Birzeit University
Faculty of Engineering and Technology
Department of Electrical and Computer Engineering
First Semester – 2024/2025
ENCS4320 - Applied Cryptography
Homework # 1 - Due Monday, Dec 16, 2024

Question 1 (10 points):

Using your cryptanalysis skills, find the *plaintext* (and the *key*) that corresponds to the ciphertext ***WLIMWXLIWSYPSJQCWSYP***, given that the ***shift cipher (ROT-k)*** was used.

Question 2 (15 points):

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

a) The substitution cipher,
b) The Vigenère cipher using period 2, or
c) The Vigenère cipher using period 3

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 3 (10 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 4 (10 points):

Alice is using the one-time pad and notices that when her key is all-zeroes $K = 0^n$, then $\text{Enc}(K, M) = M$ 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 5 (15 points):

Answer each of the following without using a calculator.

a) $3 - 11 \pmod 9 =$

b) $15 \times 29 \pmod{13} =$

c) $-12\,/\,35 \pmod{19} =$

d) Are 172 and 68 co-prime numbers?

Question 6 (20 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?

Question 7 (10 points):

Suppose that, after a particular step of ***A5/1 stream cipher***, the values in the registers are:

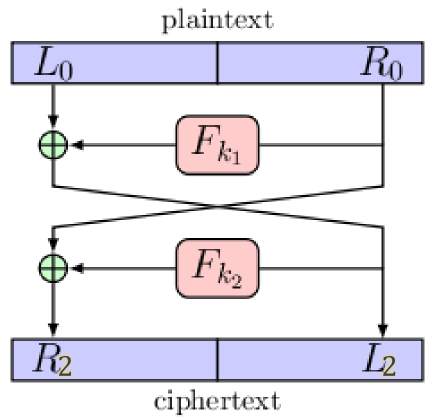
$$\boldsymbol{X = (x_0, x_1, \dots, x_{18}) = (1010101010101010110)}$$
$$\boldsymbol{Y = (y_0, y_1, \dots, y_{21}) = (1100110001101100010011)}$$
$$\boldsymbol{Z = (z_0, z_1, \dots, z_{22}) = (11100101110000011000011)}$$

a) List the next 4 keystream bits.

b) Give the contents of X, Y, and Z after the generation of each of these 4 bits.

Question 8 (15 points):

Consider a new ***block cipher***, **DES2**, that consists of only *two rounds* of the **DES** block cipher. **DES2** has the *same block and key size* as DES. For this question, you should consider the DES ***F*** function as a black box that takes two inputs, a 32-bit data segment, and a 48-bit round key, and produces a 32-bit output. Using the chosen-plaintext attack (CPA) without any restrictions on the number of oracle calls.



a) Give an algorithm to recover the 48-bit round keys for round 1 ($\boldsymbol{k_1}$) and round 2 ($\boldsymbol{k_2}$). Your algorithm should have fewer operations than the exhaustive key search for **DES2**.

b) Can your algorithm be converted into a distinguishing attack against **DES2**, i.e., an attack that distinguishes **DES2** from a random permutation?

Question 9 (20 points):

This problem deals with the ***AES-128 block cipher***.

a) Assume that the first column of the input to the InvMixColumn step is $S_{i,0}$ = (B4, 52, E0, AE)$_{16}$, find the 3rd element of the corresponding column of the output state of the InvMixColumn step.

b) Given the input $S_{2,1}$ = (7A)$_{16}$, find InvSubByte($S_{2,1}$).

c) Assume that round key 6 ($\boldsymbol{k_6}$) is (98 0F 71 AF 15 C9 47 D9 0C B7 E8 59 D6 7F 67 AD)$_{16}$, find the round keys for round 5 ($\boldsymbol{k_5}$) and round 7 ($\boldsymbol{k_7}$).

Question 10 (25 points):

This question requires you to explore and evaluate the key cryptographic properties of substitution boxes (S-Boxes) used in symmetric-key cryptography. Focus on the following properties: (1) Bijection, (2) Nonlinearity, (3) Strict Avalanche Criterion (SAC), and (4) Output Bits Independence Criterion (BIC). Start by selecting a peer-reviewed research paper that examines these performance properties of cryptographic S-Boxes, and ensure you reference this paper in your submission. Clearly define each property in your own words, ensuring accuracy and clarity. Next, analyze the AES S-Box by measuring these properties, detailing your methodology step by step, and presenting your results using well-organized tables or graphs. Submit your work in both soft and hard copy formats.