# 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 $\alpha$ 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 $\beta$ שונה מאפס ששייך ל GF(p) קיים $x$ כך ש

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

- אם נתון $\alpha, x, \mathrm{p}$ 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: $\alpha$, p
- מפתחות פרטיים: $x$, y

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

- 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 $\alpha$, 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 $\alpha^{xy}$ מתוך $\alpha^x$,$\alpha^y$ 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:

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

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: $a^x = a^{x \; mod \; \phi(n)} \; mod \; n$

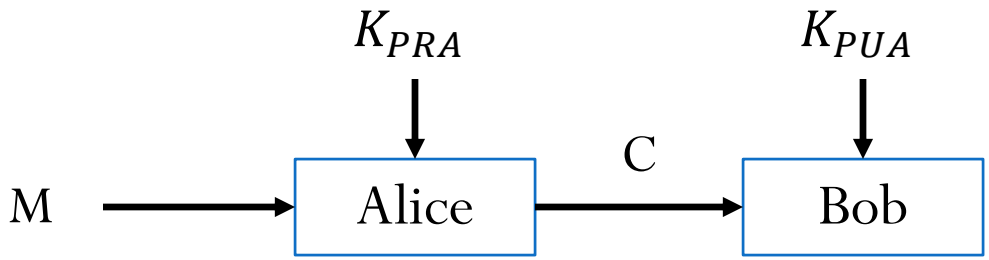
- בדומה למה שקיבלנו עבור פרמה הקטן: אם נציב $n = p$ ראשוני קיבלנו מפרמה: $a^{p-1} = 1 \; mod \; p$ שגרר: $a^x = a^{x \; mod \; p-1} \; mod$ p

# אלגוריתם RSA

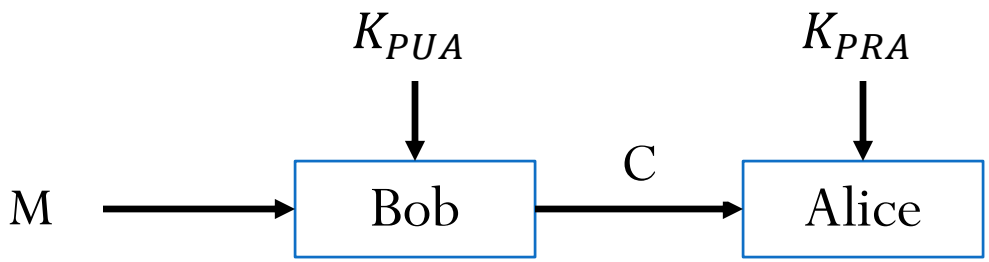
- אלגוריתם שפורסם בשנות ה 70 על ידי ריבסט, שמיר, ואדלמן
- יישום נפוץ מאד של הצפנה אסימטרית
- יישום נפוץ מאד לחתימה דיגיטלית בערוץ פתוח - משתמש מייצר חתימה שלו ולכל העולם יש יכולת לאשר את החתימה שלו מבלי היכולת לייצר את החתימה שלו
- נסמן:
- PU – ציבורי (public) , PR – פרטי (private)
- אליס תייצג את המשתמש , 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

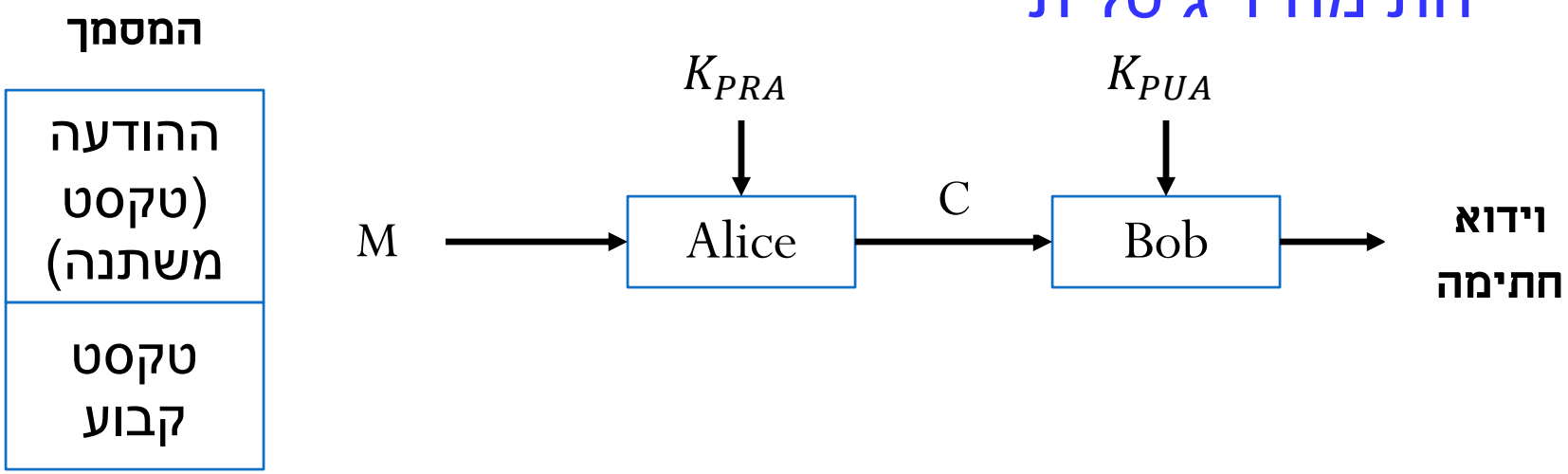
- נדון בשני סוגי תקשורת:
  - חתימה דיגיטלית – אליס נועלת את ההודעה ששולחת לעולם ואחר כך העולם פותח את ההודעה




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



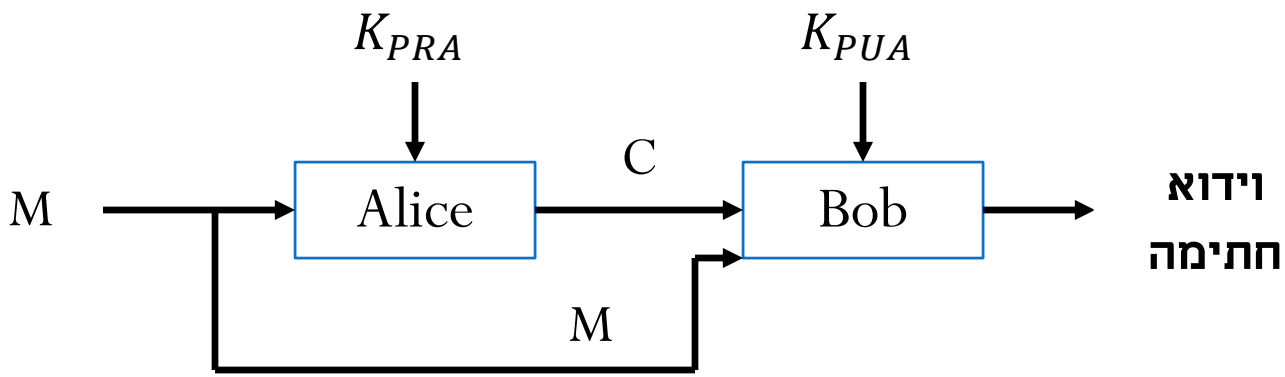
# חתימה דיגיטלית



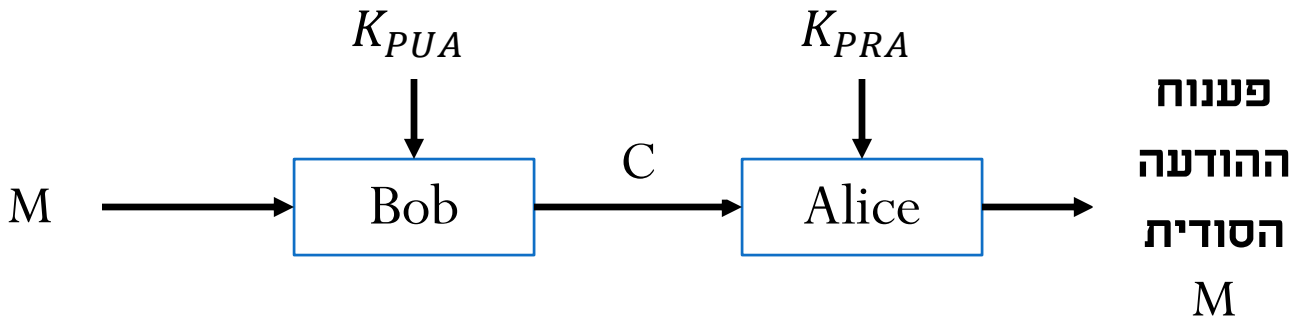

- אליס רוצה להוכיח לבוב את זהותה (שהיא זו שחותמת על המסמך)
- ההודעה לא סודית, רק דרושה הוכחת זהותה של אליס
- אליס נועלת את המסמך לפי המפתח הפרטי שלה
- שולחת את המסמך הנעול לבוב
- בוב משתמש במפתח הציבורי של אליס בשביל לפתוח את המסמך
- לאחר פתיחת המסמך בוב יחשוף את הטקסט הקבוע המוכיח את זהותה של אליס

# 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:

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

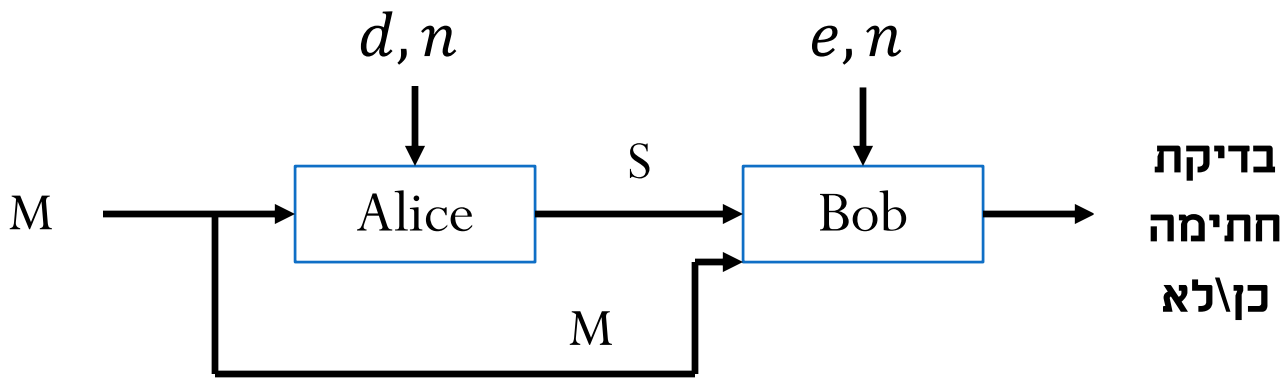
- נוריד כפולות של p או q שהם לא זרים ל $p \cdot q$:

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

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

- 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

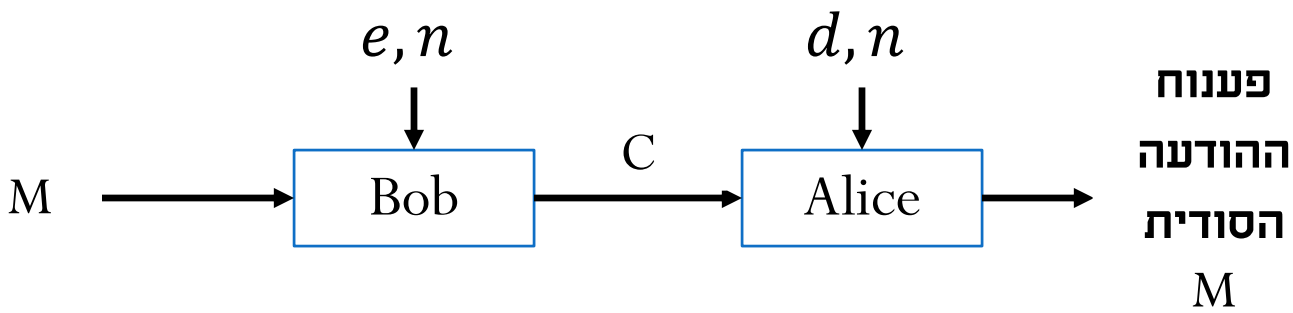
- הוכחת נכונות השיטה:
- נבדוק את הוכחת הזהות על ידי בוב:

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

- 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:

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

# הרצאה 8: בטיחות RSA

- נראה בשלילה שלא ניתן לגלות את d מתוך $e,n$
- דרך א' – נגלה את $\phi(n)$ מתוך $n$ ואז נחשב $d = e^{-1} \; mod \; \phi(n)$
  - נרשום את $\phi(n)$:

$$\phi(n) = (p-1)(q-1) = pq - (p+q) + 1$$

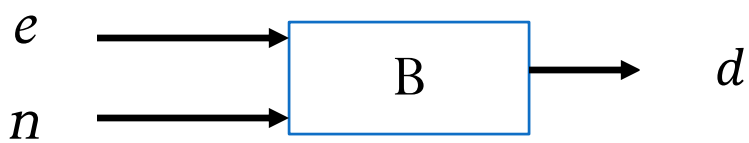
  - נניח בשלילה שישנו אלגוריתם A כך ש:

$$n \longrightarrow \boxed{\text{A}} \longrightarrow \phi(n) = pq - (p+q) + 1$$

  - אבל אז נוכל לחלץ את $p,q$ ולכן לא יתכן שנגלה את $\phi(n)$ (בעיית פקטוריזציה)

# בטיחות RSA

- דרך ב' – נגלה את $d$ מתוך $e,n$
  - נניח בשלילה שישנו אלגוריתם B שמחשב $d = e^{-1} \bmod \phi(n)$ מתוך $e,n$:




  - אם כן, נוכל לייצר הרבה $e_i$ להכניס לאלגוריתם B ולקבל $d_i$ מתאים
  - נקבל הרבה זוגות $e_i,d_i$ כך ש

$$d_i = e_i^{-1} \bmod \phi(n)$$

ולכן: $$d_i \cdot e_i = 1 \bmod \phi(n)$$

ולכן: $$d_i \cdot e_i - 1 = m_i \phi(n)$$

  - אבל אז נוכל לחלץ את $\phi(n)$ וזה לא יתכן (בעיית פקטוריזציה)
- דרך ג' – נגלה את $d$ מתוך $S = M^d \bmod n$
  - לא יתכן (בעיית לוג דיסקרטי)

# דרישה ל $M, n$ זרים ב RSA

- נזכור שהשתמשנו באוילר שדורש $M, n$ זרים כאשר $M < n$
- נראה שההסתברות ש $M, n$ לא יהיו זרים זניחה ב RSA
- כל M זר אפשרי ל $n$ שנבחר חייב להיות באחת הקבוצות:

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

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

- כלומר יש לנו פחות מ $q+p$ מסרים אבודים
- ולכן ההסתברות ש $M, n$ אינם זרים קטנה מ $\frac{p+q}{p \cdot q}$
- עבור $p$ ו $q$ טיפוסיים בגודל 512 ביט נקבל הסתברות $\frac{2^{513}}{2^{1024}} = 2^{-511}$
- הסתברות קטנה מאד

# אלגוריתם מילר-רבין למציאת $p, q$ ראשוניים ב RSA

- ב RSA אליס צריכה למצוא $p, q$ ראשוניים
- לשם כך משתמשים באלגוריתם מילר רבין
- האלגוריתם עושה שימוש בלמה של אוקלידס
- הלמה של אוקלידס:
  - נניח $p$ ראשוני, ו $a, b$ שלמים
  - אם משתנה ראשוני $p$ מחלק את המכפלה $a \cdot b$ , אזי $p$ מחלק לפחות לפחות את אחד המספרים $a$ או $b$

# הלמה של אוקלידס - דוגמאות

- דוגמה ליישום הלמה:
  - נניח $a = 56, b = 17$ , $p = 7$
  - נקבל: $56 \cdot 17 = 952 = 0 \; mod \; 7$
  - כלומר 7 מחלק את המכפלה $56 \cdot 17$ וגם מחלק את $56 = 7 \cdot 8$
- דוגמה נגדית:
  - נניח $p = 10$ (לא ראשוני), $a = 4, b = 15$
  - נקבל: $4 \cdot 15 = 60 = 0 \; mod \; 10$
  - כלומר 10 מחלק את המכפלה $4 \cdot 15 = 60$ אבל לא מחלק את 4 ולא מחלק את 15

# רעיון אלגוריתם מילר-רבין

- נניח ש $x$ הוא שורש ריבועי של *1* מודולו $p$

לכן: $x^2 = 1 \; mod \; \mathrm{p}$

ולכן: $x^2 - 1 = 0 \; mod \; \mathrm{p}$

ולכן: $(x-1)(x+1) = 0 \; mod \; \mathrm{p}$ (*)

- נשים לב כי במשוואה (*), $p$ ראשוני והוא מחלק את $(x-1)(x+1)$
- לכן לפי הלמה של אוקלידס

$x - 1 = 0 \; mod \; p$ או $x + 1 = 0 \; mod \; p$

- כלומר: $x = \pm 1 \; mod \; p$

# רעיון אלגוריתם מילר-רבין

- כעת נניח $p$ ראשוני , $p > 2$
- לכן $p - 1$ זוגי וניתן לרישום כך: $p - 1 = 2^s \cdot d$
  עבור $s, d$ שלמים, $d$ אי זוגי
  - למשל: $p = 29$ ראשוני ונוכל להציב $s = 2, d = 7$ ולרשום
    $p - 1 = 28 = 2^2 \cdot 7$
- כעת נשתמש במשפט הקטן של פרמה: $a^{p-1} = 1 \; mod \; p$ עבור $p$ ראשוני
- נציב $p - 1 = 2^s \cdot d$ בפרמה ונקבל: $a^{2^s \cdot d} = 1 \; mod \; p$
- ואפשר לרשום: $(a^{2^{s-1} \cdot d})^2 = 1 \; mod \; p$
- ולפי הלמה של אוקלידס נקבל: $a^{2^{s-1} \cdot d} = \pm 1 \; mod \; p$

# רעיון אלגוריתם מילר-רבין

- קיבלנו אפשרות אחת: $a^{2^{s-1}\cdot d} = -1 \; mod \; p$

אפשרות שנייה: $a^{2^{s-1}\cdot d} = (a^{2^{s-2}\cdot d})^2 = 1 \; mod \; p$

- נמשיך ונקבל:

אפשרות אחת: $a^{2^{s-2}\cdot d} = -1 \; mod \; p$

אפשרות שנייה: $a^{2^{s-2}\cdot d} = (a^{2^{s-3}\cdot d})^2 = 1 \; mod \; p$

- וכן הלאה..
- לסיכום נקבל:
- אפשרות אחת: $a^{2^{r}\cdot d} = -1 \; mod \; p \; , \; \text{for some} \;\; 0 \le r \le s-1$

אפשרות שנייה: $a^{d} = 1 \; mod \; p$

# אלגוריתם מילר-רבין לבדיקת $p$ ראשוני

- $p\_indicator = 1$
- חזור $T$ פעמים $(i = 1 \text{ to } T)$

1) בחר $a$ ובדוק האם מתקיים:

$$a^{2^r \cdot d} \neq -1 \; mod \; p \; , \; \text{for all} \;\; 0 \leq r \leq s-1$$

וגם:

$$a^d \neq 1 \; mod \; p$$

2) אם מתקיים, אז $p$ לא ראשוני $(p\_indicator = 0)$ וצא מהלולאה

- אם רצנו על כל הניסויים ולא יצאנו מהלולאה $(p\_indicator = 1)$ נסיק מכך ש p ראשוני בהסתברות גבוהה (עדיין יש סיכוי שקיים a שלא בחרנו וכן מקיים את התנאי בשורה 2)
- ככל שנגדיל את $T$ נוריד את ההסתברות לשגיאה

# אלגוריתם מילר-רבין לבדיקת $p$ ראשוני

- טענה:

לכל ניסוי בלולאה יש הסתברות שגיאה של 1/4. כלומר אנו חושבים ש p ראשוני כשעברנו את המבחן (כלומר המשכנו בלולאה) אך הוא לא ראשוני.

- מסקנה:

הסתברות השגיאה של המבחן היא: $(1/4)^T = 2^{-2T}$

- הסתברות השגיאה קטנה אקספוננציאלית עם מספר הניסויים. נוכל לבחור $T$ מספיק גדול שיבטיח מערכת בטוחה

- סיבוכיות:
  - בחישוב נאיבי: סיבוכיות $O\left(\sqrt{p}\right)$ לפתרון וודאי
  - במילר-רבין מבצעים העלאה בחזקה $T$ פעמים, נקבל סיבוכיות $O(T\log^3(p))$ - יעיל יותר, אך הפתרון בעל הסתברות שגיאה שיורדת אקספוננציאלית עם $T$

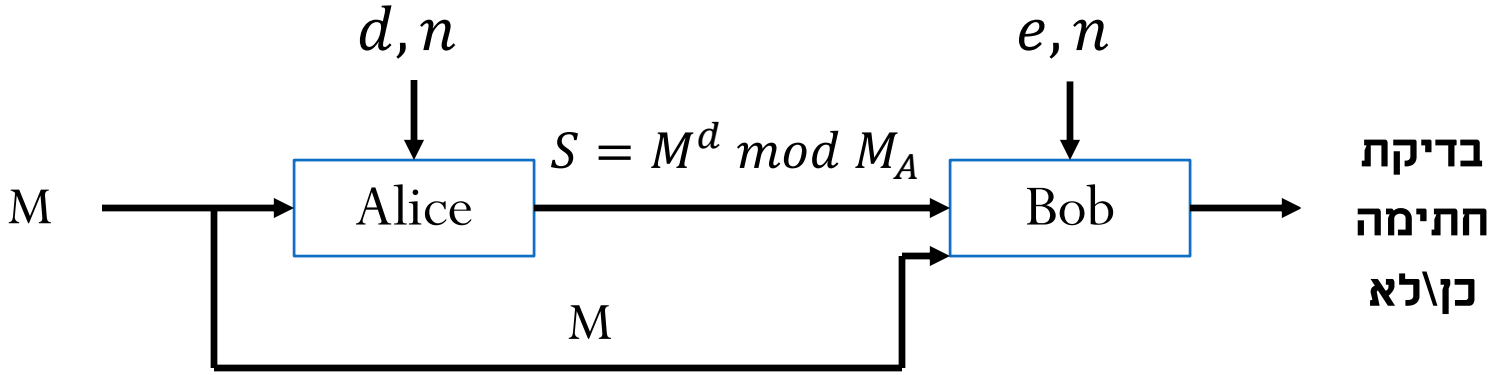
# אלגוריתם מילר-רבין לבדיקת $p$ ראשוני - דוגמה

- דוגמה:
- נבדוק אם $p = 221$ ראשוני
- $p - 1 = 220 = 2^2 \cdot 55 \Rightarrow s = 2, d = 55$
- ניסוי ראשון:
  - נבחר באקראי $1 < a < p - 1$ , נניח $a = 174$
  - נבדוק תנאי ראשון: $a^{2^r \cdot d} \neq -1 \; mod \; p$ , for all $0 \leq r \leq s - 1$
    - עבור $r = 0$ נקבל: $a^{2^0 \cdot d} \; mod \; p = 174^{55} \; mod \; 221 = 47 \neq 1$
    - עבור $r = 1$ נקבל:
      $a^{2^1 \cdot d} \; mod \; p = 174^{110} \; mod \; 221 = 220 = p - 1 = -1$
    - כלומר ממשיכים לעוד ניסוי
  - נבדוק תנאי שני (לשם תרגול): $a^d \neq 1 \; mod \; p$
    - נקבל: $174^{55} \; mod \; 221 = 47 \neq 1$

# אלגוריתם מילר-רבין לבדיקת $p$ ראשוני - דוגמה

- ניסוי שני:
  - נבחר באקראי $1 < a < p - 1$ , נניח $a = 137$
  - נבדוק תנאי ראשון: $a^{2^r \cdot d} \neq -1 \; mod \; p$ , for all $0 \leq r \leq s - 1$
    - עבור $r = 0$ נקבל: $a^{2^0 \cdot d} \; mod \; p = 137^{55} \; mod \; 221 = 188 \neq 1$
    - עבור $r = 1$ נקבל: $a^{2^1 \cdot d} \; mod \; p = 137^{110} \; mod \; 221 = 205 \neq -1$
  - נבדוק תנאי שני: $a^d \neq 1 \; mod \; p$
    - נקבל: $137^{55} \; mod \; 221 = 188 \neq 1$
  - מסקנה: $p = 221$ אינו ראשוני
  - אם היינו עוצרים לאחר ניסוי ראשון הייתה שגיאה

# חתימה על מסר ארוך ב RSA

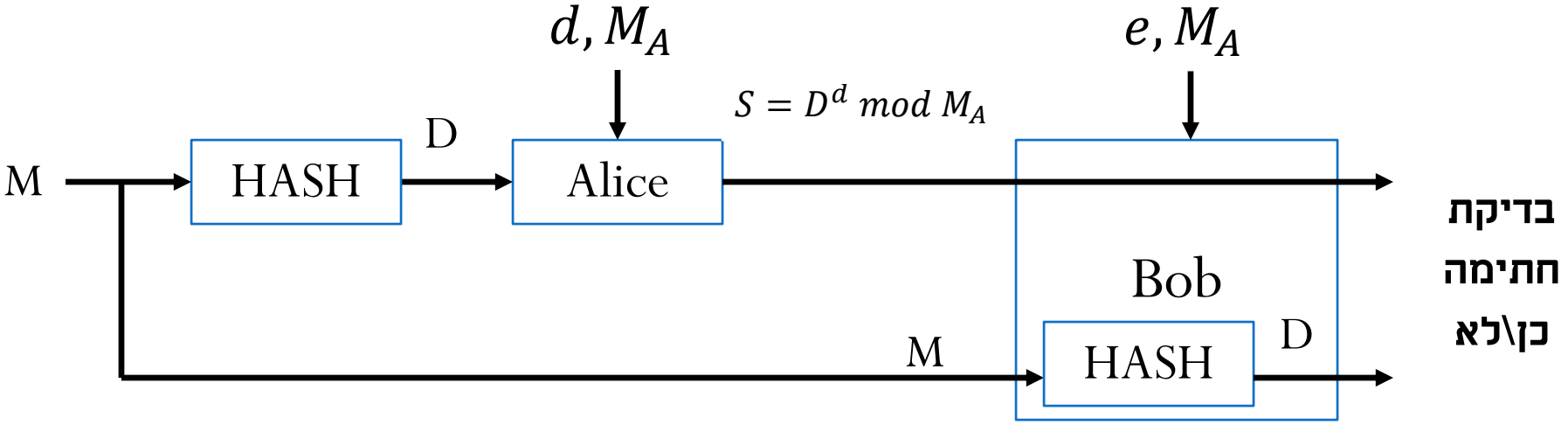



- בעבר ניתחנו את הארכיטקטורה מעלה לחתימה למסר קצר: $M < M_A$
- בשביל לחתום על מסר ארוך $M > M_A$ נבצע גיבוב (hashing):


- דרישה: לא ניתן לחשב הופכי מהמצב הדחוס ל $M$
- תקן ל HASH : Secure HASH Algorithm 1 (SHA1)

# חתימה על מסר ארוך ב RSA

- עבור חתימה ארוכה נבצע RSA כך:




- כעת אליס חייבת לשלוח את המסר $M$

# התקפת יום הולדת

- רקע – בעיית\פרדוקס יום ההולדת:
- נניח קבוצה של 23 אנשים
- מה הסיכוי שלפחות שני אנשים חוגגים יום הולדת באותו היום?
- ההסתברות שכל אחד נולד ביום שונה:

$$P = 1 \cdot \left(1 - \frac{1}{365}\right) \cdot \left(1 - \frac{2}{365}\right) \cdot \left(1 - \frac{3}{365}\right) \cdots (1 - \frac{22}{365}) < 0.5$$

- לכן ההסתברות שלפחות שני אנשים חוגגים יום הולדת באותו היום גדולה מ 0.5
- זוהי המחשה לעובדה הבאה: אם נבחר ערכים בעלי סיכוי שווה מבין $n$ אפשרויות, אז נקבל חזרות בהסתברות גבוהה לאחר שנבחר סדר גודל של $\sqrt{n}$ אפשרויות

# התקפת יום הולדת

- נוכיח:
- זורקים $m$ כדורים (אנשים) באקראי ל $n$ תאים (ימי הולדת אפשריים)
- ההסתברות ש $m$ הכדורים ייפלו לתאים שונים:

$$P = 1 \cdot \left(1 - \frac{1}{n}\right) \cdot \left(1 - \frac{2}{n}\right) \cdot \left(1 - \frac{3}{n}\right) \cdots \left(1 - \frac{m-1}{n}\right)$$

- נשתמש בחסם $1 - x < e^{-x}$ ונקבל:

$$P < e^{-1/n} e^{-2/n} \cdots e^{-\frac{m-1}{n}} = e^{-\frac{1}{n}(1+2+\cdots+m-1)} = e^{-\frac{m(m-1)}{2n}} \approx e^{-\frac{m^2}{2n}}$$

- לכן עבור $m = \sqrt{2Kn}$ (עבור $K$ איזה קבוע) נקבל: $P \approx e^{-K}$
- לכן ההסתברות $1 - P$ שנקבל חזרות שואפת ל 1 עם הגדלת $K$

# זיוף חתימה

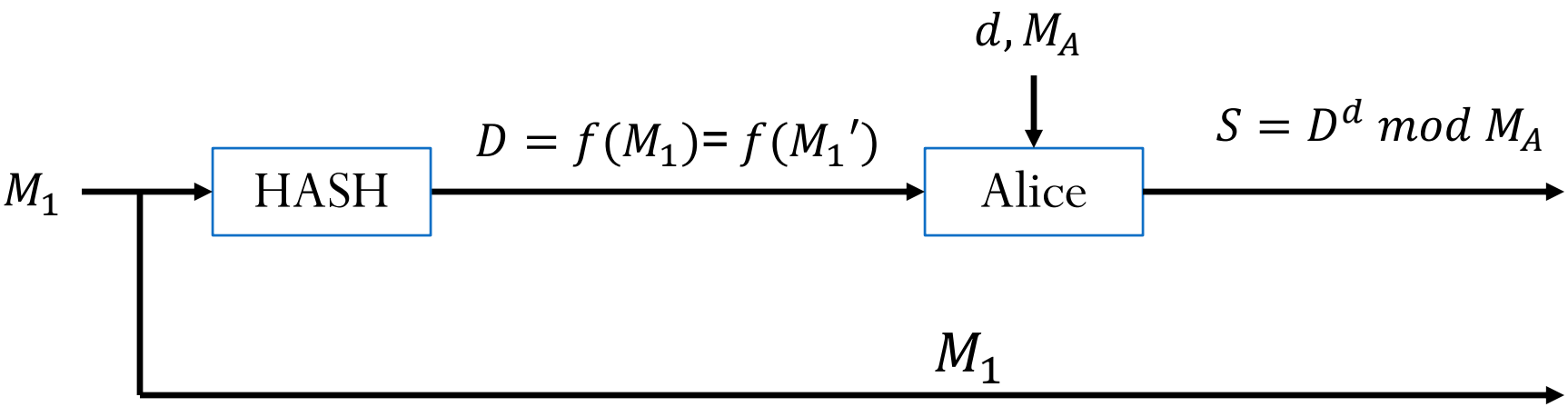
- תזכורת:
- בחתימה דיגיטלית המסר $M$ נדחס באמצעות פונקציית גיבוב, נסמנו $f(M)$ ואז חותמים $f(M)$ בעזרת מפתח סודי
- מבנה ההתקפה:
- התוקף מכין חוזה אמין $M$ וחוזה מזויף $M'$
- התוקף מכניס שינויים קטנים ל $M$ אך עדיין שומר על אמינות תוכן המסמך
  - לכן לתוקף מספר גדול של מסמכים אמינים ששקולים ל $M$ מבחינת התוכן
- התוקף מכניס שינויים קטנים גם ל $M'$ אך עדיין שומר על תוכנו המזויף
  - לכן לתוקף מספר גדול של מסמכים ששקולים ל $M'$ מבחינת התוכן המזויף

# זיוף חתימה

- התוקף מפעיל פונקציית גיבוב על כל המסמכים עד שמוצא

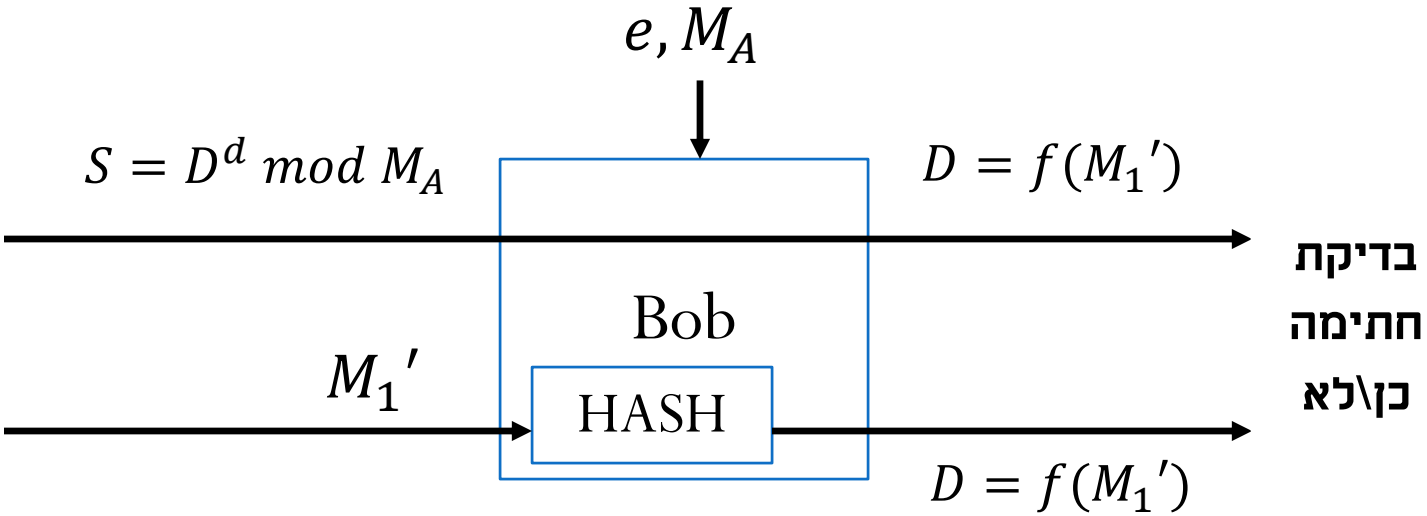
$$f(M_1)=f(M_1')$$

- צריך לשם כך סדר גודל של $\sqrt{\text{size of hashing output}}$ זוגות מסמכים
- התוקף מראה את מסמך $M_1$ הנבחר (שהוא אמין מבחינת תוכנו) לאליס שמבצעת גיבוב וחותמת עליו:



# זיוף חתימה

- התוקף מצמיד את החתימה ל $M_1{}'$ :




- נקבל שבוב מאמת שאליס חתמה על המסמך המזויף $M_1{}'$

# הגנה נגד זיוף חתימה

- פתרון 1: נשתמש בגיבוב במספר ביטים מספיק גדול כדי להקשות על התוקף
  - $2^{80}$ מסמכים הדרושים לזיוף נחשבת למערכת בטוחה
  - לכן נשתמש בפונקציית גיבוב של 160 ביט
- פתרון 2: אליס יכולה להכניס שינויים קלים למסמך לפני שחותמת ואז:

$$f(\text{modified } M_1 \text{ that Alice singed}) \neq f(M_1')$$