Birzeit University

Faculty of Engineering and Technology

Department of Electrical and Computer Engineering

First Semester – 2023/2024

ENCS4320 - Applied Cryptography

Homework # 1 - Due Saturday, December 09, 2023

Section A	**THIS SECTION CONSISTS OF SIX QUESTIONS. YOU MUST ANSWER ALL THE QUESTIONS IN THIS SECTION.**

Question 1 (8 points):

Using your cryptanalysis skills, find the *plaintext* (and the *key*) that corresponds to the ciphertext ***IURPWKHULYHUWRWKHVHSDOHVWLQHZLOOEHIUHH***, given that the *shift cipher (ROT-k)* was used (You should clearly show steps about how you get the answer.)

Question 2 (6 points):

Suppose we have a computer with a 4.2 GHz 16-core processor that executes 4.2×10^9 cycles per second per core. Considering that it can test a key per CPU cycle:

a) What is the expected time (in years) to find a key by the brute-force attack if the key size is **56** bits?

b) What is the expected time (in years) to find a key by the brute-force attack if the key size is **128** bits?

Question 3 (8 points):

Alice is using the one-time pad and notices that when her key is all-zeroes $K = 0^n$, then $\mathrm{Enc}(K, M) = M$ and her message is sent in the clear! To avoid this problem, she decides to modify the scheme to exclude the all-zeroes key. That is, the key is now chosen uniformly from $\{0,1\}^n \setminus \{0^n\}$, the set of all n-bit strings except 0^n. In this way, she guarantees that her plaintext is never sent in the clear. Is this variant still one-time perfectly secure? Justify your answer.

Question 4 (18 points):

Compute the following without the use of a calculator (Please show all steps clearly. Solutions that show all the steps with a clear explanation will be given the highest rating):

a) $23 + 28 \pmod{29}$
b) $3 - 11 \pmod{9}$
c) $15 \times 29 \pmod{13}$
d) $16 \times 13 \pmod{26}$
e) $2^5 \pmod{31}$
f) $2^{103} \pmod{31}$

Question 5 (7 points):

Using the letter encodings in the table below, the ciphertext message "***KITLKE***" was encrypted with a one-time pad:

e	h	i	k	l	r	s	t
000	001	010	011	100	101	110	111

a) What is the key if the plaintext is "***thirst***"?
b) What is the key if the plaintext is "***hikers***"?

Question 6 (17 points):

Alice shares a stream of random bits with Bob, and she encrypts a message of length n for Bob by XORing the next n bits of this stream with the message. Bob decrypts by XORing the cyphertext with the same n bits from the stream of random bits.

a) Does this scheme work if we replace XOR with OR? How about with AND?
b) Suppose you want to encrypt a message $M \in \{0, 1, 2\}$ using a shared random key $K \in \{0, 1, 2\}$. Suppose you do this by representing K and M using two bits $(00, 01, \text{or } 10)$, and then XORing the two representations. Does this scheme have the same security guarantees as the one-time pad? Explain.
c) Give an alternate encryption algorithm for carrying out the above task that does provide a strong security guarantee. Note: You must not change the message space $\{0, 1, 2\}$ or the key space $\{0, 1, 2\}$. Instead, we want you to design an encryption algorithm $E(\cdot, \cdot)$ so that $E(K, M)$ is a secure encryption of M, when K and M are distributed as above.

Section B **YOU MUST ANSWER TWO QUESTIONS FROM THIS SECTION. ANSWER ALL THE PARTS FOR THE TWO QUESTIONS YOU CHOOSE.**

Question 7 (18 points):

Show that the shift, substitution, and Vigenère ciphers are all trivial to break using a chosen-plaintext attack. How much chosen plaintext is needed to recover the key for each of the ciphers?

Question 8 (18 points):

Assume an attacker knows that a user's password is either "***abcd***" or "***bedg***". Say the user encrypts his password using:

a) The Vigenère cipher using period 2,
b) The Vigenère cipher using period 3, and
c) The Vigenère cipher using period 4

and the attacker sees the resulting ciphertext. Show how the attacker can determine the user's password, or explain why this is not possible.

Question 9 (18 points):

The following questions concern multiple encryptions of single-character ASCII plaintexts with the one-time pad using the same 8-bit key. You may assume that the plaintexts are either (upper-case or lower-case) English letters or space character. Note that the ASCII code for the space character is 20 (hex) = 0010 0000 (binary), the ASCII code for 'A' is 41 (hex) = 0100 0001 (binary), and the ASCII code for 'a' is 61 (hex) = 0110 0001 (binary), as it is clear from the table below.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	space	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
6	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	DEL

a) Say you see the ciphertexts **3D** (hex) and **44** (hex). What can you deduce about the plaintext characters these correspond to?
b) Say you see the three ciphertexts **FF** (hex), **B5** (hex), and **C7** (hex). What can you deduce about the plaintext characters these correspond to?

Section C	**EXTRA CREDIT, THE FOLLOWING QUESTION IS A BONUS.**

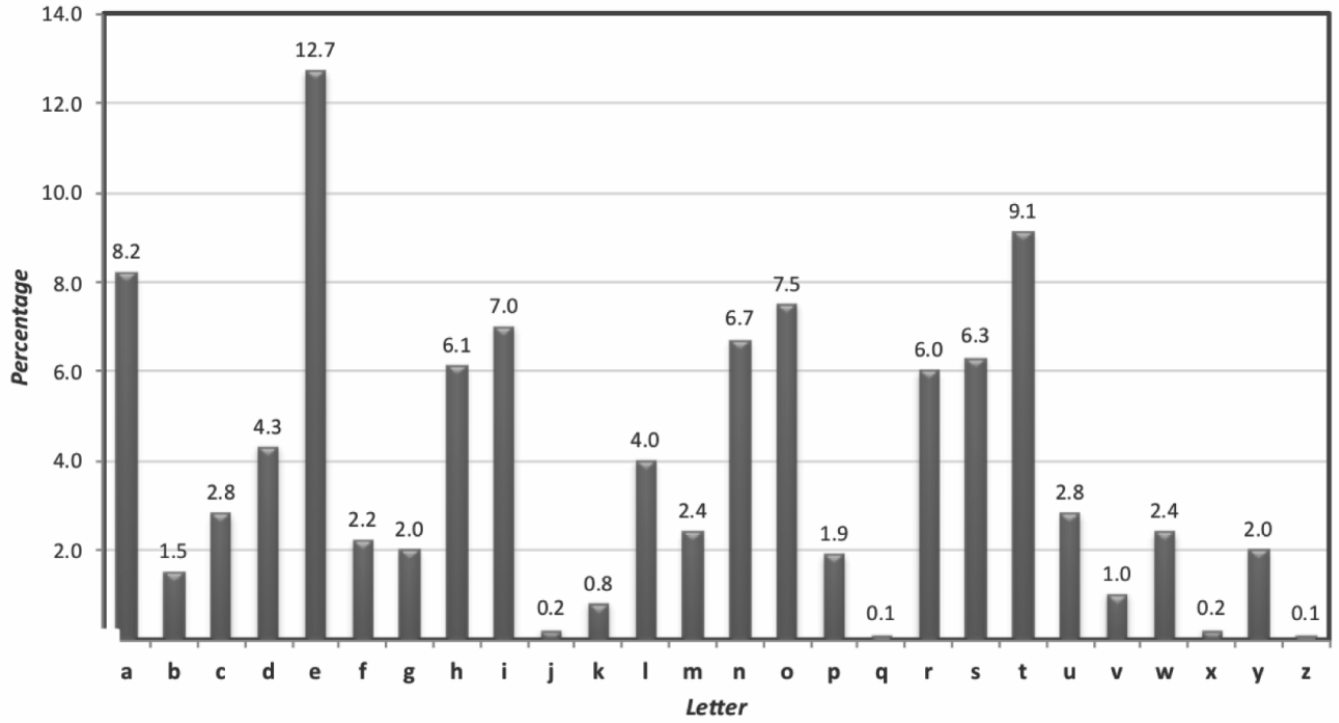
Question 10 (8 points):

Decrypt the ciphertext below given that the encryption scheme used is the mono-alphabetic substitution cipher with a secret key *K*.

JGRMQOYGHMVBJWRWQFPWHGFFDQGFPFZRKBEEBJIZQQOCIBZKLFAFGQVFZFWWE
OGWOPFGFHWOLPHLRLOLFDMFGQWBLWBWQOLKFWBYLBLYLFSFLJGRMQBOLWJVFP
FWQVHQWFFPQOQVFPQOCFPOGFWFJIGFQVHLHLROQVFGWJVFPFOLFHGQVQVFILE
OGQILHQFQGIQVVOSFAFGBWQVHQWIJVWJVFPFWHGFIWIHZZRQGBABHZQOCGFHX

Please provide your code that outputs the **key** used as well as the **plaintext**. You can use any programming language you prefer.

Hint: Design your method so that it determines the statistics of the English text, and then calculates the probability that the ciphertext comes from the same distribution. The figure below shows the frequencies of letters, as they occur in the English language.



GOOD LUCK