UNIVERSITY OF BUEA

FACULTY OF ENGINNEERING AND TECHNOLOGY

DEPARTMENT OF COMPUTER ENGINEERING

LEVEL 300

CEF350 - Security and Cryptosystems  
Answers to Exercise sheet

**Group ?:**

**Group members:**

ASHU REIZIGER ACHUO FE17A002

DOMOU NAMOU BRICE FE17A018

EBAI JENNILINE AGBOR FE17A021

KATE EVELYNE MBEMOH FE17A029

MBINO RUTH ATEM FE17A041

LOBE NYOH SERGE FE17A035

DURRELL GEMUH FE17A019

MBENG TANYI TANYI FE17A040

KOLLE HARVEY NGOE FE17A032

Course Instructor: **Mme Tsague Aline 26/06/2019**

**Exercise 1:**

Knowing that the Ceaser cypher encrypts a text by shifting each letter a particular number of times (corresponding to the key) to the right of the alphabet, to decrypt we will be shifting to the left.

In order to do this, we must first of all determine the key.

Knowing that the letter ‘**e**’ is the most common and occurring letter of the alphabet, we look at the letter with highest occurrence in the ciphertext and compute its difference with letter **e** in the alphabet.

Ciphertext: **Sodlqwhaw wr eh hqfubswhg**

Two must occurring letters are **w** and **h.**

Trying w, we have a key of 18 and the corresponding plaintext looks a lot more like another ciphertext.

Working with h, we have a key of 3 and the corresponding plaintext becomes **Plaintext to be encrypted** which sounds a lot more like a plaintext.

Ci = E(K, E(K, Mi));

K= 13

Knowing that the Ceaser cipher shifts letters of the alphabets a certain number of times to the left or right depending on the process and knowing that our key is 13 we come up with the following propositions;

E(K, Mi) encrypts the text Mi by shifting the letters 13 times forward in the alphabet. Lets say the result of this operation is C1.

Ci = E(K, C1) encrypts the encrypted text C1 by shifting the letters 13 places forward and knowing that we have just 26 letters this process takes us back to the original text Mi.

So therefore, Ci = E(K, E(K,Mi)) = Mi.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Operation | Output | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| E(K, Mi) | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| E(K, E(K,Mi)) | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

Number of encryptions with key = 2 to have the same effect as above is 13. This is because the relationship between the number of times and the key is inversely proportional.

Knowing that with a key of 13, the number of times to get this effect is 2. Therefore, our constant of proportionality is 13\*2 = 26.

So therefore number of times with a key of 2 = 26/2 = 13.

**Exercise 2:**

KNXMNSLKWJXMBFY JWGJSIXFIRNY XB  
TWIKNXMWFSITAJWMJQRNSLFSDIFD

(I haven’t gotten any key that the decrypted message makes sense in English, the only one good enough is 5)

XTHQTXJSTRFY Y JWMTBKFW  
ynyqj

(I can’t seem to find a key here)

**Exercise 3:**

* Vigenere method:

Plaintext = Supplieswillarrivetonight

Length = 25

Key = order

Length = 5

Repeating the word order 5 times to meet up the length of the plaintext gives

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *S* | *U* | *P* | *P* | *L* | *I* | *E* | *S* | *W* | *I* | *L* | *L* | *A* | *R* | *R* | *I* | *V* | *E* | *T* | *O* | *N* | *I* | *G* | *H* | *T* |
| *O* | *R* | *D* | *E* | *R* | *O* | *R* | *D* | *E* | *R* | *O* | *R* | *D* | *E* | *R* | *O* | *R* | *D* | *E* | *R* | *O* | *R* | *D* | *E* | *R* |

Table1

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

Table 2

Comparing corresponding entries of table 1 and noting their point of intersection on table 2 we have our ciphertext to be **Glstcwvvazzcdviwmhxfbzjlk**

* Columnar Transposition method

Key = (5, f)

i = 1 2 3 4 5

f(i) = 4 1 2 5 3

Grouping the plaintext into groups of five gives

Suppl ieswi llarr iveto night

Using the function f(i) we have our ciphertext to be

Psulp wieis rllra tivoe hnitg

Therefore, cyphertext is **Psulpwieisrllrativoehnitg**

* Periodic permutation

Key = (4, f)

i = 1 2 3 4

f(i) = 4 1 2 3

Grouping the plaintext into groups of four gives

Supp lies will arri veto nigh t

Using the function f(i) we have our ciphertext to be

Psup slie lwil iarr ovet hnig t

Therefore, cyphertext is **Psupslielwiliarrovethnigt**

**2.** The Virgenre cipher consist of many different alphabets **polyalphabetic** while the Ceaser cipher is **monoalphabetic**

**Exercise 4:**

Plaintext space X = *{* 0*, … ,* 25 *}*.

Ciphertext space Y = *{* 0*, … ,* 25 *}*.

Key space K = *{* 0*, … ,* 25 *}*.

Encryption function is defined by: E(X; K) = (X + K) mod n

* Decryption key is **D(Y; K) = (Y - K)mod n**
* The table below shows letters of the alphabet and their corresponding keys.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Table1

If we use “**HELLO”** as Key **“K**” it implies key-Lenght=5

Hence from the table1 above, **K=7-4-11-11-14**

Plaintext= **Mr President; I am delighted to accept your offer**.

Ignoring the space, period and comma signs, we get:

Plaintext= MRPRESIDENTIAMDELIGHTEDTOACCEPTYOUROFFER

Length = 40

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **M** | **R** | **P** | **R** | **E** | **S** | **I** | **D** | **E** | **N** | **T** | **I** | **A** | **M** | **D** | **E** | **L** | **I** | **G** | **H** | **T** | **E** | **D** | **T** | **O** | **A** | **C** | **C** | **E** | **P** | **T** | **Y** | **O** | **U** | **R** | **O** | **F** | **F** | **E** | **R** |
| **X** | 12 | 17 | 15 | 17 | 4 | 18 | 8 | 3 | 4 | 13 | 19 | 8 | 0 | 12 | 3 | 4 | 11 | 8 | 6 | 7 | 19 | 4 | 3 | 19 | 14 | 0 | 2 | 2 | 4 | 15 | 19 | 24 | 14 | 20 | 17 | 14 | 5 | 5 | 4 | 17 |
|  | **H** | **E** | **L** | **L** | **O** | **H** | **E** | **L** | **L** | **O** | **H** | **E** | **L** | **L** | **O** | **H** | **E** | **L** | **L** | **O** | **H** | **E** | **L** | **L** | **O** | **H** | **E** | **L** | **L** | **O** | **H** | **E** | **L** | **L** | **O** | **H** | **E** | **L** | **L** | **O** |
| **K** | 7 | 4 | 11 | 11 | 14 | 7 | 4 | 11 | 11 | 14 | 7 | 4 | 11 | 11 | 14 | 7 | 4 | 11 | 11 | 14 | 7 | 4 | 11 | 11 | 14 | 7 | 4 | 11 | 11 | 14 | 7 | 4 | 11 | 11 | 14 | 7 | 4 | 11 | 11 | 14 |
| **E** | 19 | 21 | 0 | 2 | 18 | 25 | 12 | 14 | 15 | 1 | 0 | 12 | 11 | 23 | 17 | 11 | 15 | 19 | 17 | 21 | 0 | 8 | 14 | 4 | 2 | 7 | 6 | 13 | 15 | 3 | 0 | 2 | 25 | 5 | 5 | 21 | 9 | 16 | 15 | 5 |
| **C** | **T** | **V** | **A** | **C** | **S** | **Z** | **M** | **O** | **P** | **B** | **A** | **M** | **L** | **X** | **R** | **L** | **P** | **T** | **R** | **V** | **A** | **I** | **O** | **E** | **C** | **H** | **G** | **N** | **P** | **D** | **A** | **C** | **Z** | **F** | **F** | **V** | **J** | **Q** | **P** | **F** |

Where **E=(x+k)mod26**

And C=Cyphertext

Cyphertext=**TVACS ZMOPB AMLXR LPTRV AIOEC HGNPD ACZFF VJQPF**

**Exercise5:**

Cyphertext= **asvphgyt**

The encryption rule is given as C = (M + K) mod 26, where C is the ciphertext, M is the  
plaintext and K is the key.

*Assumptions:*

* The plaintext is in English
* The first plaintext letter is W i.e a(K)= W

.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Table1

Since the encryption rule is C=(M +K )mod 26 decryption rule M=(C - K)mod26

Therefore:

Since a in the cypher text is w in the plaintext, it implies

a = (w + k)mod26

0 = (22 + k)mod26

Implies k = 4 since (22+4)mod26 = 0 (ie 26mod26=0)

Therefore our decryption function becomes M = (C-K)mod26

M = (C - 4)mod26

Operating this rule on each ciphertext letter we have

a = (0-4)mod26 = 22 (and the 22nd alphabet is w)

s = (18-4)mod26 = 14 (and the 14th alphabet is o)

v = (21-4)mod26 = 17 (and the 17th alphabet is r)

p = (15-4)mod26 = 11 (and the 11th alphabet is l)

h = (7-4)mod26 = 3 (and the 3rd alphabet is d)

g = (6-4)mod26 = 2 (and the 2nd alphabet is c)

y = (24-4)mod26 = 20 (and the 20th alphabet is u)

t = (19-4)mod26 = 15 (and the 15th alphabet is p)

With reference to Table 1,it shows that the Cyphertext **asvphgyt** is **worldcup** in plaintext.

**Exercise6:**

Assume that PuK = (143,11)

n= 143 e=11, n=pq

e: gcd(e, $) =1

$ = (p-1)\*(q-1) where p and q are odd prime numbers ed=1mod$

Let p= 11 and q = 13

We have $= (11-1)(13-10 = 10\*12 = 120 d:ed=1mod$ d:$ divides ed-1

Therefore $=120 divides 11d-1

If d= 11 we get 11d-1 =120 and 120 also divides 120

Private key PrK = (n,d) = (143, 11)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| C1 | C2 | C3 | C4 | C5 | C6 |
| 111 | 4 | 88 | 57 | 116 | 67 |

M1 = C1dmod n , 11111mod143=30

M2 = C2dmod n , 411mod143=114

M3= C3dmod n , 8811mod143=103

M4 = C4dmod n , 5711mod143=64

M5= C5dmod n , 11611mod143=83

M6 = C6dmod n , 6711mod143=78

Therefore M= **R3 r g @ S N**

**Exercise7:**

* If N =pq =55=n

Where p and Q are odd prime numbers say p=5 and q=11

If EA=3 and EB=7 and m=13

CA=MEA mod n CB=MEB mod n

CA=133mod 55 =**52**

CB=137mod 55 = **7**

* d : ed = 1mod $(n)

$(n) = (p-1)(q-1) = (7)(10) = 40

e: gcd(e,$)=1 d=1/e mod $(n) d: $ divides ed=1

DA: 40 diviides EADA-1 40 divides 3DA-1

Simply testing; DA=1,2,---

If d =27 which gives 3(27)-1=80

40 divides 80 DA=27

If DB= 23,, EBDB-1=7(23)-1 =160 also 40 divides 160

Private key= PRK = (n, d)

Public Key = PUK = (n, e)

PRKA= (n, dA) = (55,27)

PRKB= (n,dB) = (55,23)

* M = edmod n