אוניברסיטת בן-גוריון בנגב
Ben-Gurion University of the Negev

The Department of Information Systems Engineering

Security of Computers and Communication Networks

(372-1-4601)

Assignment #1

Submission guidelines

- **Please answer all questions**.
- Your answers should be full, short as possible, and address the question asked.
- Answers should be submitted in a word document called **answers.pdf**
- If you need more information **Google it!** Still have questions? Use the course forum on Moodle (do not use any other ways to ask questions (e.g., e-mails).
- Submission is allowed only in pairs. Please find yourself a partner from your department.
- Make sure your zip file is not corrupt – download it and extract it from Moodle
- Please submit the assignment to Moodle until 14:00 on 19/4/2020.
- Postponements will not be given (except of special cases such as Miluim, and etc.)
- Each day of delay will result in reduction of 5 points to the assignment's grade.

חלק א – קריפטוגרפיה

אנו הניחו כי גודל המפתח בשאלות המופיעות בחלק א' הוא 64 ביט אלא אם צוין אחרת.

שאלה מס' 1 (10 נק'): בתרגול למדנו את הסכמה של התקפת MAN IN THE MIDDLE על פרוטוקול ליצירת מפתחות דיפי-הלמן. הסכמה בנויה מ-4 פעולות שונות שמבוצעות ע"י התוקף לשם השגת שני מפתחות (אחד עם אליס ואחד עם בוב). צייר את כל הקומבינציות האפשרויות בהם תוקף יכול ליישם את ההתקפה.

שאלה מס' 2 (10 נק'): בנק שדרג את מערכת הצפנת הטרנזקציות שלו מ 2-DES למערכת 5-DES.
המערכת החדשה בעלת 5 מפתחות המופעלת כהרכבה של 5 הצפנות ברצף.
כמו כן ידוע כי אופן הפעלת המערכת נעשה ע"י:

$k_2 = k_1 + 1$

$k_3 = k_1 + k_2$

$k_4 = k_5$

כתוב פסאודו קוד להתקפה לשבירת המערכת 5-DES. נתח סיבוכיות זמן ריצה וזיכרון של ההתקפה שהצעת.

שאלה מס' 3 (10 נק'): נתונה מערכת הצפנה סימטרית עם מפתח K משותף בעל N ביטים.
כדי ליצר את המפתח הראשון k_1, אליס ובוס סיכמו על מספר כלשהו בעל N סיביות k_0.
את המפתח הראשון k_1, אליס ובוס יצרו בעזרת הנוסחא $k_i=1+2k_{i-1}$.
בסוף כל יום מעדכנים אליס ובוב את המפתח ליום הבא בעזרת אותה הנוסחא.

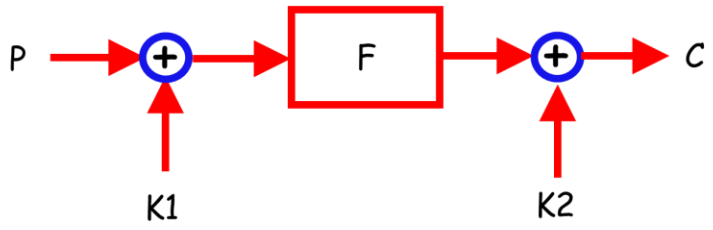
בשאלה הנ"ל הנח כי התוקף יודע מתי המערכת הותקנה.

א. כתוב פסאודו קוד להתקפה לשבירת המערכת והסבר את מודל ההתקפה כאשר התוקף מנסה למצוא את המפתח יומיים אחרי שהמערכת הותקנה. נתח סיבוכיות זמן ריצה וזיכרון של ההתקפה שהצעת. הקפד על ניתוח אדוק ככל האפשר של הזמני ריצה.
ב. הראה כי אם התוקף יעזר בסבלנות (ויתקוף את המערכת במועד מאוחר יותר) אז הוא יכול לשפר את זמני הריצה של מציאת המפתח משמעותית. נתח סיבוכיות זמן ריצה וזיכרון של ההתקפה שהצעת.

שאלה מס' 4 (5 נק'): בכיתה למדנו את התקפת MEET IN THE MIDDLE שמקטינה את סיבוכיות הזמן של הפעלת ההתקפה על מנגנון 2-DES בעזרת שימוש בזיכרון. כתוב את הפסאודו קוד של ההתקפה.

שאלה מס' 5 (15 נק'):

נתונה סכמת ההצפנה הסימטרית הבאה:



K_1 , K_2 – מפתחות בגודל 64 ביטים.
C,P – הודעות בגודל 64 ביטים.
הפונקציה F פומבית וידועה לכולם.
נתח סיבוכיות זמן ריצה וזיכרון לגילוי k1,k2 של ההתקפות הבאות:

א. Known Ciphertext
ב. Known Plaintext
ג. Known Plaintext and K_1

חלק ב – חלק מעשי

בשאלות 6-7 תלמדו לחקור קובץ PCAP שמכיל הקלטה של משתמש ולהסיק מה המשתמש עשה בגלישתו. לטובת השאלה הנ"ל יש להתקין WIRESHARK על המחשב. WIRESHARK הוא כלי ניתוח פופולארי לתעבורת רשת.

אנא הורד את הקובץ mystery.pcapng מהקישור הבא.

טען את הקובץ PCAP המצורף לעבודת בית (mystery.pcapng) ב - WIRESHARK.

הקובץ המצורף מכיל הקלטה של תעבורת רשת שנעשתה ממחשב של משתמש שה-IP שלו הוא 132.72.81.121

שאלה מס' 6 (20 נק' – כל שאלה 2 נקודות):

בשאלות הבאות תלמדו להפעיל פילטרים רלונטים.

יש מס' דרכים לענות על השאלות הבאות. אנו ממליצים לכם לפעול בדרך הבאה:

- מיצאו את הפילטר הרצוי שעונה על השאלה והכניסו אותו לשורה הרלוונטית (דוגמאות לכתיבת ביטויים לפילטרים ב WIRESHARK ניתן לראות בקישור הבא ובחיפוש באינטרנט).
- יצאו את התוצאה שהתקבלה מהפילטר לקובץ CSV ע"י:
  File->Export Packet Dissections-> As CSV
- כתבו קוד שמנתח את הקובץ CSV או נתחו בעזרת EXCEL.
- בכל סעיף אתם מתבקשים לכתוב את הפילטר שהתשמשתם בו ואת התשובה.

א. לכמה יעדי IP שונים נשלחה הודעה מהמחשב שה-IP שלו הוא 132.72.81.121?
ב. כמה יעדי IP שונים מופיעים בכל הקובץ הנ"ל?
ג. כמה הודעות UDP שונות נשלחו למחשב שה-IP שלו הוא 132.72.81.121?
ד. מה גודל הפקטה הנפוץ ביותר שנשלחה ממחשב שה-IP שלו הוא 132.72.81.121 והיא לא פקטת TCP? הבהרה לגבי התשובה הרצויה, רוב הפקטות שנשלחו ממחשב 132.72.81.121 הן בגודל _____ בייט

ה. מה הכתובות של שרתי ה DNS איתם תקשר המחשב שה-IP שלו הוא 132.72.81.121?
ו. כמה פקטות שונות אשר קשורות לסרטונים (video) נשלחו ממחשב שה-IP שלו הוא 35.172.73.102?
ז. כמה פקטות בעלות נפח מידע קטן מ-100 בייט נשלחו ממחשב שה-IP שלו הוא 35.172.73.102?
ח. האם מחשב בעל כתובת IP 35.172.73.102 ניסה לתקשר עם מחשב בעל כתובת IP 132.72.81.121 בעזרת פרוטוקול HTTP ?
ט. באמצעות כמה פרוטוקולים שונים יזם קשר מחשב בעל כתובת IP 132.72.81.121 עם מחשבים אחרים? נא ציין גם את שמות הפרוטוקולים.
י. מה הוא פרק הזמן הקצר ביותר (בשניות) בין 2 הודעות UDP שונות שנשלחו למחשב שה-IP שלו הוא 132.72.81.121? מה הוא פרק הזמן הארוך ביותר?

<u>שאלה מס' 7 (12 נק' – כל שאלה 3 נקודות):</u>

א. יצר גרף של פקטות UDP שנשלחו למחשב ש IP שלו הוא 132.72.81.121 כאשר ציר ה-X של הגרף הוא זמן (שניות מאז תחילת ההקלטה) וציר ה-Y של הגרף הוא אגרגציה של נפח ההודעות ברזולוציה של שתי שניות.

ב. נתח את הגרף שיצרת וענה על השאלה הבאה: מתי התחיל הפרק הזמן של ה-12 שניות בהן נשלח הכי הרבה מידע למחשב ש IP שלו הוא 132.72.81.121?

ג. מי המקור ששלח הכי הרבה נפח מידע של פקטות UDP למחשב 132.72.81.121 בפרק זמן הנ"ל? בתשובתך רשום את הכתובת IP של המקור ואת הנפח הכולל של פקטות UDP ששלחו אל מחשב ש-IP שלו הוא 132.72.81.121.

ד. ידוע כי המשתמש הוריד קובץ בעל נפח כבד מהרשת בפרק זמן המדובר. מאיזה שירות אחסון קבצים הורד הקובץ (רמז: האם תוכל לבדוק למי שייך ה IP מהסעיף הקודם)? הסבר כיצד מצאת.

<u>שאלה מס' 8 (18 נק' נקודות):</u>

בשאלה זו אתם צריכים לשבור צופן AES פשוט, המסומן AES_3^* .
בגרסה הפשוטה הזו של AES ישנם 3 מפתחות שונים המוגדרים כ $K_1\ K_2\ K_3$, השימוש במפתחות הללו הוא כפי שהם (כלומר אין שום מניפולציה על המפתחות). AES_3^* מבצע 3 פעמים (איטרציות iterations) של AES_1^* אשר גם הוא גירסא פשוטה של צופן AES. AES_1^* מוגדר כדלקמן:

M – הודעה לא מוצפנת Plain-text

C – הודעה. מוצפנת Cipher-text

K – מפתח הצפנה/פענוח

<u>Definition of AES_1*</u>

AES_1* is a single round implementation of AES that is defined as follows:

- $AES_1^*(M)_K = AddRoundKey(ShiftColumns(M),K) = C$
- $AES_1^{*-1}(C)_K = ShiftColumns^{-1}(AddRoundKey(C,K)) = M$

הפונקציה ShiftColumns(M) עובדת בצורה זהה לפונקציה ShiftRows(M) שנלמדה בכיתה כאשר ההזזה הציקלית היא של עמודה (במקום שורה) למעלה (במקום שמאלה).
העמודה באינדקס 0 זזה 0 תאים למעלה.
העמודה באינדקס 1 זזה תא אחד למעלה.
העמודה באינדקס 2.....
$ShiftColumns^{-1}(M)$ מבצעת את הפעולה ההפוכה, כאשר ההזזה הציקלית של כל עמודה היא כלפי מטה.

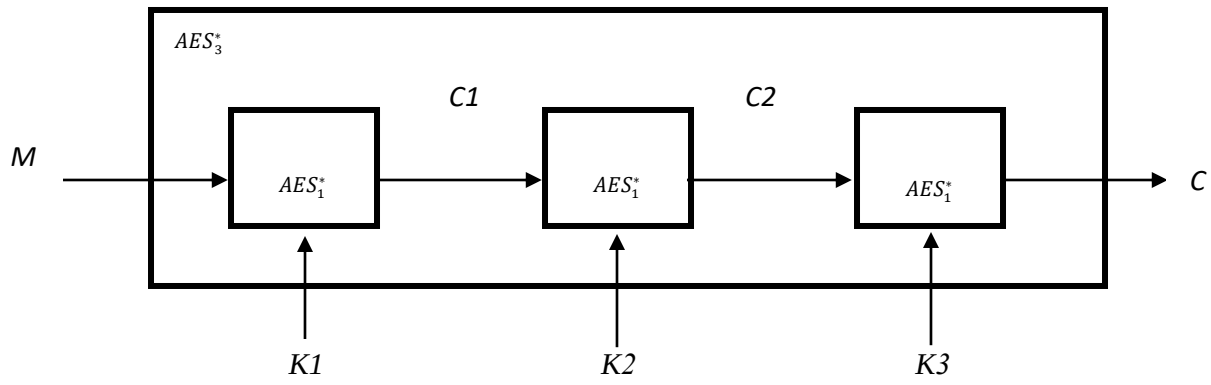
ולכן הגדרה של AES_3^* היא:

Definition of AES_3^*:

- AES_3^* is the application of AES_1^* three times with three different keys: K_1, K_2, K_3
- $AES_3^*\{M\}_{K_1,K_2,K_3} = AES_1^*\left\{AES_1^*\{AES_1^*\{M\}_{K_1}\}_{K_2}\right\}_{K_3} = C$
- $AES_3^{*-1}\{C\}_{K_1,K_2,K_3} = AES_1^{*-1}\left\{AES_1^{*-1}\{AES_1^{*-1}\{C\}_{K_3}\}_{K_2}\right\}_{K_1} = M$

בהינתן הודעה M והודעה מוצפנת C כך ש: $C = AES_3^*\{M\}_{k1,k2,k3}$, הנכם צריכים לממש שיטה יעילה למציאת 3 המפתחות K1,K2,K3 המקיימת: $C = AES_3^*\{M\}_{k1,k2,k3}$.

האלגוריתם הצפנה AES_3^* ממומש כך:



שימו לב כי במימוש שלכם לפריצה של AES_3^* עליכם להתייחס ל AES_3^* כקופסא שחורה המקבלת הודעה M ו3 מפתחות כקלט ומוציאה כפלט הודעה מוצפנת C לפי ההגדרה נ"ל. **אינכם יכולים להשתמש בהודעות הביניים C1 ו C2! כמו כן מפתחות K1 K2 K3 חייבים להיות שונים אחד מהשני**

א. רשום פתרון תיאורטי לשיטה שאתה מציע **(4 נק')**.
ב. ממש את הפתרון שהצעת ב- JAVA לפי הדגשים הבאים **(14 נק')**:

דגשים למימוש:

- הודעה M יכולה להיות ארוכה יותר מ 128 ביט, המימוש שלכם צריך לקחת בחשבון שאורך הודעה יכול להיות יותר ארוך מ 128 ביט, לחלק את ההודעה לבלוקים של 128 ביט ולהפעיל את האלגוריתם על כל בלוק, לשם הפשטות ניתן להניח כי אורך ההודעה היא מכפלה של 128 ביט.
- עליכם לממש ממשק (interface) הצפנה/פענוח כדלקמן:

  - –e : instruction to encrypt the input file
  - –d: instruction to decrypt the input file
  - –k <path>: path to the keys, the key should be 384 bit (128*3) for AES_3^*. and should be divided into 3 separate keys.
  - –i <input file path>: a path to a file we want to encrypt/decrypt
  - –o <output file path>: a path to the output file
  - Usage: Java –jar aes.jar -e/-d –k <path-to-key-file > -i <path-to-input-file> -o <path-to-output-file>
    –e –k key.txt –i message.txt –o cypther.txt Java –jar aes.jar

- עליכם לממש ממשק (interface) לשבירה של ההצפנה כדלקמן:

  - –b : instruction to break the encryption algorithm
  - –m <path>: denotes the path to the plain-text message
  - –c <path>: denotes the path to the cipher-text message
  - –o <path>: a path to the output file with the key(s) found.
  - Usage: Java –jar aes.jar -b –m <path-to-message> –c <path-to-cipher> -o < output-path>

- פורמט הפלטים והקלטים:
  - הנכם מתבקשים לכתוב ולקרוא מקבצים **בבתים Bytes ולא כטקסט.**
  - **שימו לב לסדר בתים (Endianness), ניתן לוודא את סדר הבתים בשקופיות של ההרצאה.**
  - השתמשו בקבצי בדיקה שסופקו לכם ביחד עם התרגיל על מנת לבדוק את התוכנית שלכם.

- שימו לב כי זמן ריצה של התוכנית צריך להיות בזמן סביר **הלא עולה מעל דקה אחת**.
- אין להשתמש ב brute force.
- עליכם להגיש את כל קבצי המקור וקובץ jar מקומפל של התוכנית שלכם.
- הבדיקה מתבצעת בתוכנה אוטומטית, אנא בדקו היטב כי התוכנית שלכם עונה על כל הדרישות הנמצאות בקובץ הזה.
- שימו לב כי תוכנה אוטומטית תצליב בין כל קבצי המקור לזיהוי קוד דומה, אנא הימנעו מהעתקות.
- ההגשה היא במודל, יש להגיש קובץ zip בלבד בפורמט הבא: ass1_id1_id2.zip בתוך הקובץ יש לשים את כל קבצי המקור וקובץ jar. קובץ jar חייב להיות בשם aes.jar
- קבצי בדיקה ניתן להוריד מהקישור הבא