.



E(4) --> B(1)
T(19) --> U(20)

(P,C)=(4,1) (P,C)=(19,20)
Encryption equation: C=(aP+b)mod26
C=Ciphertext
P=Plaintext

1=(4a+b)mod26
20=(19a+b)mod26

Solving two simultaneous equations, by subtracting the equations:

a = (1/15).19 mod 26 = 7.19 mo 26 = 133 mod 26 = 3 ---> a=3
where (1/15) is found using:
(1/15) . 15 = 1 mod 26 By trial and error: (1/15)= 7

To find b:
1=(4.3+b)mod26 --> b=-11mod26 = 15

Key: (a,b) = (3,15) --> Code is broken!!

Problem 2. What is multiplicative inverse of 8 in the rings $\mathbb{Z}_{12}$, $\mathbb{Z}_{13}$, and $\mathbb{Z}_{14}$.

Answer:

Ring Z12: gcd(12,8) is not 1, so (1/8) does not exist.

Ring Z13: gcd(13,8)=1, so (1/8) exists: (1/8).8 = 1 mod 13
Using trial and error between numbers 1 trough 7: 1/8=5

Ring Z14: gcd (14,8) is not 1, so (1/8) does not exist.

Problem 3. Compute x in the following without the use of a calculator:

(a) $x = 3^{100} mod\ 13$

Answer:

$$x = (3^4)^{25} mod13 = (3)^{25} mod13 = (3^4)^6 .3 mod13 = (3^6 .3) mod13$$
$$= (3^4 .3^3) mod13 = (3.1) mod13 = 3$$

(b) $13^x = 1\ mod\ 18$

Answer:

$13^1 mod18 = 13$
$13^2 mod18 = 169 mod18 = 7$
$13^3 mod18 = (13^2 \times 13) mod18 = (7 \times 13) mod18 = (91) mod18 = 1$
$13^4 mod18 = (13^3 \times 13) mod18 = (1 \times 13) mod18 = 13$
$13^5 mod18 = (13^4 \times 13) mod18 = (13 \times 13) mod18 = (169) mod18 = 7$
$13^6 mod18 = (13^5 \times 13) mod18 = (7 \times 13) mod18 = (91) mod18 = 1$
13,7, and 1 will repeat. The answer is x = 0,3,6,9,…

(c) $x = 7^{50} mod\ 19$

Answer:

$x = 7^{50} mod\ 19 = (7^2)^{25} mod\ 19 = 11^{25} mod\ 19 = (11^2)^{12}.11 mod\ 19$
$= 7^{12}.11 mod\ 19 = (7^2)^6.11 mod\ 19 = 11^6.11 mod\ 19$
$= (11^2)^3.11 mod\ 19 = 7^3.11 mod\ 19 = 7^2.7.11 mod\ 19$
$= 11.7.11 mod\ 19 = 7.7 mod\ 19 = 11$

Problem 4. Prove that double encryption with the affine cipher is only as secure as single encryption.

Answer:

$$C1 = (aP + b) mod 26$$
$$C2 = (aC1 + b) mod 26$$

P= Original Plaintext

We have to figure out how C2 is related directly to P.

$$C2 = (aC1 + b) mod 26 = \left[a\left((aP + b)\right) + b\right] mod 26$$
$$= (a.a.P + a.b + b) mod 26$$

With choosing of: $A = a.a\ ; B = a.b + b$

$$C2 = (A.P + B) mod 26$$

This will be another affine cipher with the key (A=a.a , B=a.b+b)

So it is as secure as only a single affine cipher.

Problem 5. Find the plaintext in the affine cipher with the key parameter **a = 7** and **b =22**: falszztysyjzyjkywjrztyjztyynaryjkyswarztyegyyj

Answer:

(1/a).7=1mod26 → 1/a=15

Decryption equation: P=[(1/a).(C-b)]mod26=[15.(C-22)]mod26

a: 15.(0-22)mod26=15.4mod26=8 →i

e: 15.(4-22)mod26=15.8mod26=16 →q

f: 15.(5-22)mod26=15.9mod26=5 →f

g: 15.(6-22)mod26=15.10mod26=20 →u

j: 15.(9-22)mod26=15.13mod26=13 →n

k: 15.(10-22)mod26=15.14mod26=2 →c

l: 15.(11-22)mod26=15.15mod26= 17→r

n: 15.(13-22)mod26=15.17mod26=21 →v

r: 15.(17-22)mod26=15.21mod26=3 →d

s: 15.(18-22)mod26=15.22mod26=18 →s

t: 15.(19-22)mod26=15.23mod26= 7→h

w: 15.(22-22)mod26=15.0mod26=0 →a

y: 15.(24-22)mod26=15.2mod26=4 →e

z: 15.(25-22)mod26=15.3mod26=19 →t

falszztysyjzyjkywjrztyjztyynaryjkyswarztyegyyj

first the sentence en…

Problem 6. The requirement for an encryption function **E** to be one-to-one is that for any two plaintext **p1 ≠ p2** and the key, **K**, then the **E**(**K**,**p1**) ≠ **E**(**K**,**p2**). Find and prove the condition for the affine cipher to be one-to-one.

Answer:

p1 ≠ p2 → E(**K**,**p1**) ≠ **E**(**K**,**p2**)

This is equivalent to:

E(**K**,**p1**) = **E**(**K**,**p2**) **→ p1 = p2**

So:

E(**K**,**p1**) = **E**(**K**,**p2**) **→ E**(**(a,b)**,**p1**) = **E**(**(a,b)**,**p2**) **→ (ap1+b)mod26 = (ap2+b)mod26 → a.(p1-p2)mod26=0**

In order to have this condition satisfied, **a** should be having multiplicative inverse:

There should be such (1/a) that (1/a).a = 1mod26

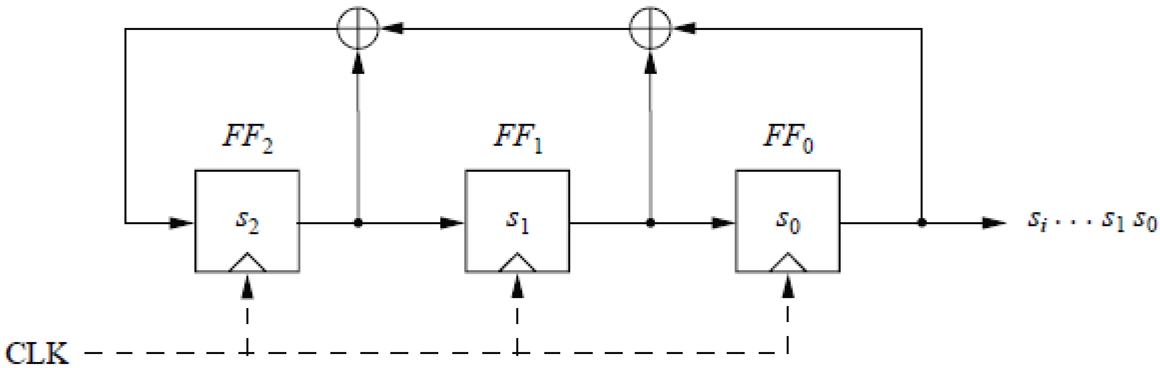
(1/a).a.(p1-p2)mod26 = 0

→ (p1-p2)mod26=0 → p1=p2

Condition is existence of (1/a) in mod 26:

gcd(26,a)=1 → **a={1,3,5,7,9,11,15,17,19,21,23,25}**

Problem 7. In the following LFSR:



(a) Find the sequence generated from initialization vector (S2=1, S1=0, S0=1). What is the period?

$$S3 = S2 \oplus (S1 \oplus S0)$$

In general form:

$$S_{i+3} = S_{i+2} \oplus (S_{i+1} \oplus S_i)$$

S3=0, S4= $S3 \oplus (S2 \oplus S1) = 0 \oplus (1 \oplus 0) = 1$, S5= $S4 \oplus (S3 \oplus S2) = 1 \oplus (0 \oplus 1) = 0$, S6= $S5 \oplus (S4 \oplus S3) = 0 \oplus (1 \oplus 0) = 1$,
S0,S1,S2,S3,S4,S5,S6,… = 1,0,1,0,1,0,…
Period = 2

(b) Find the sequence generated from initialization vector (S2=0, S1=1, S0=1). What is the period?

$$S3 = S2 \oplus (S1 \oplus S0)$$

In general form:

$$S_{i+3} = S_{i+2} \oplus (S_{i+1} \oplus S_i)$$

S3= $S2 \oplus (S1 \oplus S0) = 0$, S4= $S3 \oplus (S2 \oplus S1) = 0 \oplus (0 \oplus 1) = 1$, S5= $S4 \oplus (S3 \oplus S2) = 1 \oplus (0 \oplus 0) = 1$,
S6= $S5 \oplus (S4 \oplus S3) = 1 \oplus (1 \oplus 0) = 0$
S0,S1,S2,S3,S4,S5,S6,… = 1,1,0,0,1,1,0,…
Period = 4