20 באוגוסט 2021

אבטחת מידע 10313

<u>תרגיל 3</u>

יש להגיש לכל היאוחר עד: 6 בספטמבר 2021 בשעה 23:59

מרצה: ד"ר עמית קליינמן

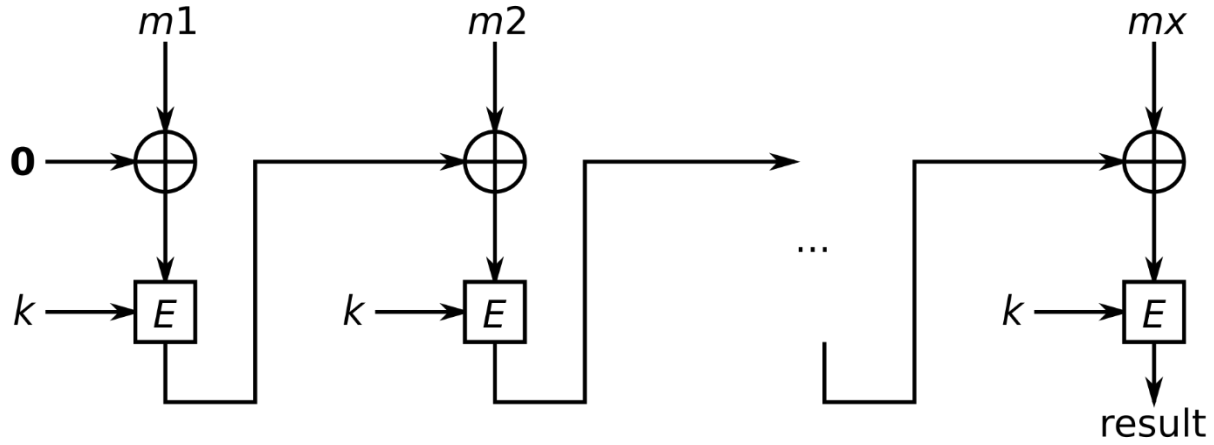
בודק: ערד פלד

1. מצא/י את השורשים הפרימיטיביים של 11 הסבר והראה את חישובך!

2. הדיאגרמה הבא מתארת טכניקה המכונה CBC-MAC ליצירת MAC ממצפין בלוקים. ההודעה מוצפנת עם אלגוריתם הצפנת בלוקים באופן CBC.

נתונים הפרמטרים <u>הפומביים</u> הבאים:
M ההודעה הגלויה המחולקת לבלוקים: m1, m2,…, mx
E פונקציית הצפנה סימטרית
⊕ פונקציית XOR
O בלוק IV כאשר כל הביטים שלו מאותחלים לערך אפס.
Result החתימה של m, להלן מסומנת כ: CBC-MAC(M, K)

נתון גם:
K מפתח סודי <u>הידוע רק לשולח ולמקבל של ההודעה (אליס ובוב)</u>.



אליס מחברת הודעה M = m1||m2||m3 המורכבת משלושה בלוקים (כאשר הסימן || מציין שרשור) ושולחת הן את M והן את CBC-MAC(M, K) <u>באופן לא מוצפן</u> לבוב.

א. מהו CBC ומה הוא מבטיח?
ב. ציינ/י שלוש מטרות אבטחה להן מספק המנגנון הנ"ל מענה. תאר את כל אחד מהמנגנונים הללו, מפני מה הם מגינים? הסבר!
ג. הסבר/י מהו IV (לא רק פירוש של הראשי תיבות, אלא גם הסבר מדוע הוא נדרש, מהו ומה תפקידו).
ד. רשום/רישמי ביטוי ל CBC-MAC(M, K) תוך שימוש בערכי: K, m_1, m_2, m_3, O ובפונקציות E ו- ⊕.
ה. מהי סדרת הפעולות שעל בוב לבצע כדי לאמת את ההודעה שהוא קיבל מאליס?

3. נשלחת במסגרת חילופי סטודנטים לאוניברסיטה בחו"ל. בהגיעך לשם את/ה מקבל הודעה שע"פ הנוהלים במקום האימיילים שלך יסרקו ויתכן שפרטיותך תפגע. לפיכך, את/ה מחליט/ה לדרוש מחבריך בישראל להצפין את כל האימיילים שישלחו אליך בהצפנת RSA ולשם כך את/ה בוחר/ת את הערכים הבאים: $p = 23$, $q = 5$ וכן: $e = 19$

א. איזו סוג הצפנה מממש אלגוריתם RSA?

ב. מדוע בחרת דווקא בהצפנת RSA? פיתרון לאיזו מטרת אבטחה עוזר RSA לממש מלבד שמירה על סודיות? הסבר/י!

ג. חשב/י את: Modulus n ו- $\phi(n)$, האם הערך שנבחר עבור e זר ל- $\phi(n)$? הסבר/י!

ד. מהו המפתח הפומבי שתפרסם לחבריך?

ה. מהו המפתח הפרטי שתשמור/רי לעצמך ? הראה/י את כל החישוב

ו. האם יש קשר מתמטי כלשהו בין המפתח הפומבי למפתח הפרטי? הסבר/י!

ז. חברך רוצים לשלוח אליך את ההודעה "אש" הנח/י שהאלפבית שלכם כולל את האותיות העבריות בלבד, ללא התו רווח, כאשר אין הבדל בין אות רגילה (כגון "מ") לאות סופית (כגון "ם"). לכמה בלוקים תחלק/י את ההודעה? מהו המסר המוצפן? השתמש/י בחישוב חזקות מהיר הראה/י את <u>כל</u> חישוביך

ח. קיבלת את ההודעה המוצפנת, לכמה בלוקים תחלק/י את ההודעה המוצפנת?

ט. נסמן באות C את אחד מהבלוקים במסר המוצפן. מהי הפונקצייה המתמטית שתפעיל כדי לפענח את C?.

4. פונקציות גיבוב:

במערכות בהם נשמרים חשבונות משתמש אין לשמור סיסמאות אלא סיסמאות מגובבות וממולחות.

א. מדוע טוב יותר לשמור סיסמאות מגובבות מאשר את הסיסמאות כשלעצמן?

ב. מדוע נדרש להמליח אותן?

ג. האם תוכל להפוך את ערך הגיבוב שלהלן? מהי הסיסמה המקורית? באיזו פונקציית גיבוב השתמשו?
ערך הגיבוב: 00225b3d0d8dd59287998962ba4bd9e01f6e8b7314d806474de84062e2c527fd

בהצלחה!