דף סיכום בחינה

מזהה בחינה: 0039856191 מזהה סטודנט: 315368134

מזהה קורס: 20740-0 שם קורס: הגנת סייבר בסביבות מבוססות 2

#	תיאור	הערה	ציון מקסימאלי	ציון שאלה סופי	שאלת בונוס	שאלה מבוטלת
1			20.00	20.00	0	0
2			20.00	20.00	0	0
3			20.00	20.00	0	0
4			20.00	20.00	0	0
5			20.00	20.00	0	0

ציון בחינה סופי : 100.00

הבחינה הבדוקה בעמודים הבאים

המכללה
הטכנולוגית
באר שבע
בשיתוף WORLD ORT
קדימה מדע

מחברת בחינה

אין לכתוב מעבר לקו האדום משני צידי הדף

הוראות נוספות לנבחן בגב המחברת

מחברת מס' _____
מתוך _____ מחברות

שים לב! באחריותך לוודא שמדבקת הברקוד הינה שלך

מס' ת.ז. 3 1 5 3 6 8 1 3 4

הגנת סייבר בסביבות מבוססות 2
מועד 1 29/01/2019 08:30 חדר: B303
בן זקן יוסי 315368134

0039856191

ועדת המשמעת מזהירה!

נבחן שימצאו ברשותו חומרי עזר אסורים,
טלפון סלולרי (גם כבוי) או יתפס בהעתקה,
יענש בחומרה עד כדי הרחקתו מהמכללה!

שם המשגיח/ה אלי קרוס

לשימוש המרצה הבודק

(יש להשחיר את העיגול)

	יחידות	עשרות	מאות
0	○	○	
1	○	○	○
2	○	○	
3	○	○	
4	○	○	
5	○	○	
6	○	○	
7	○	○	
8	○	○	
9	○	○	

ציון הבחינה _____

שם _____

חתימה _____

תאריך _____

אל תקרע! השולים נחתכו לפני הסרקה!

יוסי בן כהן
315368134

המכללה
הטכנולוגית
באר שבע
בשיתוף WORLD ORT
קדימה מדע

המכללה הטכנולוגית באר שבע

המגמה לתוכנה

הנדסאי תוכנה בוקר – שנה ב

תשע"ט סמסטר א'

תאריך הבחינה: 29/01/2019

שם הבחינה – הגנת סייבר בסביבות מבוססות 2

מועד - א

שם המרצה - קוציי אלונה

חומר עזר - מחשבון ללא יכולת תכנות בלבד

משך הבחינה - 3 שעות

הוראות מיוחדות – יש לענות בטופס הבחינה בלבד! יש לענות רק במקום המיועד לתשובה. תשובה לא במקום הנכון לא תבדק!

במידה ואינכם יודעים את התשובה לסעיף כלשהו, רשמו "לא יודע" ותזכו ב-20% מניקוד הסעיף.

השאלון מכיל 10 דפים (כולל דף זה).

בהצלחה !

==========

המכללה
הטכנולוגית
באר שבע
בשיתוף WORLD ORT
קדימה מדע

שאלה 1: (20 נק')

מרגל מצליח לשים את ידו על ההודעה המוצפנת (ciphertext) הבאה:

good afternoon students
TBBQNSGREABBAFGHQRAGF!

k = 13

אין ברשותו של המרגל מפתח כדי לפענח את ההודעה, אך הוא יודע שההודעה הוצפנה באמצאות צופן הזזה.

מהי ההודעה שהוצפנה (plaintext) ומהו המפתח בו היא הוצפנה?

בסוף לשתובה, יש להסביר במילים (לא יותר מ-2 שורות) כיצד שברתם את הצופן.

תשובה:

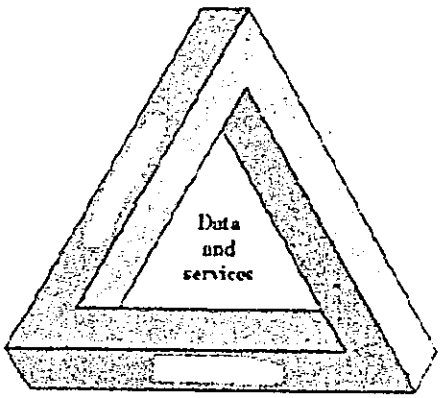
ההודעה היא Good Afternoon students! המפתח הוא 13

חיפשתי בגוגל אותיות גדולות ואותיות הגלה וכך שברתי את הכאך 00 בתקרים bb

20
(1)

שאלה 2: (20 נק')

באיור הבא מופיע משולש דרישת אבטחה.



The Security Requirements Triad

המכללה
הטכנולוגית
באר שבע
בשיתוף WORLD ORT
קדימה מדע

מהן שלושת הדרישות האבטחה?

נא להסביר בקצרה למה הן חשובות. האם ייתכן שבתוכנה כלשהי תחסור אחת מהדרישות (או כמה מהן)? יש לתת דוגמא לכך.

תשובה:

20
(2)

שלושת הדרישות מבטחה הן: שלמות - שלא בוצעה שלמות של האתר שלה יהיה שונים שלמות הנתונים
סודיות - שרק המשתמש יוכל לראות את הדברים שלו האישיים
3. זמינות - תמיד להיות זמין בשביל הלקוח

לא ייתכן שהתוכנה יהיה חסר אחת מהדרישות לדוגמא:
בנק חייב שיהיה שלמות הנתונים שיהיו אמינים חייב סודיות כי יש שם דברים פרטיים, וחייב חייב להיות זמין עבור הלקוח

שאלה 3: (20 נק')

התקפות בטיחות מתחלקות להתקפות אקטיביות (active attacks) והתקפות פסיביות (passive attacks).

המכללה
הטכנולוגית
באר שבע
בשיתוף WORLD ORT
קדימה מדע

נא להסביר בקצרה מהי התקפת Denial of Service (DoS), ולאיזה סוג ההתקפה היא שייכת.

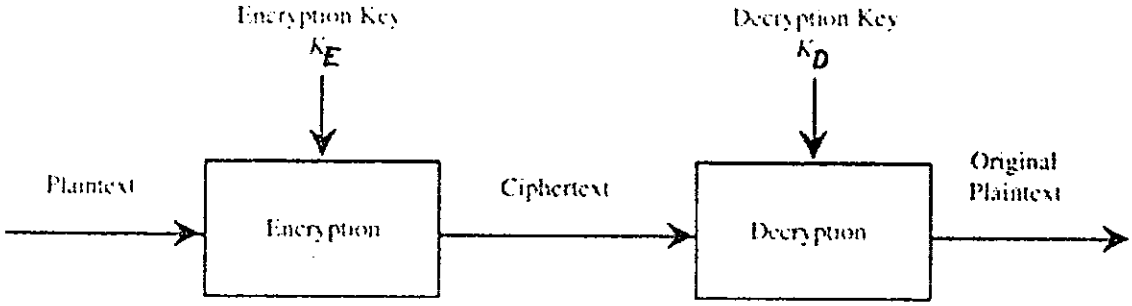
תשובה:

התקפת DoS זאת התקפה שתקפה את הרשת
היו שיכת להתקפה אקטיבית (active attacks)

20
(3)

שאלה 4: (20 נק')

נא להסביר איזה סוג קריפטוגרפיה (סימטרית / אסימטרית) מתוארת באיור הבא:



נא לתת דוגמא להצפנה זו (אילו אלגוריתמים קיימים). נא להסביר מהם יתרונות בשימוש בהצפנה זו.

תשובה:

זאת התקפה אסימטרית שיש פה שתי מפתחות אחת להצפנה
ואחת לפיענוח
דוגמא לאלגוריתמים קיימים: RSA, Elgamal
יתרונות בדף הבא

20
(4)

המכללה
הטכנולוגית
באר שבע
בשיתוף WORLD ORT
קדימה מדע

יתרון של שיטה זאת הינו: שמתבצעת לסנכרן בעצמו רק אבל
בן אדם אחר ובכך יותר קשה לסנכרן והיבחנת סודי.

שאלה 5: (20 נק')

באיזה אלגוריתם הצפנה משתמשים על מנת לשמור סיסמא של המשתמש בבסיס נתונים?

מה יתרון של האלגוריתם הזה לאומת אלגוריתמם הצפנה אחר?

מה חסרון של האלגוריתם הזה לאומת אלגוריתמם הצפנה אחר?

תשובה:

משתמשים באלגוריתם הצפנה SHA256 על מנת לשמור סיסמא
של משתמש בבסיס נתונים
יתרון של SHA256: לא ניתן לסנכרן אותו השכל לראות סיסמא
בגרסה מוצפנת באמצעות SHA256 ונשמרים בדן תוצאה של ההצפנה
עם מה שיש בבסיס הנתונים לאומת הצפנות אחרות

חסרון של SHA256: לא ניתן לדעת אם בה הצפן אותו כמו שרציו
לאומת הצפנות אחרות

20
(5)

המכללה
הטכנולוגית
באר שבע
בשיתוף WORLD ORT
קדימה מדע

המכללה הטכנולוגית באר שבע
רמיר רזל 71 ת.ד. 45 באר-שבע 8410001

המכללה
הטכנולוגית
באר שבע
בשיתוף WORLD ORT
קדימה מדע

דפי עזר:

1. **Eglish ABC:**

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

2. **Vigenere Cipher:**

	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

3. **One-Time Pad Cipher:**

binary	000	001	010	011	100	101	110	111

המכללה
הטכנולוגית
באר שבע
בשיתוף WORLD ORT
קדימה מדע

דף טיוטה. לא יבדק!!!!

המכללה
הטכנולוגית
באר שבע
בשיתוף WORLD ORT
קדימה מדע

דף טיוטה. לא יבדק!!!!

המכללה הטכנולוגית באר שבע
רמות רזל 71 ת.ד. 45 באר-שבע 8410001

המכללה
הטכנולוגית
באר שבע
בשיתוף WORLD ORT
קדימה מדע

דף טיוטה. לא יבדק!!!!

המכללה הטכנולוגית באר שבע
רמיר רזל 71 ת.ד 45 באר-שבע 8410001

המכללה
הטכנולוגית
באר שבע
בשיתוף WORLD ORT
קדימה מדע

הנחיות כלליות לנבחנים:

1. המשגיח יקבע את מקום ישיבתך ובידו הסמכות להעבירך במהלך הבחינה ממקום למקום.

2. הנח ליד הלוח את חפציך האישיים: תיקים, ספרים, מחברות, **מכשירים סלולאריים כבויים** וקלמרים.

3. הנח על השולחן **תעודה מזהה וכרטיס נבחן תקף**, ללא מסמכים אלו **לא תורשה להבחן**.

4. **יש לכתוב את הבחינה בעט שחור או כחול בלבד!**

5. אין להשתמש בטיפקס למחיקה!

6. אין לכתוב בשוליים משני צידי הדף, **השוליים נחתכים** לפני סריקת המחברות!

7. טיוטה יש לכתוב בצד הימני של המחברת. את הטיוטה יש למחוק בהעברת X.

8. אסור לתלוש דפים מהמחברת!

9. היציאה לשירותים במהלך הבחינה תותר באופן יוצא מן הכלל וחד פעמי, בליווי משגיחה **חצי שעה לאחר תחילת שעת הבחינה** ועד חצי שעה לפני סיומה. יציאה לשירותים תאושר פעם אחת בלבד במהלך הבחינה

10. את שאלון הבחינה ניתן לקבל רק בסיום הבחינה, אם המרצה יתיר זאת.

11. אין להעביר חומר עזר, כולל מחשבונים מנבחן לנבחן.

12. בתום הבחינה יש למסור למשגיחה את המחברת בשלמותה כולל השאלון. יש לשמור את **הספח לסטודנט שקיבלת**.

13. סטודנט המאחר לבחינה עד חצי שעה מתחילתה יורשה להיבחן באישור המרצה, אך לא יזכה לתוספת זמן.

14. ניתן **לערער** על ציון בחינה בצורה ממוחשבת! מידע אישי ← ציונים ← מטלת "בחינת סמסטר".

15. ניתן להגיש ערעור **עד שלושה ימים** מתאריך פרסום ציון הבחינה.

16. הערעור חייב להיות ממוקד. עליך להתייחס לשאלה, סעיף ותוכן ספציפי בתשובה.

17. לידיעתך - הערעור יביא לבדיקה והערכה מחודשת של תשובתך!

18. תשובה על ערעור תתקבל במייל של הסטודנט.

19. סטודנט שעבר בחינה מועד א' ונכשל בציון סופי או סטודנט המעוניין לשפר ציון **חייב** להירשם לבחינת מועד ב' לשיפור ציון עד שלושה ימים לפני הבחינה. הרישום יתבצע באמצעות מידע אישי לסטודנט או רישום במנהל הסטודנטים.

אבטח לבד! השוליים נחתכו לפני הסריקה. חל איסור מוחלט לכתוב כאן