הרצאה 7 (המשך): הצפנה אסימטרית

נחזור לענייננו: הצפנה אסימטרית

- מטרה: ליצור מפתח משותף סודי על ערוץ פתוח

<u>בעיית הלוג הדיסקרטי:</u>

לפני הצגת הבעיה נגדיר:

- שדה גלואה מעל המספר הראשוני p: GF(p), המכיל מספרים:

  0, 1, 2, ..., p-1

- סגור תחת חיבור, חיסור, כפל במודולו p.
- מספר הופכי: לכל מספר a שונה מאפס בשדה ישנו מספר אחר (שלם חיובי) a^{-1} הנמצא בשדה כך ש: $a \cdot a^{-1} = 1 \; mod \; p$.
- למשל: $\mathrm{GF}(13) = \{0,1,\ldots,12\}$
  - פעולת חיסור: $5 - 12 = -7 + 13 = 6$
  - פעולת חיבור: $12 + 11 = 23 - 13 = 10$

בעיית הלוג הדיסקרטי

נגדיר איבר פרימיטיבי

- נתחיל בלהסביר על ידי דוגמה
- נסתכל על $GF(5) = \{0,1,2,3,4\}$, עם סדר שדה $p = 5$.
- נסתכל על חזקות $2^i,\ i = 0,1,\ldots$
- לפי המשפט הקטן של פרמה: $a^{p-1} = 1\ mod\ p$
- לפי פרמה נציב $a = 2,\ p = 5$ ונקבל: $2^4 = 1\ mod\ 5$
- כעת נשאל: האם $2^0, 2^1, \ldots, 2^{p-2}$ פורשים את כל איברי השדה מלבד איבר האפס?
- אם התשובה חיובית, אז 2 הוא איבר פרימיטיבי של $GF(5)$.
- נבדוק: $2^0 = 1\ ,\ 2^1 = 2\ , 2^2 = 4,\ 2^3 = 8\ mod\ 5 = 3$
- לכן 2 הוא איבר פרימיטיבי של $GF(5)$

בעיית הלוג הדיסקרטי

- האם 3 הוא איבר פרימיטיבי של GF(5)?
- נבדוק: $3^0 = 1$, $3^1 = 3$, $3^2 = 9 mod\ 5 = 4$, $3^3 = 27\ mod\ 5 = 2$
- לכן גם 3 הוא איבר פרימיטיבי של GF(5)
- האם 4 הוא איבר פרימיטיבי של GF(5)?
- נבדוק: $4^0 = 1$, $4^1 = 4$, $4^2 = 16 mod\ 5 = 1$
- לכן 4 אינו איבר פרימיטיבי של GF(5)
- <u>כעת לאחר שראינו את הדוגמה נגדיר</u>
- איבר פרימיטיבי α של GF(p) (לא בהכרח יחיד) הוא איבר בעל התכונה הבאה:
  $\alpha^i \bmod p,\ i = 0,1,\dots,p-2$ פורשים את כל איברי השדה השונים מאפס ב GF(p)

בעיית הלוג הדיסקרטי

- עובדה: לכל β שונה מאפס ששייך ל GF(p) קיים x כך ש

$$\alpha^x = \beta \bmod \mathrm{p}$$

- אם נתון α, x, p ניתן לחשב בקלות: $\beta = \alpha^x \bmod \mathrm{p}$
- לעומת זאת, כעת נציג את בעיית הלוג הדיסקרטי (בעיה בשלמים מודולו) שהיא בעיה קשה:
- נתונים $\alpha, \beta, \mathrm{p}$ יש למצוא x שלם בטווח $0 \le x \le p-2$ שפותר:

$$\alpha^x = \beta \bmod \mathrm{p}$$

- לא קיים אלגוריתם יעיל לפתרון הבעיה ועל זה מתבסס ההצפנה.
- כעת נלמד על תהליך דיפי הלמן (Diffi Hellman (DH)) ליצירת מפתח משותף על ערוץ פתוח בהתבסס על תובנה זו.

תהליך DH ליצירת מפתח משותף על ערוץ פתוח

- פרמטרים ידועים לכל העולם: α, p
- מפתחות פרטיים: x, y

Alice		Bob
מייצרת x אקראי $(0 < x < p - 1)$		מייצר y אקראי $(0 < y < p - 1)$
מחשבת $\beta = \alpha^x \bmod p$		מחשב $\gamma = \alpha^y \bmod p$
משדרת β לבוב	ערוץ פתוח	משדר γ לאליס
מחשבת $K_A = \gamma^x \bmod p$		מחשב $K_B = \beta^y \bmod p$

- טענה: $K = K_A = K_B$, ורק אליס ובוב יודעים את הערך הזה.
- K זהו המפתח המשותף לאליס ובוב
- x, y אלו מפתחות פרטיים

תהליך DH ליצירת מפתח משותף על ערוץ פתוח

- הוכחה ש: $K_A = K_B$:

$$K_A = \gamma^x = (\alpha^y)^x = \alpha^{yx} = (\alpha^x)^y = \beta^y = K_B$$

- הוכחה שרק אליס ובוב יודעים את K:
- נזכור כי α, p וגם $\beta = \alpha^x \bmod \mathrm{p}$, $\gamma = \alpha^y \bmod \mathrm{p}$ ידועים לכל העולם
- מספיק לדעת x או y כדי לחשב את K ולשבור את המערכת
- ברור שפעולת לוג דיסקרטי מחלצת את x מתוך $\beta = \alpha^x \bmod \mathrm{p}$ ואת y מתוך $\gamma = \alpha^y \bmod \mathrm{p}$ ושוברת את המערכת
- ההשערה של דיפי הלמן: לא ניתן לחשב את α^{xy} מתוך α^y, α^x ללא שימוש בפעולת לוג דיסקרטי
- קיבלנו שתחת השערת דיפי הלמן רק אליס ובוב יודעים את K

הוכחת זהות

- עדיין קיימת בעיה: איך ידעו אליס ובוב שהם אכן מדברים אחד עם השנייה? חסרה פה הוכחת זהות. נראה בהמשך פרוטוקול RSA שפותר זאת.
- לשם כך נצטרך רקע מתמטי נוסף
- פונקציית אוילר (Euler's Totient Function):
- $\phi(n)$ עבור n שלם וחיובי היא מספר המספרים השלמים החיוביים שקטנים מ n וזרים לו.
- דוגמה:
- עבור $n=12$, קיימים $1, 5, 7, 11$ ולכן $\phi(12) = 4$
- עבור $n=8$, קיימים $1, 3, 5, 7$ ולכן $\phi(8) = 4$
- עבור $n=5$, קיימים $1, 2, 3, 4$ ולכן $\phi(5) = 4$
- עבור $n=p$ *ראשוני*, $\phi(p) = p - 1$

הוכחת זהות

- משפט אוילר:

$$\alpha^{\phi(n)} = 1 \; mod \; n$$

עבור $a \neq 0$ וכן $(a\,,n) = 1$ (סימון ל GCD, כלומר $a\,,n$ זרים)

- מה מקבלים עבור n ראשוני?
- טענה:

עבור $a \neq 0$ וכן $(a\,,n) = 1$ נקבל: $a^x = \alpha^{x \; mod \; \phi(n)} \; mod \; n$

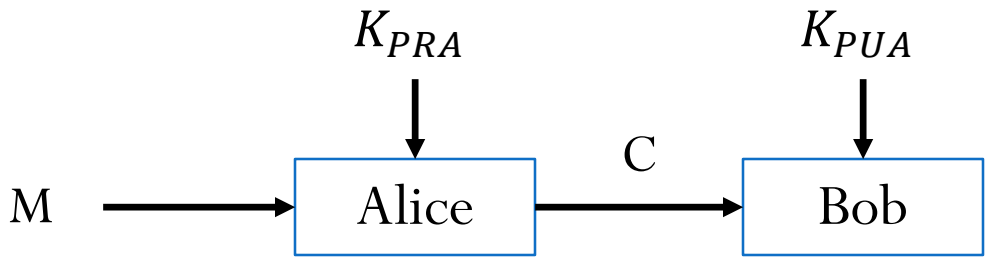
- בדומה למה שקיבלנו עבור פרמה הקטן: אם נציב $n = p$ ראשוני קיבלנו מפרמה: $\alpha^{p-1} = 1 \; mod \; p$ שגרר: $a^x = \alpha^{x \; mod \; p-1} \; mod$ p

אלגוריתם RSA

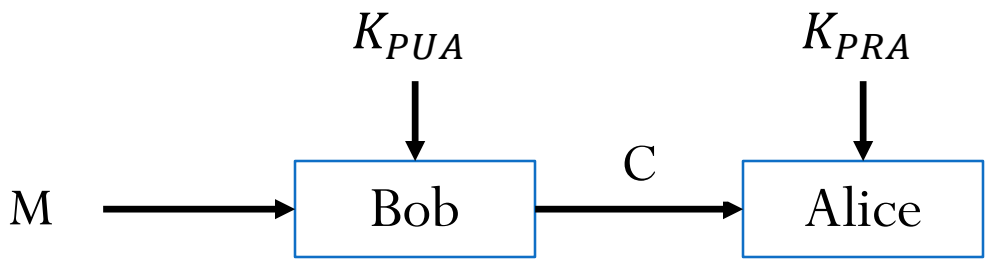
- אלגוריתם שפורסם בשנות ה 70 על ידי ריבסט, שמיר, ואדלמן
- יישום נפוץ מאד של הצפנה אסימטרית
- יישום נפוץ מאד לחתימה דיגיטלית בערוץ פתוח - משתמש מייצר חתימה שלו ולכל העולם יש יכולת לאשר את החתימה שלו מבלי היכולת לייצר את החתימה שלו
- נסמן:
- PU – ציבורי (public) , PR – פרטי (private)
- אליס תייצג את המשתמש , בוב ייצג נציג של העולם
- K_{PRA} - מפתח פרטי של אליס, ידוע רק לה
- K_{PUA} - מפתח ציבורי של אליס, ידוע לכל העולם
- דרישה - אי אפשר למצוא את K_{PRA} מתוך K_{PUA}

אלגוריתם RSA

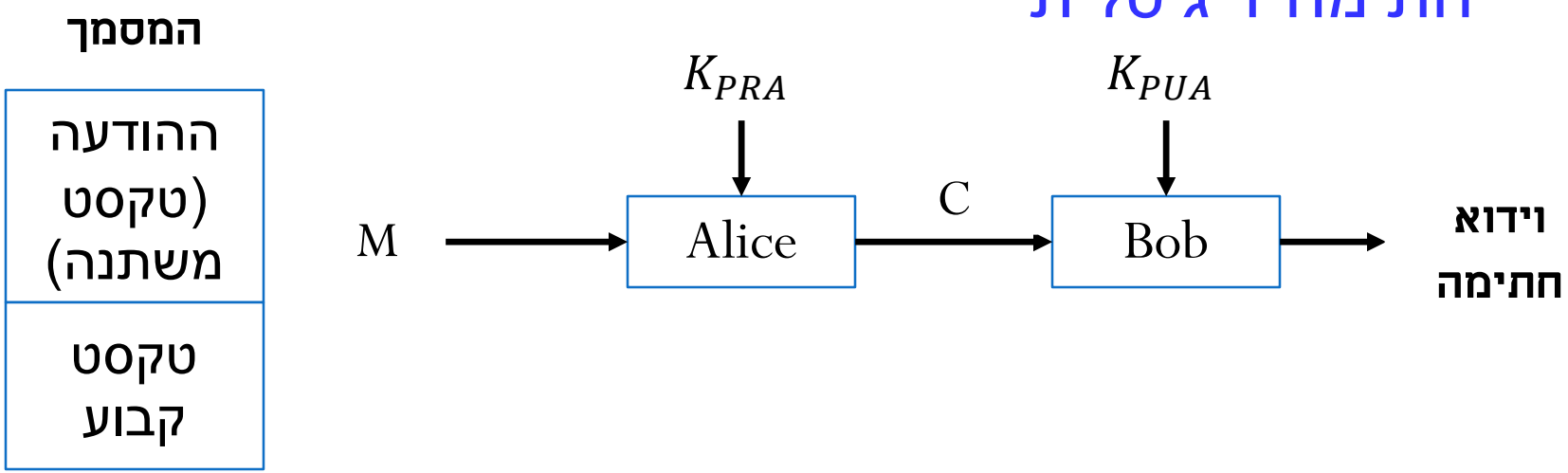
- נדון בשני סוגי תקשורת:
  - חתימה דיגיטלית – אליס נועלת את ההודעה ששולחת לעולם ואחר כך העולם פותח את ההודעה



  - הצפנה – העולם נועל את ההודעה ששולח לאליס ואחר כך אליס פותחת את ההודעה



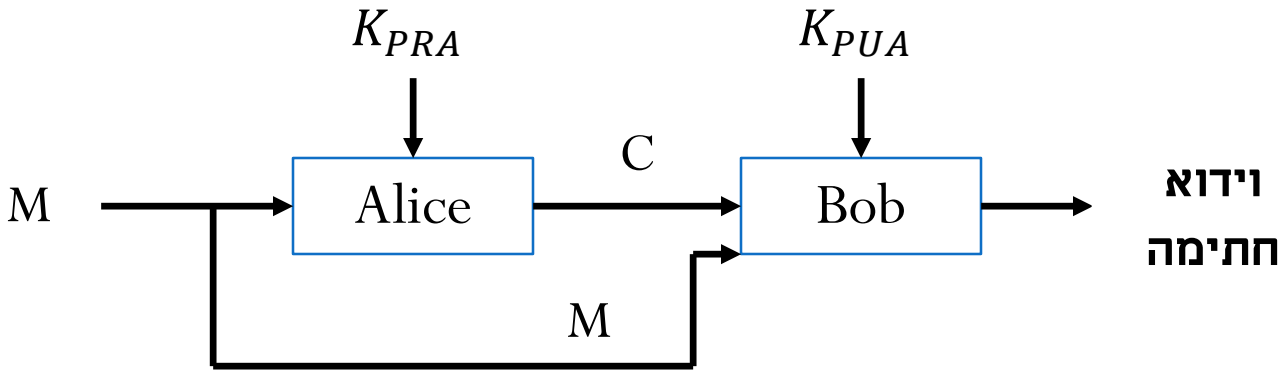
חתימה דיגיטלית



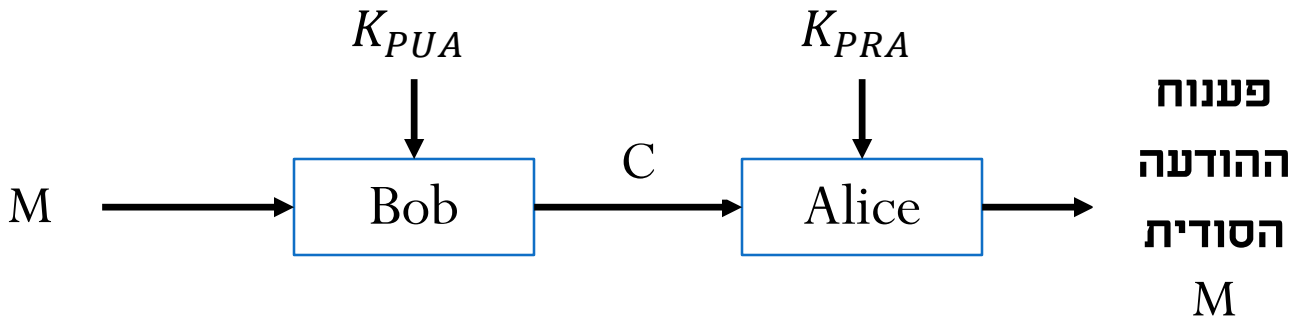
- אליס רוצה להוכיח לבוב את זהותה (שהיא זו שחותמת על המסמך)
- ההודעה לא סודית, רק דרושה הוכחת זהותה של אליס
- אליס נועלת את המסמך לפי המפתח הפרטי שלה
- שולחת את המסמך הנעול לבוב
- בוב משתמש במפתח הציבורי של אליס בשביל לפתוח את המסמך
- לאחר פתיחת המסמך בוב יחשוף את הטקסט הקבוע המוכיח את זהותה של אליס

חתימה דיגיטלית

- ואריאציה נוספת היא לשלוח את M בנוסף ל C:



הצפנה



- בוב משתמש במפתח הציבורי של אליס בשביל לנעול הודעה סודית המיועדת לאליס
- רק אליס יכולה לפתוח את ההודעה בעזרת המפתח הפרטי שלה
- בטיחות של RSA מתבסס על קושי פירוק לגורמים של מספר גדול (בעיית פקטוריזציה)

פקטוריזציה ב RSA

- נסמן p,q מספרים ראשוניים, נסמן את המכפלה $n = p \cdot q$
- נניח p,q לא ידועים, n ידוע
- אין שיטה יעילה למציאת p,q מתוך n , RSA מתבסס על עובדה זו

כעת נדון כיצד אליס מייצרת מפתח פרטי וציבורי

- אליס מייצרת שני מספרים ראשוניים p,q סודיים
- מחשבת את המכפלה $n = p \cdot q$
- מחשבת: $\phi(n) = (p-1) \cdot (q-1)$ (נוכיח בהמשך) ושומרת ערך בסוד
- מייצרת פרמטר ציבורי e בתחום $1 < e < \phi(n)$, זר ל $\phi(n)$
- מחשבת: $d = e^{-1} \; mod \; \phi(n)$
- מפיצה פרמטרים ציבוריים: e, n בערוץ פתוח (מפתח ציבורי)
- מפתח פרטי של אליס: d

פקטוריזציה ב RSA

- נוכיח כי $\phi(n) = (p-1)\cdot(q-1)$:
- בסך הכול המספרים הקטנים מ $n = p \cdot q$ או שווים לו:

$$\{1, 2, \ldots, p \cdot q\}$$

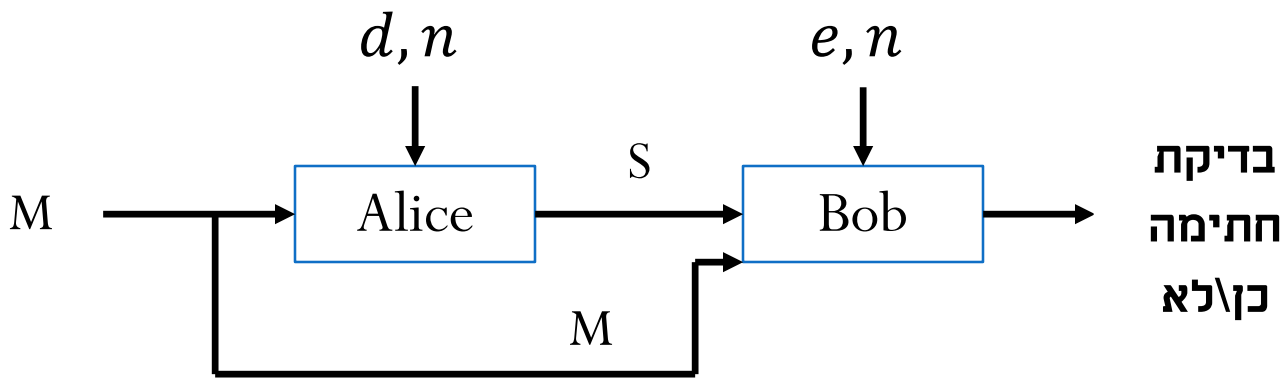
- נוריד כפולות של p או q שהם לא זרים ל $p \cdot q$:

$$|\{1 \cdot p,\ 2 \cdot p,\ \ldots, q \cdot p\}| = q$$

$$|\{1 \cdot q, 2 \cdot q,\ \ldots, p \cdot q\}| = p$$

- אבל הורדנו $p \cdot q$ פעמיים ולכן נוסיף 1
- בסך הכול נקבל: $\phi(n) = p \cdot q - p - q + 1 = (p-1)(q-1)$

ייצור חתימה ובדיקת חתימה ב RSA



- ייצור חתימה על ידי אליס: $S = M^d \bmod n \quad , \quad M < n$
- בדיקת חתימה על ידי בוב:
  - משתמש במפתח הציבורי e, n , בהודעה M (לא סודית), ובחותמת S
  - בודק האם השוויון הבא מתקיים: $S^e = M \bmod n$
  - שוויון מתקיים – החתימה אמיתית, שוויון לא מתקיים – החתימה לא אמיתית

ייצור חתימה ובדיקת חתימה ב RSA

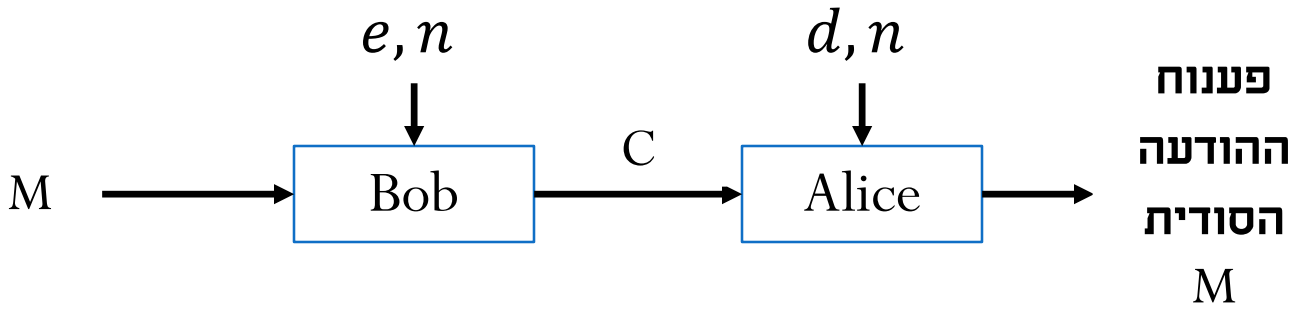
- הוכחת נכונות השיטה:
- נבדוק את הוכחת הזהות על ידי בוב:

$$S^e = (M^d)^e \; mod \; n$$

- מאוילר ידוע כי: $a^x = a^{x \; mod \; \phi(n)} \; mod \; n$
- ולכן: $S^e = (M^d)^e = M^{d \cdot e \; mod \; \phi(n)} \; mod \; n$
- ומכיוון ש $d = e^{-1} \; mod \; \phi(n)$ נקבל:

$$S^e = (M^d)^e = M^{d \cdot e \; mod \; \phi(n)} \; mod \; n = M \; mod \; n = M$$

הצפנה



- הצפנת ההודעה M על ידי בוב למסר מוצפן שרק אליס יכולה לפענח:

$$C = M^e \ mod \ n$$

- פענוח על ידי אליס:

$$M = C^d \ mod \ n$$

הצפנה

- הוכחת נכונות השיטה:
- נבדוק את הפענוח על ידי אליס:

$$C^d = (M^e)^d \; mod \; n$$

- מאוילר ידוע כי: $a^x = a^{x \; mod \; \phi(n)} \; mod \; n$
- ולכן: $C^d = (M^e)^d = M^{e \cdot d \; mod \; \phi(n)} \; mod \; n$
- ומכיוון ש $d = e^{-1} \; mod \; \phi(n)$ נקבל:

$$C^d = (M^e)^d = M^{e \cdot d \; mod \; \phi(n)} \; mod \; n = M \; mod \; n = M$$