****

**The Department of Information Systems Engineering**

**אבטחת מחשבים ורשתות תקשורת**

**עבודה מס' 1**

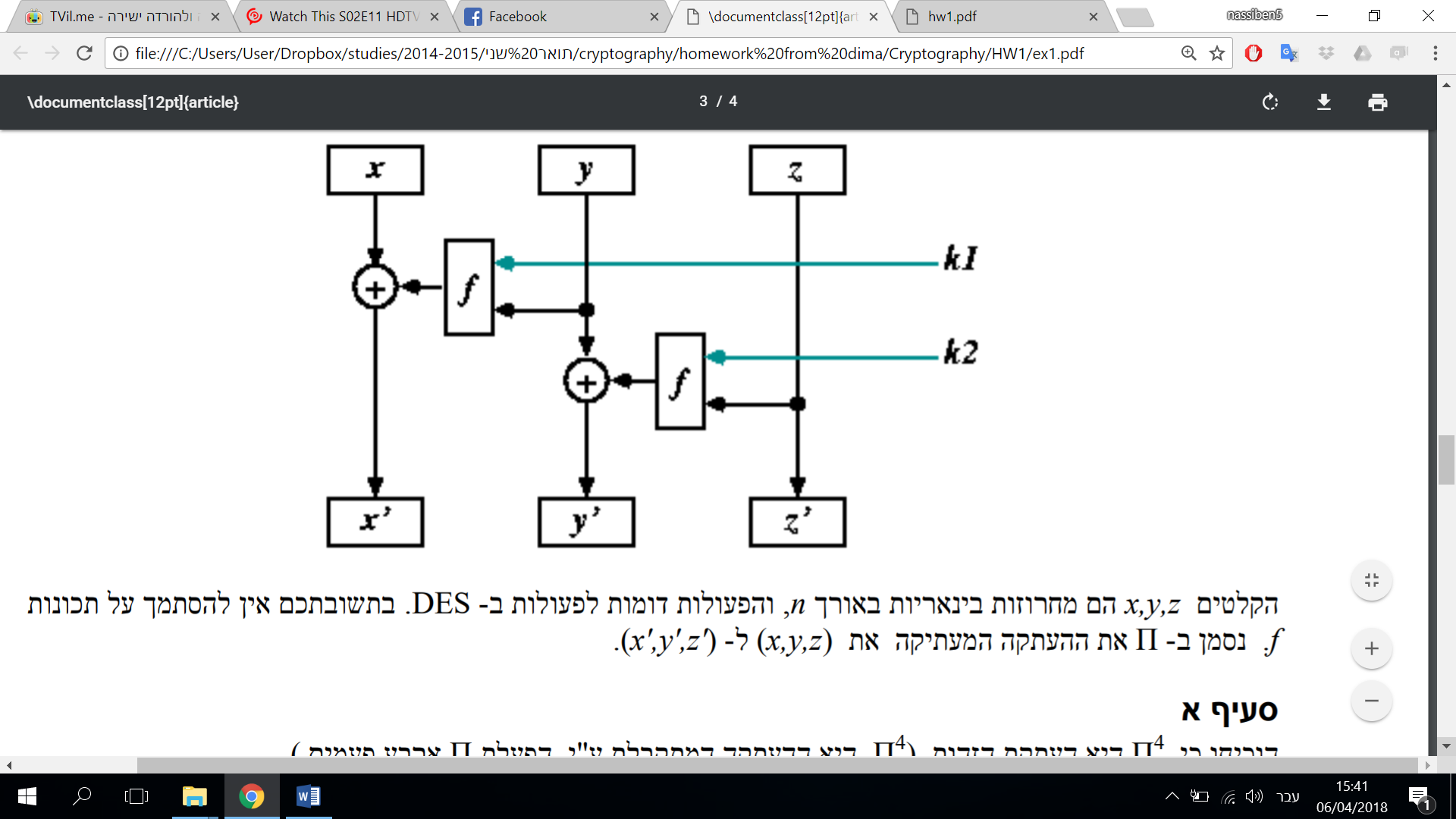
**הוראות הגשה**

* לעבודה יש שני חלקים.
* את החלק הראשון (WIRESHARK), אתם מתבקשים להגיש עד לתאריך 20/5/19 בשעה 23:00 במערכת מודל לתיבת ההגשה המתאימה.
* את החלק השני (קריפטוגרפיה), אתם מתבקשים להגיש עד לתאריך 10/4/19 בשעה 23:00 במערכת מודל לתיבת ההגשה המתאימה.
* יש להגיש את כל קבצי העבודה לתיבת ההגשה המיועדת במודל, מכווצים ב ZIP כאשר שם הקובץ מכיל את שתי הת.ז של בני הזוג מופרדים בקו תחתון. לדוגמא: ass1\_id1\_id2.zip
* שאלות על העבודה יש לשאול בפורום העבודה במודל.
* כל יום איחור יוריד 5 נקודות מציון העבודה.
* הארכות ינתנו רק במקרים מיוחדים.

**חלק ב' – קריפטוגרפיה**

**שאלה מס' 3 (15 נק'):**

1. נגדיר פונקציה כללית חדשה Δ ע"י (a,b,c) = b,c,a Δ. הוכיחו כי Δ3 היא פונקציית הזהות.   
   כלומר הוכיחו (a,b,c) = a,b,c Δ3 **(5 נק')**
2. התבונן בסכמה הבאה:



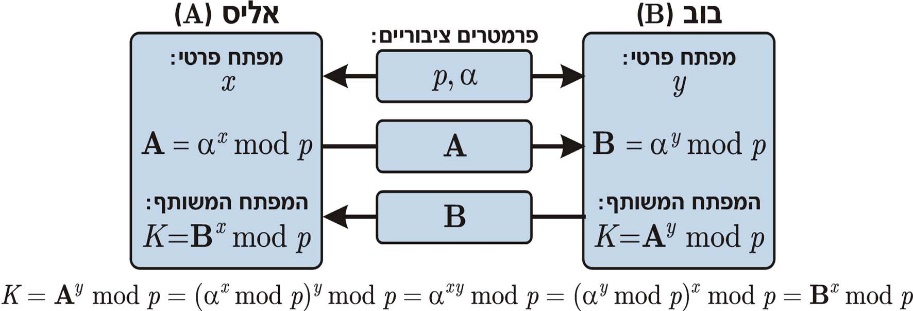
הקלטים x,y,z הם מחרוזות בינאריות באורך n, והפעולות דומות לפעולות ב – DES. בתשובתכם אין להסתמך על תכונות *f*. נגדיר את הסכמה למעלה ע"י הפונקציה x',y',z'=(x,y,z)π.

הוכיחו כי 4π היא פונקציית הזהות. כלומר הוכח x,y,z=(x,y,z) 4π. **(5 נק')**

1. אליס מגדירה מערכת הצפנה סימטרית ע"י 1πΔπ2Δ π3. בכל πj משתמשים במפתחות סיבוב *k1*j, *k2*j של הסיבוב ה-j. מהו אלגוריתם הפענוח המתאים למערכת של בוב? **(5 נק')**

**שאלה מספר 4 ( 20נק'):**

להלן סכמה של פרוטוקול דיפי הלמן כפי שתוארה במהלך הקורס:



1. תאר כיצד תוקף בעל יכולת Man in the middle יכול לתקוף את פרוטוקול Diffie-Hellman (DH). בתשובתך צייר תרשים המראה במדויק את סדר שליחת ההודעות (מיספור כרונולוגי של החיצים) והמניפולציה אשר באמצעותה מצליח התוקף ליישם את ההתקפה על הפרוטוקול (5 נק')

אליס ובוב מתכננים להחליף מפתחות באמצעות פרוטוקול DH, מאחר והפרוטוקול חשוף להתקפת Man in the middle סטודנט בקורס אבטחת מידע הציע להשתמש במנגנון זיהוי מבוסס (יפורט בהמשך). על כן, אליס ובוב פנו לשרת צד ג' אמין בדרישה להנפקת . שרת האמון הנפיק לאליס ולבוב שני אשר כל אחד מהם כולל מפתח פרטי ופומבי (זוג אחד לאליס והזוג השני לבוב).

**נגדיר את הסימונים הבאים:**

|  |  |
| --- | --- |
| **סימון** | **הגדרה** |
|  | ה – של אליס (המכיל את השם של אליס והמפתח הפומבי של אליס חתומים ע"י השרת אמון) |
|  | ה – של בוב (המכיל את השם של בוב והמפתח הפומבי של בוב חתומים ע"י השרת אמון) |
|  | החתימה של אליס על הודעה |
|  | החתימה של בוב על הודעה |
|  | מפתח סימטרי שהופק תוך שימוש בפרוטוקול DH |
|  | אלגוריתם ההצפנה שאליס ובוב עושים בו שימוש לאחר החלפת המפתחות |
|  | הצפנה של הודעה באמצעות אלגוריתם תוך שימוש במפתח ההצפנה |

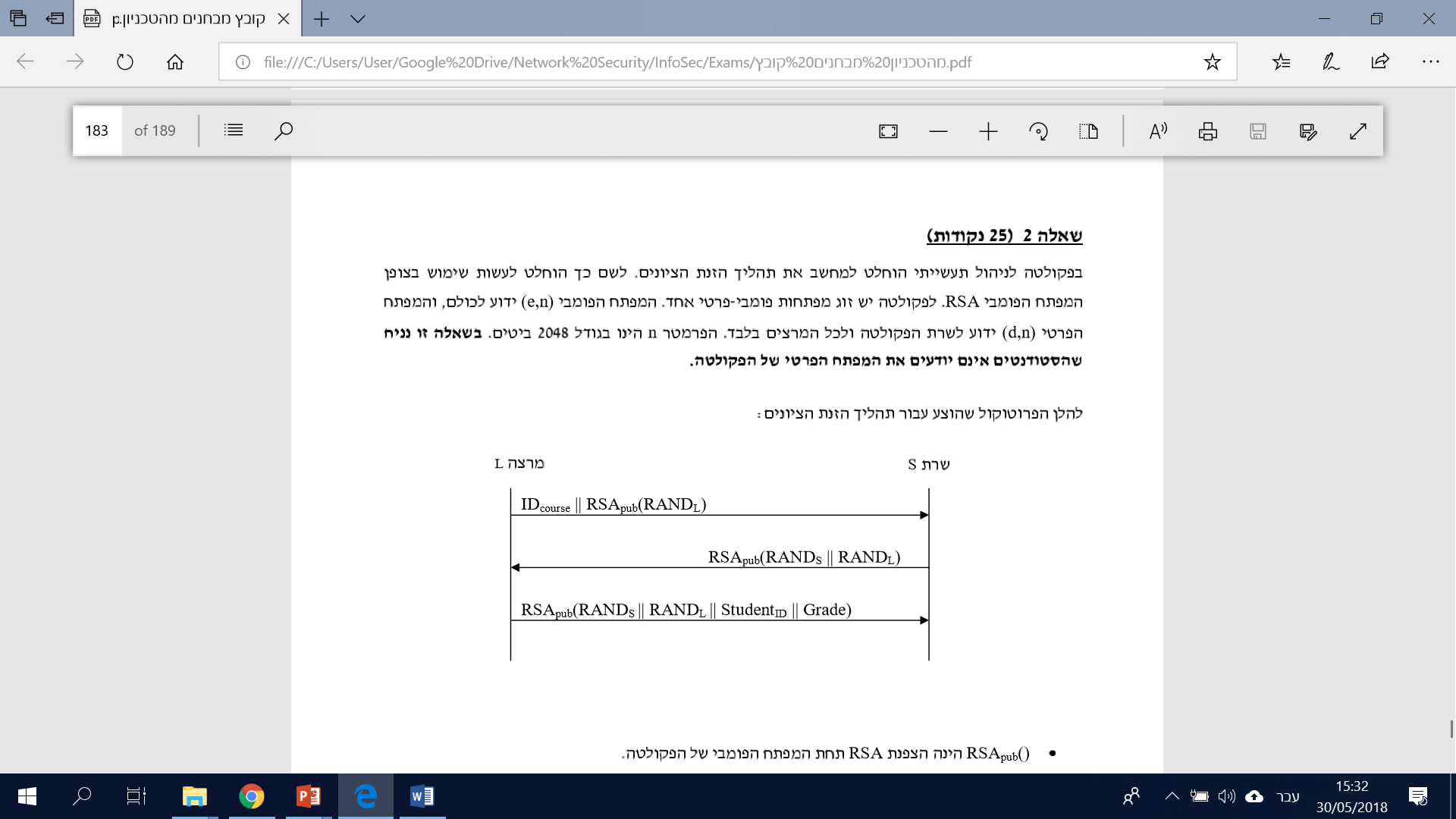
**להלן תיאור התהליך**

1. אליס ובוב יוצרים מפתח משותף תוך שימוש בפרוטוקול DH
2. אליס בוחרת מספר רנדומי ושולחת לבוב את ההודעה –
3. בוב בוחר מספר רנדומי ושולח לאליס את ההודעה –
4. אליס מוודא את ה – של בוב, במידה הווידוא הצליח היא שולחת לבוב את ההודעה –
5. בוב מוודא את ה – של אליס, במידה הווידוא הצליח הוא שולח לאליס את ההודעה –
6. אליס ובוב מוודאים את החתימות שהם קיבלו, במידה והווידוא הצליח הם ממשיכים בהתקשרות מוצפנת באמצעות המפתח
7. בהסתמך על סעיף א', תאר כיצד תוקף בעל יכולת Man in the middle יכול לתקוף את המנגנון אותו הציע הסטודנט. בתשובתך צייר תרשים המראה את תרשים של סדר שליחת ההודעות (מספור כרונולוגי) ואת המניפולציה אשר באמצעותה מצליח התוקף ליישם את ההתקפה על המנגנון אותו תיאר הסטודנט באופן בו הוא מצליח לקרוא את ההודעות מבלי שאליס ובוב מודעים לכך (10 נק').
8. כיצד ניתן לתקן את המנגנון אותו הציע הסטודנט ללא שינוי פרוטוקול DH **וללא הוספת שלבים נוספים למנגנון**. בתשובתך מנה את השינויים הנדרשים בהתייחסות לשלבי הפרוטוקול. בנוסף, צייר תרשים מעודכן של ההתקפה אותה תיארת בסעיף ב' והראה מדוע התקפה זו אינה ניתנת ליישום (5 נק').

**שאלה מספר 5 (15 נק'):**

בפקולטה לניהול תעשייתי הוחלט למחשב את תהליך הזנת הציונים. לשם כך הוחלט לעשות שימוש בצופן המפתח הפומבי RSA. לפקולטה יש זוג מפתחות פומבי - פרטי אחד. המפתח הפומבי (e,n) ידוע לכולם. המפתח הפרטי (d,n) ידוע לשרת הפקולטה ולכל המרצים בלבד. הפרמטר n הינו בגודל 2048 ביטים. בשאלה זו נניח שהסטודנטים אינם יודעים את המפתח הפרטי של הפקולטה.

להל הפרוטוקול שהוצע עבור תהליך הזנת הציונים:



1. RSApub() הינה הצפנת RSA תחת המפתח הפומבי של הפקולטה.
2. הנתון IDcourse הוא מספר באורך 128 ביטים המזהה את הקורס (למשל 094011). ניתן להניח שערכי ה-IDcourse של כל הקורסים ידועים לכולם.
3. הנתונים RANDL ו-RANDS הם מספרים אקראיים באורך 28 ביטים כל אחד שהמרצה והשרת מגרילים בכל הפעלה של הפרוטוקול.
4. הנתון StudentID הוא מספר שלם המזהה את הסטודנט ואורכו הוא 128 ביטים. כל מספר שלם הוא מספר זהות חוקי.
5. הנתון Grade הינו הציון (מספר שלם בין 0 ל 100), ואורכו הוא 128 ביטים.
6. אין הגבלה על מספר ההרצות של הפרוטוקול. אם לסטודנט מסוים מוזן הציון לקורס כלשהו יותר מפעם אחת, ציונו נקבע עפ"י הפעם האחרונה שבה הפרוטוקול הסתיים בהצלחה.
7. ניתן להניח שכל סטודנט יודע את ציונו בקורס ויודע מתי המרצה יזין את הציון לשרת.
8. ניתן להניח שכל סטודנט כבר האזין להזנות של ציוניו בלבד בקורסים אחרים.
9. הסבר כיצד השרת מוודא שאכן אחד המרצים הזין את הציון ולא אחד הסטודנטים **(5 נק')**.
10. הסטודנט מרכוס יודע שלא הצליח כל כך בקורס "אתיקה למהנדסים" שניתן בשנה ג' וכי ציונו הסופי שיוזן ע"י המרצה הוא 2 מתוך 100 (הציון הנמוך ביותר בתואר שלו). האם מרכוס יכול לבצע התקפת man in the middle להעלות את ציונו? אם כן תאר את ההתקפה היעילה ביותר שהוא יכול לבצע ונתח זמן ריצה וזיכרון. אחרת, נמק מדוע הפרוטוקול המוצע חסין להתקפות man in the middle. **(5 נק')**
11. הסטודנט שמואל הציע להתבסס על ניצול החולשה של אלגוריתם RSA לבעית הכפליות בפרוטוקול המוצע מעלה לטובת עדכון הציון. לטענתו ההתקפה הנ"ל משיגה את אותו האפקט ויעילה יותר מההתקפה של מרכוס. האם שמואל צודק? נמק/י **(5 נק')**

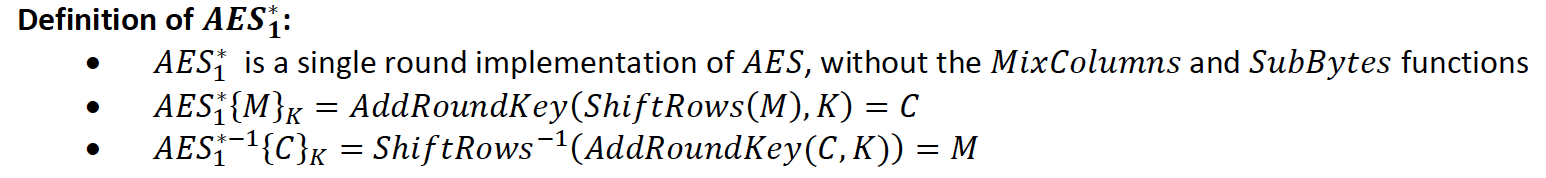
**שאלה מספר 6 (25 נק'):**

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

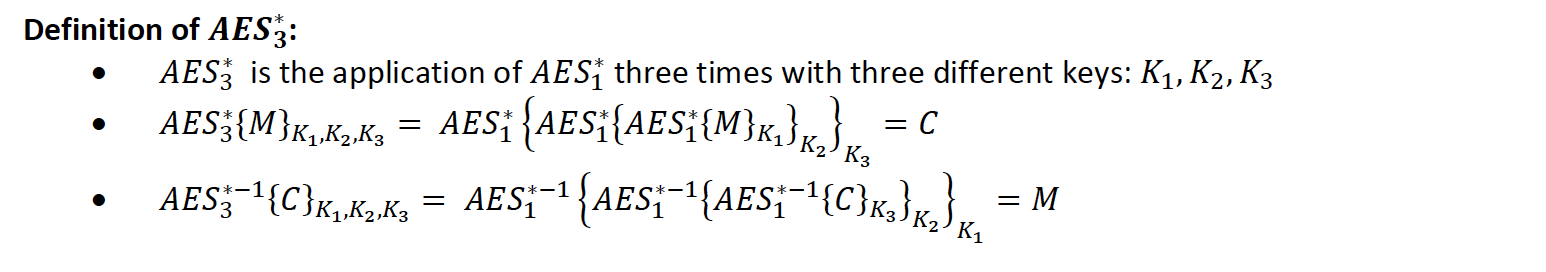
M – הודעה לא מוצפנת Plain-text

C – הודעה. מוצפנת Cipher-text

K – מפתח הצפנה/פענוח



ולכן הגדרה של היא:



בהינתן הודעה M והודעה מוצפנת C כך ש: , הנכם צריכים לממש שיטה יעילה למציאת 3 המפתחות K1,K2,K3 המקיימת: .

האלגוריתם הצפנה ממומש כך:

*C2*

*C1*

*M*

*C*

*3K 2K K1*

שימו לב כי במימוש שלכם לפריצה של עליכם להתייחס ל 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**

1. רשום פתרון תיאורטי לשיטה שאתה מציע **(5 נק')**.
2. ממש את הפתרון שהצעת ב- JAVA לפי הדגשים הבאים **(20 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 . 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>

Java –jar aes.jar –e –k key.txt –i message.txt –o cypther.txt

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

o –b : instruction to break the encryption algorithm

o –m <path>: denotes the path to the plain-text message

o –c <path>: denotes the path to the cipher-text message

o –o <path>: a path to the output file with the key(s) found.

o 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