

דף סיכום בחינה

מזהה בחינה: 0156672111

מזהה קורס: 30-1301026-1 שם קורס: אבטחת מערכות תוכנה (מקוון)

מספר שאלה	ניקוד מירבי	ציון
1.1	6.00	6.00
1.2	5.00	5.00
1.3	8.00	8.00
1.4	6.00	0.00
2.1	12.00	9.00
2.2	8.00	8.00
2.3	5.00	1.50
3.1	6.00	6.00
3.2	12.00	6.00
3.3	7.00	4.00
4.1	12.00	9.00
4.2	6.00	6.00
4.3	7.00	7.00

ציון בחינה סופי : 75.50

הבחינה הבדוקה בעמודים הבאים

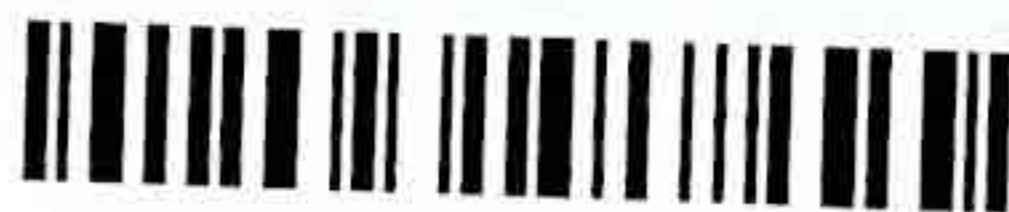
ד

מכללת הנגב ע"ש פ' ספיר (עיר)

מחברת מס' \_\_\_\_\_

מתוך \_\_\_\_\_ מחברת

למחברת נוספת חובה  
להעתיק מספר נבחן



מס.נבחן: 3920889

מועד 1 26/03/2024 09:00 חדר: 703-אחוזה  
(אבטחת מערכות תוכנה (מקוון ד"ר גל-עוז נורית, מר עמר אי

2ה3/אה!

ד

המכללה האקדמית ספיר (עיר)  
Sapir College

אין לכתוב מעבר לקו משני צידי הדף

הוראות לנבחן בצידו השני של הספח

לשימוש המרצה הבודק

יחידות | עשרות | מאות

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	3
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	6
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	7
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	8
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	9

נא לסמן את הציון ע"י סימן X

ציון הבחינה \_\_\_\_\_

שם \_\_\_\_\_

חתימה \_\_\_\_\_

תאריך \_\_\_\_\_

ד

המכללה האקדמית ספיר

ד

מכללת הנגב ע"ש פ' ספיר

ד

המכללה האקדמית ספיר



## הוראות לנבחן

7. יש לכתוב את התשובות בעט, בכתב יד ברור ונקי. נבחן הבוחר לכתוב טיוטה יעשה זאת בעמוד הימני של דפי מחברת הבחינה ויציין בראש העמוד "טיוטה". אין לתלוש דפים מהמחברת.
8. מחברות הבחינה שקיבל הנבחן תהיינה בפיקוחו ואחריותו במשך כל הבחינה. בעת יציאה מהחדר יופקדו המחברות והשאלון בידי המשגיח.
9. בתום הבחינה יחזיר הנבחן את המחברות והשאלון ויקבל מידי המשגיח ספח מחברת הבחינה.
10. אין להעתיק חומר כלשהו משאלון הבחינה, אלא אם ניתן לכך היתר מפורש.
11. הנוהג בניגוד להוראות צפוי להעמדה לדין משמעת.

בהצלחה!

1. על הנבחן להיבחן רק בחדר בו הוא רשום.
2. עם הכניסה לחדר הבחינה יש להניח את החפצים בצד לרבות מכשירי קשר ואמצעי תקשורת אחרים כשהם כבויים.
3. אסור להחזיק בהישג יד, בחדר הבחינה או סמוך לו, כל חומר הקשור לבחינה פרט לחומר שהשימוש בו הותר בכתב על-ידי המרצה.
4. יש למלא את הפרטים על מחברת הבחינה במקומות המיועדים לכך בלבד, אין לכתוב את השם או כל פרט מזהה אחר בתוך המחברת.
5. יש להישמע להוראות המשגיח. נבחן לא יעזוב את מקומו ללא קבלת רשות המשגיח. הפונה בשאלה או בקשה ירים את ידו. אין לדבר בזמן הבחינה.
6. נבחן שנכנס לחדר הבחינה וקיבל את השאלון (טופס הבחינה) לידי ייחשב כמי שנבחן במועד זה. היה והחליט לא לכתוב את הבחינה, לא יהא רשאי לעזוב את חדר הבחינה, אלא כעבור חצי שעה ממועד התחלתה ולאחר שהחזיר את המחברת והשאלון. ציונו בבחינה יהיה "0".



26/03/2024	תאריך הבחינה:
דר' נורית גלעז	שם המרצה:
אבטחת מערכות תוכנה	שם הקורס:
מדעי המחשב	מחלקה:
30-1301026-1	מספר הקורס:
שנה: תשפ"ד	סמסטר: א' מועד: א'
משך הבחינה: 2.5 שעות	
חומר עזר: מוגבל (דף 4A משני הצדדים)	
בחינה חסויה	

מדעי המחשב  
המכללה האקדמית ספיר

הנחיות כלליות:

- 1) נא לוודא כי בשאלון זה 10 עמודים כולל עמוד זה
- 2) סך הניקוד במבחן הוא 100 נקודות לפי הפירוט הבא:
  - שאלה 1: בקרת גישה = 25 נק'
  - שאלה 2: הצפנה = 25 נק'
  - שאלה 3: הגנה בבסיסי נתונים = 25 נק'
  - שאלה 4: אימות זהות = 25 נק'
- 3) אם אינכם יודעים את התשובה, ניתן לכתוב "לא יודעת" ולקבל 20% מהניקוד על הסעיף/השאלה. כלל זה אינו חל על שאלת הבונוס.
- 4) אין לכתוב בעיפרון.

בהצלחה!





## שאלה 1 [ 25 ] בקרת גישה

א. [6] נתונות הקבוצות הבאות שהוגדרו לצורך שימוש עם מערכת ההרשאות של יוניקס

Group 1: Alice, Bob, Clair, David

Group 2: Alice, Bob, Clair

Group 3: Bob, Clair

נתונה רשומת הגישה הבאה לקובץ File 1:

File 1: Group 1, R; Group 2, RW

המדיניות להענקת הרשאות על פי רשומות גישה, מוגדרת באמצעות כללים שעליכם לנסח.

בהינתן הקבוצות וההרשאות לעיל:

א.1. נסחו כלל שלפיו אליס יכולה לכתוב לקובץ File1: רשמו שם משמעותי לכלל והסבירו את הרעיון העומד

מאחוריו. הכלל ייתרן הרשאת כתיבה למספר קבוצות שיש להן הרשאת כתיבה  
 (כאן ה- read/write) הורשאות. יהיה גבוהה קבוצת אליס (היא  
 RW וכלל קבוצת רשומות גישה של אליס יהיו קבוצת  
 קבוצת אליס וכלל קבוצת רשומות גישה של אליס יהיו קבוצת  
 כתובות אליס וכלל קבוצת רשומות גישה של אליס יהיו קבוצת  
 אליס יהיו קבוצת רשומות גישה של אליס יהיו קבוצת

6  
(1.1)

א.2. נסחו כלל שלפיו אליס לא יכולה לכתוב לקובץ File1: רשמו שם משמעותי לכלל והסבירו את הרעיון העומד

מאחוריו.

הכלל ייתרן הרשאת כתיבה למספר קבוצות שיש להן הרשאת כתיבה  
 ההרשאת קבוצת אליס יהיו קבוצת רשומות גישה של אליס יהיו קבוצת  
 אליס יהיו קבוצת רשומות גישה של אליס יהיו קבוצת  
 אליס יהיו קבוצת רשומות גישה של אליס יהיו קבוצת  
 אליס יהיו קבוצת רשומות גישה של אליס יהיו קבוצת

ב. [ 5 ] נתון קובץ הרצה של תכנית P שצריכה לגשת לקובץ F במערכת.

את התכנית מריץ דני במערכת הפעלה יוניקס ולדני אין הרשאות גישה לקובץ F. כפי שלמדנו במודל

מטריצת הגישה גם לתהליכים יש להעניק הרשאות כדי שיוכלו לגשת למשאבי המערכת. במימוש ACL

ביוניקס כל השדות ב-ACL מתייחסים למשתמשים בלבד ולא לתהליכים. הסבירו כיצד יכולה התוכנית P

לקבל הרשאות שאין לדני.







5  
(1.2)

אשר לא הרשאת מבט (view) של חלק P  
ואם יש אורח אחר בהרשאות אחרות

לעצמם נוסף להם כמה בוססות אחרות

זה שיש יורש להם F שיש כמה ואם יש מה שיש

פיר, כפי שיש להם P של שאלה יחסית F של P יורש בוססות  
שם לא נוספת במה שיש להם אחרות ואם יש יורש

ג. [8] נתונה מערכת שמשמשת N משורות שונות. בכל משרה  $i$  ישנם  $U_i$  עובדים ומספר ההרשאות הנדרשות

על מנת למלא את המשרה הוא  $P_i$ .

לכל עובד עלינו לבצע רישום של ההרשאות שיש לו במערכת.

ציינו כמה פעולות רישום יהיו במערכת בכל אחד מהמודלים הבאים ונמקו את תשובתכם.

(פעולת רישום יכולה להיות: רישום כניסה במטריצת גישה, שיוך הרשאה לתפקיד, שיוך תפקיד למשתמש)

8  
(1.3)

• במודל ההרשאה לפי שיקול דעת DAC

$$\sum_{i=1}^N P_i \cdot U_i$$

כאשר זה לא היורש לא אחר בוססות

לכן בוססות (אם יש אחרות אחרות)

• במודל RBAC

$$\sum_{i=1}^N P_i + U_i$$

כאשר זה לא אחרות אחרות אחרות

הרשאות אחרות ואם לא נוספת כדור-סט  
ואם נוספת יש אחרות ואם אחרות אחרות אחרות

ד. [6] הורדת דרגת הסיווג של מסמך פוגעת בתכונת הכוכבית property\* במודל בל לה פדולה Bell

0  
(1.4)

LaPadula מכיוון שהמידע באובייקט זורם מסיווג גבוה לנמוך.

האם העלאת רמת הסיווג של מסמך פוגעת באחת מתכונות האבטחה של המודל? אם כן ציינו באיזו

תכונה והסבירו את הפגיעה ואם לא הסבירו מדוע.

~~אם כן יש לה קטגוריה נמוכה של אובייקט נמוך~~

~~אם כן יש לה קטגוריה נמוכה של אובייקט נמוך~~

~~אם כן יש לה קטגוריה נמוכה של אובייקט נמוך~~

~~אם כן יש לה קטגוריה נמוכה של אובייקט נמוך~~

~~אם כן יש לה קטגוריה נמוכה של אובייקט נמוך~~

אם כן יש לה קטגוריה נמוכה של אובייקט נמוך

העלאת רמת הסיווג אומרת שהוא היה חשוף לאנשים בסיווג יותר נמוך ואנשים בסיווג זה הם שכתבו לתוכו ויכלו לקרוא אותו. הם לא יוכלו לקרוא אותו יותר אבל אין כאן פגיעה באבטחה לפי תכונות המודל.







## שאלה 2 [25] הצפנה

א. [12] אליס ובוב רוצים להעביר ביניהם הודעה. יש להם אפשרות להשתמש בשיטת המפתח הציבורי.

המפתחות של אליס הם  $PU_A$  ו  $PR_A$  המפתחות של בוב הם  $PU_B$  ו  $PR_B$ . ( $PR=Private$ ;  $PU=Public$ ).

להלן מוצעות שתי אפשרויות לשליחת ההודעה  $M$ .  $K$  הוא מפתח רנדומלי להצפנה בשיטת מפתח סימטרי

לפי אלגוריתם ידוע  $H$  היא פונקציית גיבוב ידועה.

1. Alice  $\rightarrow$  Bob:  $\{K\}_{PUB}, \{M\}_K$

2. Alice  $\rightarrow$  Bob:  $\{H(M)\}_{PRA}, M$

\*הסימון  $\{X\}_Y$  מסמן הצפנת  $X$  בשיטת המפתח הסימטרי  $Y$  ניה AES אמצעות מפתח  $Y$ .

לכל אחת מהתכונות הבאות רישמו האם אפשרות 1 מקיימת אותה והאם אפשרות 2 מקיימת אותה, אם

מקיימת - נמקו את תשובתכם.

9  
(2.1)

a. הבטחת שלמות ההודעה (ההודעה המקורית שנשלחה תגיע)

b. לא מאפשרת התכשורת השולח (השולח לא יוכל לטעון שלא הוא שלח)

c. הבטחת סודיות ההודעה (רק בוב יוכל לקרוא את ההודעה)

d. הבטחת אותנטיות השולח (ניתן לדעת בוודאות מי השולח)

-1.5  
(2.1)

-1.5  
(2.1)

יוכל לפתוח אבל  
לא לשנות. אף  
אחד לא יכול  
יהצפין גיבוב של  
הודעה אחרת עם  
הפדטי של אליס

תוקף שתופס את התקשורת יכול  
להעביר מפתח אחר והודעה אחרת

רשמו את תשובותיכם בטבלה הבאה:

תכונה	אפשרות	מקיימת/לא מקיימת	נימוק
A	1	<input checked="" type="checkbox"/>	ההודעה $\{K\}_{PUB}$ היא פונקציית גיבוב של $K$ ו $K$ הוא מפתח רנדומלי. לכן, אם $\{K\}_{PUB}$ ישתנה, $K$ ישתנה, ו $\{M\}_K$ ישתנה. לכן, הבטחת שלמות ההודעה מתקיימת.
	2	<input checked="" type="checkbox"/>	ההודעה $\{H(M)\}_{PRA}$ היא פונקציית גיבוב של $H(M)$ ו $H(M)$ היא פונקציית גיבוב של $M$ . לכן, אם $\{H(M)\}_{PRA}$ ישתנה, $H(M)$ ישתנה, ו $M$ ישתנה. לכן, הבטחת שלמות ההודעה מתקיימת.
B	1	<input type="checkbox"/>	ההודעה $\{K\}_{PUB}$ היא פונקציית גיבוב של $K$ ו $K$ הוא מפתח רנדומלי. לכן, אם $\{K\}_{PUB}$ ישתנה, $K$ ישתנה, ו $\{M\}_K$ ישתנה. לכן, הבטחת סודיות ההודעה מתקיימת.
	2	<input type="checkbox"/>	ההודעה $\{H(M)\}_{PRA}$ היא פונקציית גיבוב של $H(M)$ ו $H(M)$ היא פונקציית גיבוב של $M$ . לכן, אם $\{H(M)\}_{PRA}$ ישתנה, $H(M)$ ישתנה, ו $M$ ישתנה. לכן, הבטחת סודיות ההודעה מתקיימת.
C	1	<input type="checkbox"/>	ההודעה $\{K\}_{PUB}$ היא פונקציית גיבוב של $K$ ו $K$ הוא מפתח רנדומלי. לכן, אם $\{K\}_{PUB}$ ישתנה, $K$ ישתנה, ו $\{M\}_K$ ישתנה. לכן, הבטחת אותנטיות השולח מתקיימת.
	2	<input type="checkbox"/>	ההודעה $\{H(M)\}_{PRA}$ היא פונקציית גיבוב של $H(M)$ ו $H(M)$ היא פונקציית גיבוב של $M$ . לכן, אם $\{H(M)\}_{PRA}$ ישתנה, $H(M)$ ישתנה, ו $M$ ישתנה. לכן, הבטחת אותנטיות השולח מתקיימת.
D	1	<input type="checkbox"/>	ההודעה $\{K\}_{PUB}$ היא פונקציית גיבוב של $K$ ו $K$ הוא מפתח רנדומלי. לכן, אם $\{K\}_{PUB}$ ישתנה, $K$ ישתנה, ו $\{M\}_K$ ישתנה. לכן, הבטחת אותנטיות השולח מתקיימת.
	2	<input type="checkbox"/>	ההודעה $\{H(M)\}_{PRA}$ היא פונקציית גיבוב של $H(M)$ ו $H(M)$ היא פונקציית גיבוב של $M$ . לכן, אם $\{H(M)\}_{PRA}$ ישתנה, $H(M)$ ישתנה, ו $M$ ישתנה. לכן, הבטחת אותנטיות השולח מתקיימת.

הי אין נפרד בין  $\{K\}_{PUB}$  ו  $\{M\}_K$  כי  $\{K\}_{PUB}$  היא פונקציית גיבוב של  $K$  ו  $K$  הוא מפתח רנדומלי. לכן, אם  $\{K\}_{PUB}$  ישתנה,  $K$  ישתנה, ו  $\{M\}_K$  ישתנה. לכן, הבטחת שלמות ההודעה מתקיימת.

ההודעה  $\{H(M)\}_{PRA}$  היא פונקציית גיבוב של  $H(M)$  ו  $H(M)$  היא פונקציית גיבוב של  $M$ . לכן, אם  $\{H(M)\}_{PRA}$  ישתנה,  $H(M)$  ישתנה, ו  $M$  ישתנה. לכן, הבטחת שלמות ההודעה מתקיימת.

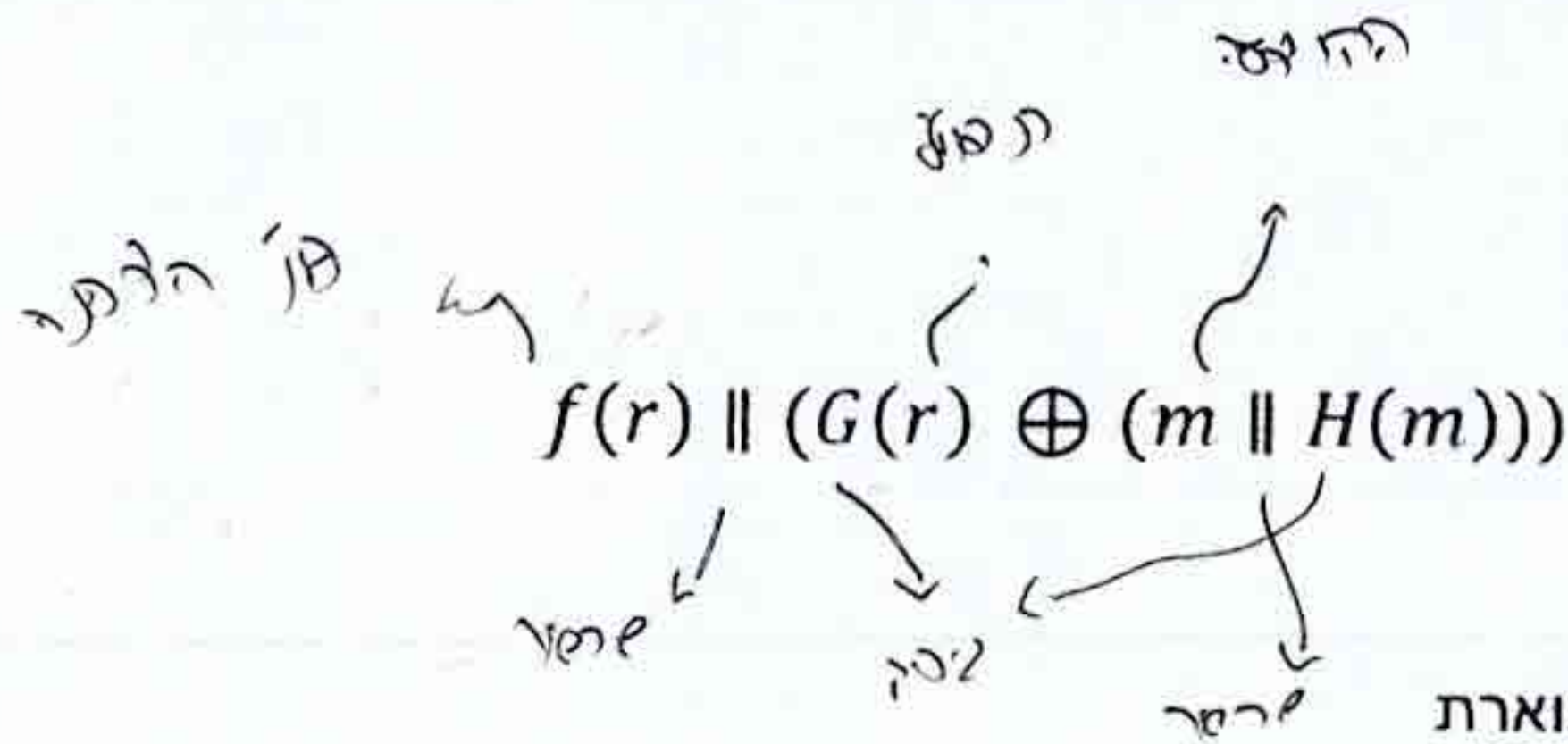
ההודעה  $\{K\}_{PUB}$  היא פונקציית גיבוב של  $K$  ו  $K$  הוא מפתח רנדומלי. לכן, אם  $\{K\}_{PUB}$  ישתנה,  $K$  ישתנה, ו  $\{M\}_K$  ישתנה. לכן, הבטחת שלמות ההודעה מתקיימת.







ב. [ 8 ] נתונה סכמת ההצפנה הבאה:



z הוא מספר רנדומלי

m היא ההודעה אותה מצפינים בסכימה המתוארת

f היא פונקציית הצפנה ידועה בשיטת מפתח ציבורי.

G H הן שתי פונקציות גיבוב ידועות

|| מסמל את פעולת השרשור על מחרוזות של ביטים

⊕ פעולת XOR על מחרוזות של ביטים באורך זהה.

ב.1. רשמו בנקודות את תהליך הפיענוח בצד המקבל.

המקבל יקבל את הנתון  $f(r) || (G(r) \oplus (m || H(m)))$  ויפצלו אותו לשני חלקים:  $f(r)$  ו- $G(r) \oplus (m || H(m))$ .

הוא יפצלו את  $G(r) \oplus (m || H(m))$  לשני חלקים:  $G(r)$  ו- $m || H(m)$ .

הוא יפצלו את  $m || H(m)$  לשני חלקים:  $m$  ו- $H(m)$ .

הוא יפצלו את  $m$  לשני חלקים:  $m$  ו- $H(m)$ .

הוא יפצלו את  $H(m)$  לשני חלקים:  $H(m)$  ו- $m$ .

הוא יפצלו את  $m$  לשני חלקים:  $m$  ו- $H(m)$ .

הוא יפצלו את  $H(m)$  לשני חלקים:  $H(m)$  ו- $m$ .

ב.2. באיזה מפתח כדאי לשלוח להשתמש על מנת להצפין את ההודעה ב? ציבורי שלו? פרטי שלו?

ציבורי של המקבל? פרטי של המקבל? נמקו את תשובתכם

הוא יפצלו את  $m$  לשני חלקים:  $m$  ו- $H(m)$ .

הוא יפצלו את  $H(m)$  לשני חלקים:  $H(m)$  ו- $m$ .

הוא יפצלו את  $m$  לשני חלקים:  $m$  ו- $H(m)$ .

הוא יפצלו את  $H(m)$  לשני חלקים:  $H(m)$  ו- $m$ .

הוא יפצלו את  $m$  לשני חלקים:  $m$  ו- $H(m)$ .

הוא יפצלו את  $H(m)$  לשני חלקים:  $H(m)$  ו- $m$ .

8

(2.2)







ג. [ 5 ] נתונה ההתקפה הבאה: אליס חייבת לבוב סכום כסף קטן ובוב רוצה שתאשר לו את החוב על ידי כך

שתשלח לו בחזרה את ההודעה מוצפנת עם המפתח הפרטי שלה. בוב מוצא שתי הודעות עם פונקציות

גיבוב זהה: אחת מציינת את הסכום המדוייק והשניה מנוסחת קצת שונה ומציינת סכום גבוה בהרבה.

איזו מהתכונות הבאות של פונקצית גיבוב קריפטוגרפית  $h$  תגן מפני התקפה זאת? נמקו את תשובתכם.

בהינתן  $h(x)$  קשה למצוא את  $x$ . (נכון/לא נכון)

החומר נמצא בחדר 105-106

(2) בהינתן  $x$  קשה למצוא  $y \neq x$  כך ש-  $h(y) = h(x)$ . (נכון ללא נכון)

כך נהג 'דאס' ערער גיטל פארוואס וועט מען קומען ביי אים און אים  
אויסווארפן דאס וועט מען אים אויסווארפן און אים אויסווארפן

(3) קשה למצוא  $x$  ו- $y$  כך ש- $y \neq x$  ו- $h(y)=h(x)$ . (נכון/לא נכון)

מה יתא עקר זכור שנים אס היא כן פ תוסס מ<sub>a</sub> על זהו ש' חסד

\*את המילה קשה המופיעה בתכונות פרשנו כ"לא ישים מבחינה חישובית".

**ממי בוב מקבל ערכי גיבוב שונים? הוא צריך למצוא הודעות עם ערכי גיבוב שונים**

ולא מקבל אחת וצריך למצוא את השניה.

## שאלה 3 [ 25 ] הגנה בבסיסי נתונים

א. [ 6 ] בבסיס הנתונים של ארגון מוגדרים משתמשים סטטיסטיים וכן על מנת להגן מפני התקפת היסק,

בנקטת גישת הגבלת השאילות Query restriction.

לדני מותר לגשת לנתונים בבסיס הנתונים של מחלקת משאבי אנוש רק באמצעות שאלות

## סטטיסטיקות.

בבסיס הנתונים קיימת טבלת עובדים המכילה עמודת שכר. דני מבקש שלוש שאילתות שמתבצעות על

עמודת השכר בטבלה בסדר הבא : SUM (2 COUNT (3 MAX .

בכל השאלות הגדיר דני את אותו תנאי לבחירת הרשומות ז"א ששלושתן יתבצעו בסופו של דבר על

אותו סט של רשומות מהטבלה.

א.1. דני הריץ את שתי השאילות הראשונות וקיבל תשובות. האם התשובות היו מדויקות? נמקו את

תשובתכם.

החברים: ד"ר נחמיה מנחם, מנחם כהן, רחל כהן, אריאל כהן, אריאל כהן, אריאל כהן

[illegible]

פרק חג המולד

הן נחשבות (כיום) שהן לא שם לעולם והיון מהם אדם אחר







הסבירו מדוע.

10. דבר  
 11. דבר  
 12. דבר  
 13. דבר  
 14. דבר  
 15. דבר  
 16. דבר  
 17. דבר  
 18. דבר  
 19. דבר  
 20. דבר  
 21. דבר  
 22. דבר  
 23. דבר  
 24. דבר  
 25. דבר  
 26. דבר  
 27. דבר  
 28. דבר  
 29. דבר  
 30. דבר  
 31. דבר  
 32. דבר  
 33. דבר  
 34. דבר  
 35. דבר  
 36. דבר  
 37. דבר  
 38. דבר  
 39. דבר  
 40. דבר  
 41. דבר  
 42. דבר  
 43. דבר  
 44. דבר  
 45. דבר  
 46. דבר  
 47. דבר  
 48. דבר  
 49. דבר  
 50. דבר  
 51. דבר  
 52. דבר  
 53. דבר  
 54. דבר  
 55. דבר  
 56. דבר  
 57. דבר  
 58. דבר  
 59. דבר  
 60. דבר  
 61. דבר  
 62. דבר  
 63. דבר  
 64. דבר  
 65. דבר  
 66. דבר  
 67. דבר  
 68. דבר  
 69. דבר  
 70. דבר  
 71. דבר  
 72. דבר  
 73. דבר  
 74. דבר  
 75. דבר  
 76. דבר  
 77. דבר  
 78. דבר  
 79. דבר  
 80. דבר  
 81. דבר  
 82. דבר  
 83. דבר  
 84. דבר  
 85. דבר  
 86. דבר  
 87. דבר  
 88. דבר  
 89. דבר  
 90. דבר  
 91. דבר  
 92. דבר  
 93. דבר  
 94. דבר  
 95. דבר  
 96. דבר  
 97. דבר  
 98. דבר  
 99. דבר  
 100. דבר

ב. [12] נתונה הטבלה הבאה שנגזרת מבסיס הנתונים של מערכת משאבי אנוש ללא עמודת השם:

	NAME (not stored)	SEX	LEV (job level)	LOC (work location)	SAL (salary)
1	Jackson	M	60	SF	24
2	Gaga	F	56	NY	20
3	Lopez	F	57	LA	30
4	Timberlake	M	58	LA	28
5	Bieber	M	60	LA	34
6	Swift	F	58	SF	30
7	Adel	F	58	SF	40

ללא קשר לסעיף הקודם, על טבלה זאת חלה הגבלה (query size restriction) על גודל הסט עליו מתבצעת

$k \leq X(C) \leq N - k ; k > 1$  :השאילתא  $X(C)$

ב.1. בהינתן  $K=2$  הראה איזו התקפת עוקב יכולה לעזור ל Swift העובדת בחברה לגלות את המשכורת של

חברתה Adel .

$$\text{Count}(F) = 4 \quad \text{Count}(F \circ (N \cup F)) = 2 \rightarrow$$

$$\text{Sum}(F, \text{SAL}) - \text{Sum}(F \circ (\sim_S F), \text{SAL}) = 70 \rightarrow \text{max } 10$$

[illegible]










ג. [7] שאלה זאת מתייחסת ל טכניקת הפרעה output perturbation

### 1.1.2

נתונים חלקיים = נתונים שכוללים רק חלק מהתוצאות שמחזירה השאילתא המקורית.

נכון/לא נכון: סכום 6 : 200 המאות התקומם



כרמלה נותן תשובה לך, לא נכנסים



## נכונים?

נכון/לא נכון. נימוק: סדרה במ (ו) להחיל קנסים אם לא =



## 2.2

4  
(3.3)

(3.3)

ק' יצ' זצ"ס יתרוה י' ה' א' אס"ח ו' רצ"ט ח"א

105 10' E 160 E 170 W 180 W 190 W 200 W 210 W 220 W 230 W 240 W







## שאלה 4 [ 25 ] אימות זהות

א. [12] נזכיר את פרוטוקול קרברוס המאפשר ניהול שירותים מבוזרים ברשת כך ששרת יוכל להבטיח את זהות המשתמש ויכול להוכיח למשתמש את זהותו :

1. Client --> KDC:  $ID_c, ID_{TGS}, nonce_1$
2. KDC --> Client:  $E_{K_c}(K_{c,TGS}, nonce_1), Ticket_{c,TGS}$
3. Client --> TGS:  $Auth_{c,TGS}, Ticket_{c,TGS}, ID_s, nonce_2$
4. TGS --> Client:  $E_{K_{TGS}}(K_{c,s}, nonce_2), Ticket_{c,s}$  →
5. Client --> Server:  $Auth_{c,s}, Ticket_{c,s}$
6. Server --> Client:  $[Auth_{s,c}]$

9  
(4.1)

לכל אחד מהמשפטים הבאים ציינו נכון/לא נכון . אם סימנתם נכון, נמקו.

(4) משתמש הקצה יצטרך להכניס שם וססמא פעם אחת בכל login למערכת. (נכון/לא נכון) ✗

(5) מטרת ה  $nonce$  להבטיח שמדובר במשתמש אותנטי. (נכון/לא נכון) ✓

(6) בשלב 2  $E_{K_c}$  הוא המפתח בין ה KDC למשתמש. (נכון/לא נכון) ✓

(7) הכרטיס  $Ticket_{c,s}$  (שלב 4) מוצפן באמצעות המפתח בין ה KDC ל TGS. (נכון/לא נכון) ✓

ב. [6] מנו שלוש בעיות שונות שיש בעת שימוש בסיסמאות לצורך אימות זהות המשתמש. לכל בעיה ציינו אם קיימת דרך כלשהיא להתמודד עמה (אפילו באופן חלקי).

(1) וסמא עם אותה כמטה רכזה נערכו ואז האות יצאה בקליף לרבים

פרק בעצם זה קיים כאלה גם שם נעזר האות נכונה לא יהיה נכון אולם  
הוא כי פרק הפסד מן ה אלף זה ייתכן

(2) האם האות עם יב א דוב רכזתן לא רעיה כי הוא נא לנדים

כמטא א נאמא וליאחטא אלה את כק גם זה פרק יצאן זהו ש

אלף לא יד רוכה קרה לו הקה לנדים כמטא וסמ קרה לא כך יארכ

כמטא ויסמ את הערך וזה זה יצאן לנדים א סמא א אלף וזה פרק שפצה

הוא א סמא ד אלף ננעל סמ ין כיכס נפלה זב ספין לא יחזה

הי א כיכס הישי נארכה עם פרק סמא קמח לנדים

הי א אלף זה האת יא לנדים פרק א כיכס ואז ארמ יא כמטא סמא

וקי א יצאן סמא ה אלף זה לא יאסמ לו







(3) תיבת עסקת-אמנות יקל לעבוד ויש להעמיד נשמתה תחתם  
 לרפוא אלו פנים, הולך יח עליו לא ולו יד כך ליכל קבטה (היה אמר)  
 מה זה דבר קטן למשל ותנו עצמו כזה שאתם סוף קצת אל נח קמות לא  
 יורד חסוד מורה.

ג. [ 7 ] אתגר תגובה הוא שם כללי למספר פרוטוקולים המשתמשים באמצעים שונים על מנת לשלוח אתגר ולקבל

תגובה מהגורם שאת זהותו רוצים לאמת.

1.g. תארו בשלבים כיצד מתבצע הפרוטוקול על מנת לאמת זהות באמצעים ביומטריים. בכל שלב ציינו מה

מחשב כל צד ( שרת האימות והלקוח -המשתמש אותו מאמתים) וכן מה הם מעבירים ביניהם עד לקבלת

## ההחלטה.

[illegible]

2.g. האם התקפת שידור חוזר replay attack אפשרית על פרוטוקול אתגר תגובה המשתמש באמצעי זהירות?

ביומטריים דינאמיים (קול / חתימה) . נמקו את תשובתכם.

[illegible]

תחנת זרע ביטחון וסמליות בהדפסה וזו נחשבת למקום יסודי  
 קיומו עומד סמליות וזוהי קרבן פסח בהדפסה א נחשבת למקום יסודי  
 אל הכיכר אל עבר המזרח והמזרח ימין נחשבת למקום יסודי  
 מקום יסודי וזוהי קרבן פסח בהדפסה וזוהי קרבן פסח בהדפסה  
 אל עבר המזרח והמזרח ימין נחשבת למקום יסודי



