EECE 632 – Cryptography and Computer Security

Homework #1 – Solution

CHAPTER 2

Exercise #1

A generalization of the *Caesar Cipher* is the *Affine Cipher* given by: $C = (a.P + b) \bmod 26$, Where P is the plain character and C is the cipher character after encryption, a and b are coefficients. The decryption of the Affine Cipher is given by: $P = a^{-1}(C - b) \bmod 26$, where a^{-1} is the inverse of $a \bmod 26$. Note that characters are assigned values of $A=0$ and $Z=25$.

a) Encrypt "HI" using the *Affine Cipher* with $a = 11$ and $b = 5$.
b) The cipher "ME" was obtained after *Affine* encryption with $a = 11$ and $b = 5$. Decrypt it.

a) $P = HI \Rightarrow P_1 = 7$ (H) and $P_2 = 8$ (I)
$C_1 = (a.P_1 + b) \bmod 26 = (11x7 + 5) \bmod 26 = 82 \bmod 26 = 4 = E$
$C_2 = (a.P_2 + b) \bmod 26 = (11x8 + 5) \bmod 26 = 93 \bmod 26 = 15 = P$
$\Rightarrow$ **C = EP** **10 POINTS**

b) $C = ME \Rightarrow C_1 = 12$ (M) and $C_2 = 4$ (E)
By inspection: $a^{-1} = 19$
Check: $axa^{-1} \bmod 26 = 11x19 \bmod 26 = 209 \bmod 26 = 1$ ✓
$P_1 = a^{-1}(C_1 - b) \bmod 26 = 19(12 - 5) \bmod 26 = 3 = D$
$P_2 = a^{-1}(C_2 - b) \bmod 26 = 19(4 - 5) \bmod 26 = 7 = H$
$\Rightarrow$ **P = DH** **10 POINTS**

Exercise #2

We know that the most frequent letters of the English alphabet are *E* and *T*. After doing *Affine* encryption to a plaintext, the most frequent letters became *J* and *k*. Break the code by finding the values of *a* and *b*.

E = 4 becomes J = 9
T = 19 becomes K = 10
$C = (a.P + b) \bmod 26$
$\Rightarrow 9 = (4a + b) \bmod 26$ eq. 1
& $10 = (19a + b) \bmod 26$ eq. 2
Subtract eq. 1 from eq. 2 to remove b: $1 = (15a) \bmod 26$
By inspection: **a = 7** **10 POINTS**
Check: $15x7 \bmod 26 = 105 \bmod 26 = 1$✓
Get b from eq. 1: $9 = (4x7 + b) \bmod 26$
By inspection: **b = 7** **10 POINTS**
Check: $(4x7 + 7) \bmod 26 = 35 \bmod 26 = 9$ ✓

Exercise #3

Use *Playfair* code to encrypt the message "HELLOS" using the keyword "homework".

The matrix is: **10 POINTS**

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

HE LX LO SX
HE becomes OW
LX becomes GZ
LO becomes FW
SX becomes QY
C = OWGZFWQY **10 POINTS**

Exercise #4

Using *Vigenere* cipher, encrypt the word "assignment" using the key "cryptology".

Key	c	r	y	p	t	o	l	o	g	y
Plain	a	s	s	I	g	n	m	e	n	t
Cipher	**c**	**j**	**q**	**x**	**z**	**b**	**x**	**s**	**t**	**r**

10 POINTS

Exercise #5

Use the *Hill Cipher* with key $K = \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}$ in order to encrypt "DOGS". Use the same cipher to decrypt "PLAN".

a) D = 3
O = 14
G = 6
S = 18

$C_1 = K.P_1 \bmod 26 = \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}\begin{bmatrix} 3 \\ 14 \end{bmatrix} = \begin{bmatrix} 127 \\ 93 \end{bmatrix} \bmod 26 = \begin{bmatrix} 23 \\ 15 \end{bmatrix} = \begin{matrix} X \\ P \end{matrix}$

$C_2 = K.P_2 \bmod 26 = \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}\begin{bmatrix} 6 \\ 18 \end{bmatrix} = \begin{bmatrix} 174 \\ 156 \end{bmatrix} \bmod 26 = \begin{bmatrix} 18 \\ 0 \end{bmatrix} = \begin{matrix} S \\ A \end{matrix}$

$\Rightarrow$ **C = XPSA** **10 POINTS**

b) P = 15
L = 11
A = 0
N = 13

$K = \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}$

$Det(K) = 5x3 - 8x17 \bmod 26 = -121 \bmod 26 = 9$

By inspection: $9^{-1} = 3$

Check: $3x9 \bmod 26 = 27 \bmod 26 = 1$ ✓

$\Rightarrow K^{-1} = 3\begin{bmatrix} 3 & -8 \\ -17 & 5 \end{bmatrix} \bmod 26 = \begin{bmatrix} 9 & -24 \\ -51 & 15 \end{bmatrix} \bmod 26 = \begin{bmatrix} \mathbf{9} & \mathbf{2} \\ \mathbf{1} & \mathbf{15} \end{bmatrix}$ **10 POINTS**

$P_1 = K^{-1}C_1 \bmod 26 = \begin{bmatrix} 9 & 2 \\ 1 & 15 \end{bmatrix}\begin{bmatrix} 15 \\ 11 \end{bmatrix} = \begin{bmatrix} 157 \\ 180 \end{bmatrix} \bmod 26 = \begin{bmatrix} 1 \\ 24 \end{bmatrix} = \begin{matrix} B \\ Y \end{matrix}$

$P_2 = K^{-1}C_2 \bmod 26 = \begin{bmatrix} 9 & 2 \\ 1 & 15 \end{bmatrix}\begin{bmatrix} 0 \\ 13 \end{bmatrix} = \begin{bmatrix} 26 \\ 195 \end{bmatrix} \bmod 26 = \begin{bmatrix} 0 \\ 13 \end{bmatrix} = \begin{matrix} A \\ N \end{matrix}$

$\Rightarrow$ **P = BYAN** **10 POINTS**