Birzeit University

Faculty of Engineering and Information Technology

Computer Science Department

CSEC1310 Midterm Exam

(Introduction To Cybersecurity and professional ethics)

First Semester 2022-2023

Question one (Security Overview 20%)

Match those cases with one of the security aspects you learn through security overview materials (Confidentiality, Integrity,.. etc)

1) Preventing others from knowing your grades in Computer security course. (Confidentiality)
2) Preventing any modification to data in health care system. (Integrity)
3) The system is totally protected against all forms of Denial-of-service attack (DOS OR DDOS). (Availability)
4) Presenting your passport at security borders when you are traveling abroad. (Authentication)
5) Providing unforgeable evidence that a certain user is included in a certain intrusive action. (Network level) (Accountability)
6) Providing a link-ability (Application level) that a certain user is responsible for a certain action or included in a certain event. (Accountability)
7) Assuring that students can only see the grades on Ritaj system, but cannot modify them. (Authorization)
8) An identified weakness or flaw of an asset. (Vulnerability)
9) A cybersecurity approach that deploys security mechanisms at multiple layers/levels of a system. (Defense in Depth Approach/Layered Approach)
10) The process of deploying social skills to convincing people to reveal valuable information such as passwords. (Social Engineering)

Question two (Authentication, Passwords and Biometrics 27%)

A) What is the total number of 5 character passwords that have at least 3 capital letters? (4Marks)

Exactly 3 + Exactly 4+ Exactly 5
(3 selected from 5)*26^3*68^2 + (4 selected from 5)* 26^4*68+ 26^5

B) What is the total number of 6 character passwords that have 6 different characters? (3Marks)

94*93*92*91*90*89

C) Fill each one of the following authentication examples in the table based on its authentication factor type: (8Marks)
PIN-code, Token, password, smart card, fingerprint, gait, DNA, voice

Something you know	Something you have	Behavioral	Physiological
PIN-code	token	gait	DNA
password	smart card	voice	fingerprint

D) What we mean by standard and non-standard according to Face recognition system. (4marks)

Standard: face-recognition system in a static environment with controlled conditions (e.g. fixed lightning and background).
Non-standard: face-recognition system in a dynamic environment (e.g. inconstant lightning).

E) Consider the Fingerprints system .Is the system covert or overt and why?(5 Marks)

Overt, because user is aware that the fingerprint feature is being measured.

F) A hand geometry recognition system is tested and the total comparison scores are listed on Table 1. A1, B1, C1, D1 and E1 are enrolled persons and A2, B2, C2, D2 and E2 are test samples from the same persons.

Find the value of FNMR and FMR when the threshold value is 0.25 (3marks)

FNMR = 1/5
FMR = 0/20

Users	A2	B2	C2	D2	E2
A1	0,12	3,74	1,52	3,31	4,31
B1	3,81	0,08	0,97	3,00	3,85
C1	1,53	1,21	0,98	1,22	2,21
D1	3,24	3,00	0,99	0,25	3,45
E1	4,30	3,65	2,45	3,46	0,17

Question three (Cryptology, 33%)

The following message needs to be Decrypted TO BE Understandable. The Encryption process is done with two phases first Ceaser cipher using a key 1 then transposition cipher using a key (3,1,2,5,4).

VJFD STDB TUJG JQPF FBFL

1) What is the plain text? (6marks)

First step: Decrypting the ciphertext by deploying transposition cipher with key (3, 1, 2, 5, 4) as the following:

3	1	2	5	4
T	V	S	F	J
U	J	T	B	Q
J	F	D	F	P
G	D	B	L	F

Second step: Decrypting the output of the transposition cipher by deploying Caesar cipher with key 1 as the following:

S	U	R	E	I
T	I	S	A	P
I	E	C	E	O
F	C	A	K	E

Then by taking the rows, the plaintext is:
(SURE IT IS A PIECE OF CAKE)

2) Ceaser Cipher belongs to what type of classical ciphers?(2 marks)

Belongs to the monoalphabetic substitution ciphers

3) What is the advantage of the cipher process used above over other classical ciphers?(2 marks)

The used cipher provides stronger and more secure approach by combining two different cryptographic algorithms (becomes harder to break). The two principles of Shannon's theory are deployed, confusion by using Caesar cipher and diffusion by using transposition cipher.

4) Explain the weakness and what type of attack can be performed on Ceaser cipher?(2marks)

Caesar cipher can be easily broken by deploying counting statistics of natural language (i.e. frequency analysis), In addition to the limited number of shifts/cycles. Brute force attack can break Caesar cipher.

5) The diffusion and confusion principles of Shannon are implemented in modern ciphers and this can be easily shown in DES. Please discuss this statement.(5marks)

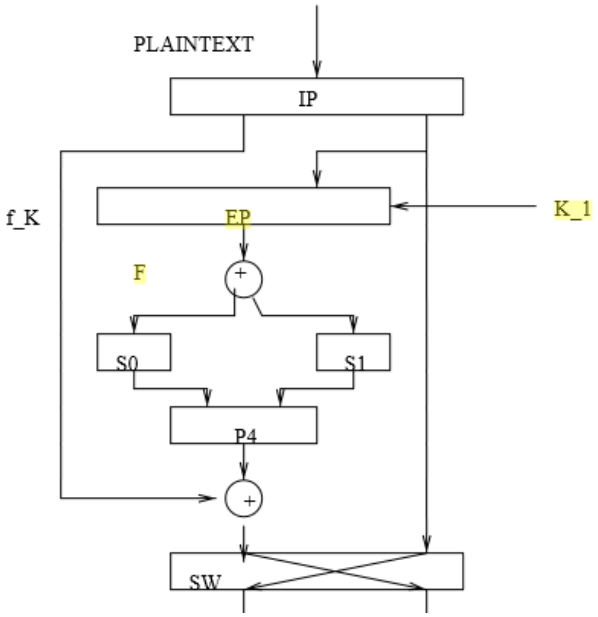
In DES cipher, the principle of confusion is implemented by using the substitution tables (such as S0 and S1), in addition to the XOR operation. While the principle of diffusion is implemented by using the permutation tables (such as P10, P8, and P4).

6) Given a block $(1B)_{16}$ (00011011)in simple DES and a key k1 $(25)_{16}$ (00100101)Find the cipher text for next round(simple iteration) (10Marks)

$$IP: \begin{pmatrix} 2 & 6 & 3 & 1 & 4 & 8 & 5 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}$$

EP

$$\begin{pmatrix} 4 & 1 & 2 & 3 & 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}$$



$$S0 = \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \quad S1 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix}$$

P4

$$\begin{pmatrix} 2 & 4 & 3 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

k_1: 00100101
Plaintext: 00011011
IP: 00001111
R-half: 1111
L-half: 0000
EP: 11111111 (deployed on R-half)
XOR: 11011010 (EP XOR k_1)
S0: 11 (left half of XOR deployed on S-Box 0)
S1: 00 (right half of XOR deployed on S-Box 1)
S0S1: 1100
P4: 1001 (deployed on S0S1)
XOR: 1001 (P4 XOR L-half)
Result: 10011111 (XOR + R-half)
SW: 11111001