Fall 2015 CIS 3362 Homework #2 Solutions (Both Groups)

1) Given that the encryption function for an affine cipher in a language with 65 alphabet characters is f(x) = (24x + 11) % 65, determine the corresponding decryption function. Please show all of your work.

Solution

Take the given equation and solve for x:

f(x)=(24x+11)%65
f(x)-11=24x%65
24x=(f(x)-11)%65

We must multiply both sides of the equation by 24^{-1} mod 65. Let's run the Extended Euclidean Algorithm to find this value:

65 = 2 x 24 + 17
24 = 1 x 17 + 7
17 = 2 x 7 + 3
7 = 2 x 3 + 1

7 - 2 x 3 = 1
7 - 2(17 - 2 x 7) = 1
7 - 2 x 17 + 4 x 7 = 1
5 x 7 - 2 x 17 = 1
5(24 - 17) - 2 x 17 = 1
5 x 24 - 5 x 17 - 2 x 17 = 1
5 x 24 - 7 x 17 = 1
5 x 24 - 7(65 - 2 x24) = 1
5 x 24 - 7 x 65 + 14 x 24 = 1
19 x 24 - 7 x 65 = 1
Thus, $24^{-1} \equiv 19 \bmod 65$

24x=(f(x)-11)%65
19(24x) = 19(f(x) - 11) % 65
x = (19f(x) - 209) % 65
x = (19f(x) + 51) % 65

Thus, the corresponding decryption function is $f^{-1}(x) = (19x + 51)$ % 65.

2) Encrypt the following message below using the affine cipher function, f(x) = (9x + 17) % 26.

PACKMYBOXWITHFIVEDOZENLIQUORJUGS

Solution

In order to encrypt for each alphabetic we should do following steps:

P=15 → f(15)=(9*15+17)%26=22 → ‘W’

A=0 → f(0)=(9*0+17)%26=9 → ‘R’, here are all of the letters, encrypted:

plaintext	values	(9x+17)%26	ciphertext
P	15	23	W
A	0	17	R
C	2	9	J
K	10	3	D
M	12	21	V
Y	24	25	Z
B	1	0	A
O	14	13	N
X	23	16	Q
W	22	7	H
I	8	11	L
T	19	6	G
H	7	2	C
F	5	10	K
I	8	11	L
V	21	24	Y
E	4	1	B
D	3	18	S
O	14	13	N
Z	25	8	I
E	4	1	B
L	11	4	E

N	13	12	M
I	8	11	L
Q	16	5	F
U	20	15	P
O	14	13	N
R	17	14	O
J	9	20	U
U	20	15	P
G	6	19	T
S	18	23	X

The corresponding ciphertext is:

WRJDVZANQHLGCKLYBSNIBEMLFPNOUPTX

3) Consider a language with an alphabet size of 165. How many possible affine cipher keys could there be for this language?

Solution

if f(x)=(ax+b)%165 then:
The “a’ ” only exist if “a” and 165 are coprime, or if their gcd=1 . So, this limits the amounts which “a” can accept. If their gcd is not equal to 1, then a single cipher letter will have multiple plain letters possible. 165 = 3 x 5 x 11, thus we must count the number of values from 1 to 165 that share a common factor with 11 or 15 and subtract that from 165. There are 165/3 = 55 multiples of 3, 165/5 = 33 multiples of 5 and 165/11 = 15 multiples of 11. But, of these, we are counting the following multiples twice: 15, 30, 45, 60, 75, 90, 105, 120, 135, 150, 33, 66, 99, 132, 55, 110. Finally, we had counted 165 three times. Thus our final count of values that share a common factor with 165 is 55 + 33+ 15 - 16 - 2 = 85. It follows that there are 80 integers that are relatively prime with 165 in the range [1, 165].

It follows that the number of possible keys for the affine cipher of an alphabet of this size is 165 x 80 = **13,200.**

4) You are attempting to break an affine cipher (in English). You believe that the ciphertext ‘G’ maps to the plaintext letter ‘e’ and that the ciphertext ‘P’ maps to the plaintext ‘t’. Determine the **decryption** function used based on these two pieces of information.

Solution

First, summarize information in the question as follows:

‘G’ → ‘e’ ⇒ 6 → 4

‘P’ → ‘t’ ⇒ 15 → 19

and we know that for decryption : $f^{-1}(x)=(ax+b)\%26$

So, we have following equations:
$6a+b=4 \%26$
$15a+b=19 \%26$

Subtracting, we get:
$9a = 15 \bmod 26$, multiply through by $9^{-1} = 3 \bmod 26$
$3(9a) = 3(15) \bmod 26$
$a \equiv 45 \equiv 19 \bmod 26$.

Using the first equation, we find $6(19) + b = 4 \bmod 26$, so $b = (4 - 114) \bmod 26$, thus, $b \equiv -110 \equiv 20 \bmod 26$.

Thus, the decryption function is $f^{-1}(x)=(19x+20)\%26$.

5) Let M =$\begin{pmatrix}8 & 17\\ 7 & 9\end{pmatrix}$. Determine M^{-1} , the corresponding decryption for the Hill cipher with an encryption key of M.

Solution

We can calculate inverse of M by following formula:

$$M^{-1}= \frac{1}{\det(M)} \times (adjoint\ of\ (M))$$

So, we have:

adjoint of (M)=$\begin{bmatrix}9 & -17\\ -7 & 8\end{bmatrix}$ mod(26)= $\begin{bmatrix}9 & 9\\ 19 & 8\end{bmatrix}$

det (M)=(9*19)-(8*9)=5

So:

M^{-1}= (5^{-1})* $\begin{bmatrix}\mathbf{9} & \mathbf{9}\\ \mathbf{19} & \mathbf{8}\end{bmatrix}$ mod(26)=21*$\begin{bmatrix}\mathbf{9} & \mathbf{9}\\ \mathbf{19} & \mathbf{8}\end{bmatrix}$ mod(26)= $\begin{bmatrix}\mathbf{189} & \mathbf{189}\\ \mathbf{399} & \mathbf{168}\end{bmatrix}$ mod(26)= $\begin{bmatrix}\mathbf{7} & \mathbf{7}\\ \mathbf{9} & \mathbf{12}\end{bmatrix}$

6) Encrypt the plain text "COMPUTERS" with the Hill cipher using the encryption key $\begin{pmatrix}4 & 1 & 3\\ 5 & 9 & 7\\ 15 & 1 & 2\end{pmatrix}$

Solution

To encrypt this message, we need to break the message into chunks of 3 (because size of encryption matrix is 3*3). So, we have:

COM PUT ERS

2-14-12 15-20-19 4-17-18

“COM”= $\begin{pmatrix}2\\ 14\\ 12\end{pmatrix}$

“COM”=$\begin{pmatrix}4 & 1 & 3\\ 5 & 9 & 7\\ 15 & 1 & 2\end{pmatrix}\times\begin{pmatrix}2\\ 14\\ 12\end{pmatrix}= \begin{pmatrix}58\\ 220\\ 68\end{pmatrix}$ mod(26)= $\begin{pmatrix}6\\ 12\\ 16\end{pmatrix}$= “GMQ”

“PUT”= $\begin{pmatrix}15\\ 20\\ 19\end{pmatrix}$

“PUT”=$\begin{pmatrix}4 & 1 & 3\\ 5 & 9 & 7\\ 15 & 1 & 2\end{pmatrix}\times\begin{pmatrix}15\\ 20\\ 19\end{pmatrix}= \begin{pmatrix}137\\ 388\\ 283\end{pmatrix}$ mod(26)= $\begin{pmatrix}7\\ 24\\ 23\end{pmatrix}$= “HYX”

“ERS”= $\begin{pmatrix}4\\ 17\\ 18\end{pmatrix}$

“ERS”=$\begin{pmatrix}4 & 1 & 3\\ 5 & 9 & 7\\ 15 & 1 & 2\end{pmatrix}\times\begin{pmatrix}4\\ 17\\ 18\end{pmatrix}= \begin{pmatrix}87\\ 299\\ 113\end{pmatrix}$ mod(26)= $\begin{pmatrix}9\\ 13\\ 9\end{pmatrix}$= “JNJ”

Finally, the encrypted message is “GMQHYXJNJ”

7) What is the index of coincidence of the following set of letters: 15 As, 45 Bs, 40 Cs, 60 Ds, 40 Es? For full credit, please express your answer as a **fraction in lowest terms.**

Solution

$$IC = \frac{15 \times 14 + 45 \times 44 + 40 \times 39 + 60 \times 59 + 40 \times 39}{200 \times 199} = \frac{8850}{39800} = \frac{\mathbf{177}}{\mathbf{796}}$$

8) The following ciphertext was encrypted using the Vigenere cipher with the keyword "FORK": GFVKPTRCYTFYI. What was the original plaintext?

Solution

For decrypting this message with should use Vigenere Table. First, the keyword must repeat as follows:
GFVKPTRCYTFYI
FORKFORKFORKF

To decrypt, we pick a letter in the ciphertext and its corresponding letter in the keyword, use the keyword letter to find the corresponding row, and the letter heading of the column that contains the ciphertext letter is the needed plaintext letter.

So, the original plaintext was: “BREAKFASTFOOD”

9) Using the Extended Euclidean Algorithm determines 80^{-1} mod 153. Please answer with an integer in between 0 and 152, inclusive.

Solution

153 = 1 x 80 + 73
80 = 1 x 73 + 7
73 = 10 x 7 + 3
7 = 2 x 3 + 1

7 - 2 x 3 = 1
7 - 2(73 - 10 x 7) = 1
7 - 2 x 73 + 20 x 7 = 1
21 x 7 - 2 x 73 = 1
21(80 - 73) - 2 x 73 = 1
21 x 80 - 21 x 73 - 2 x 73 = 1
21 x 80 - 23 x 73 = 1
21 x 80 - 23(153 - 80) = 1
21 x 80 - 23 x 153 + 23 x 80 = 1
44 x 80 - 23 x 153 = 1

Thus, $80^{-1} \equiv 44$ mod 153.

10) Encrypt the message "90210WASMYFAVORITESHOW" using the ADVGFX cipher with the square shown below and the keyword "PRIESTLY".

	A	D	F	G	V	X
A	K	Q	C	7	U	G
D	V	D	1 (# one)	N	M	0
F	J	P	5	6	F	Z
G	9	R	B	T	3	H
V	E	I (letter I)	W	2	X	4
X	L (letter L)	S	8	O (letter O)	Y	A

Solution

First, we find each letter of message in table and substitute it with letters in far left side on the same row, followed by the letter at the top in the same column. So, we will have:
“GA DX VG DF DX VF XX XD DV XV FV XX DA XG GD VD GG VA XD GX XG VF”

Then:

P	**R**	**I**	**E**	**S**	**T**	**L**	**Y**
G	A	D	X	V	G	D	F
D	X	V	F	X	X	X	D
D	V	X	V	F	V	X	X
D	Z	X	G	G	D	V	D
G	G	V	A	X	D	G	X
X	G	V	F				

Next, Perform a columnar transposition. Sort the code word alphabetically:

E	**I**	**L**	**P**	**R**	**S**	**T**	**Y**
X	D	D	G	A	V	G	F
F	V	X	D	X	X	X	D
V	X	X	D	V	F	V	X
G	X	V	D	Z	G	D	D
A	V	G	G	G	X	D	X
F	V		X	G			

Finally, the encrypted message is:
“XFVGAFDVXXVVDXXVGGDDDGXAXVZGGVXFGXGXVDDFDXDX”

11) The following ciphertext was created using the Playfair cipher with the keyword “KNIGHTS” and the padding character X. What is the corresponding plaintext? (Note: The ciphertext is broken up into digraphs for convenience.)

```
NM LY GA FE FJ BQ PK WL AS LP FT ZY
```

Answer:

The key is as follows:

K	N	I	G	H
T	S	A	B	C
D	E	F	L	M
O	P	Q	R	U
V	W	X	Y	Z

Next, we use the rules of Playfair cipher (in backward) to get original plaintext.

Cipher text	Plain text
NM	HE
LY	BR
GA	IB
FE	ED
FJ	AX
BQ	AR
PK	ON
WL	YE
AS	ST
LP	ER
FT	DA
ZY	YX

So, the plaintext was:
“HE BR IB ED AX AR ON YE ST ER DA YX”
or: “HE BRIBED AARON YESTERDAY”