16-124-836
Marcel Matti ZAUDER

2.3 Question 3

2.3.A Can you find the encryption algorithm? Is it secure? Why?

CIPHERTEXT: SIDKHKDM AF HCRKIABIE SHIMC KD LFEAILA
TEXT USED FOR ENCRYPTION: The snow lay thick on the steps and the snowflakes driven by the wind looked back in the headlights of the cars

As the task description was very ambiguous and very unclear/incomplete, I googled and found out that the text can be used for coding the alphabet as follows (reference Chegg-Website[1]):

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
t	h	e	s	n	o	w	l	a	y	i	c	k	p	d	f	r	v	b	g

Therefore the decryption of the CIPHERTEXT would be:
PLAINTEXT: basilisk to leviathan blake is contact

On first sight this encryption does look very secure, however as we have a 1-to-1 correspondence of each letter an analysis can be made for large texts on the frequency of each letter and therefore the letter with the most occurences can be mapped to the letter 'e', the second most-often letter to 't' and so on. For smaller texts like this example it might be already sufficient enough but not the very best method to encrypt something.
For this particular encryption scheme there are also "only":

$$26! = 403.291.461.126.605.635.584.000.000 < 2^{89}$$

different possible keys.

2.3.B Encryption with Playfair matrix

PLAYFAIR MATRIX:

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

PLAINTEXT: I only regret that I have but one life to give for my country
CLEANED PLAINTEXT[2]: IONLYREGRETXTHATIHAVEBUTONELIFETOGIVEFORMYCOUNTRYX
CIPHERTEXT: MAPAZOQHGKHWHMLITMIAKHPBASDGMCDHROCAFKRAFOFANPBLZY

2.3.C Encryption with Viginere Cipher

PLAINTEXT: cryptographic
(3-LETTER) KEY: wutwutwutwutw
CIPHERTEXT: ylrlnhcltlbby

[1] https://www.chegg.com/homework-help/cryptography-and-network-security-7th-edition-chapter-3-problem-5p-solution-9780134444635
[2] As we would have an odd amount of letters an "X" is appended at the end