<u>**יסודות הקריפטוגרפיה תרגול 6#**</u>

מבחני ראשוניות:

<u>מבחן פרמה</u>:

מתבסס על משפט פרמה הקטן:

- אם n ראשוני אז לכל $a \in \mathbb{Z}_n^*$ מתקיים: $a^{n-1} = 1 (\mathrm{mod}\, n)$.
- אם n לא ראשוני אז נוכל להגיד שיש הרבה a-ים כאלה שעבורם לא מתקיים התנאי לעיל.

אבל זה לא נכון, למשל מספרי קרמייקל. לכן לא משתמשים במבחן זה.

<u>מבחן מילר-רבין</u>:

- אם n ראשוני: לכל $a \in \mathbb{Z}_n^*$ מתקיים שאם $a^2 = 1$ אז $a = \pm 1$.
- אם n לא ראשוני אז במקרה זה יש הרבה, $\frac{3}{4}$ לפחות, a-ים כך ש- $a^2 = 1$ וגם $a \neq \pm 1$.

מספרים ראשוניים צריכים לצאת תמיד ראשוניים, ואם הם לא ראשוניים הם צריכים להתפס ככאלה בסיכוי טוב. הטעות של אלגוריתם זה ואחרים הוא לכיוון שאם n לא ראשוני התשובה לא בטוחה (אם הוא ראשוני תמיד יוחזר תשובת אמת).

<u>מבחן *LUCA*</u>:

- אם n ראשוני: קיים $a \in \mathbb{Z}_n^*$ שיוצר אותו, כלומר $ord(a) = n - 1$. זה מתבסס על הוכחה שראינו, שלכל שדה ראשוני יש שורש פרמיטיבי.
  אם n ראשוני אז יש בדיוק $n - 1$ איברים וזה סדר החבורה. האמת שיש הרבה איברים שמקיימים זאת, ליתר דיוק $\phi(n-1)$ איברים.
- אם n לא ראשוני: לכל $a \in \mathbb{Z}_n^*$ מתקיים: $ord(a) < n - 1$, כי $\phi(n) < n - 1$ - הסדר לא יכול להיות יותר גדול מגודל החבורה.

במקרה זה הבדיקה הפוכה מאשר מילר-רבין: עבור בדיקת ראשוניות בודקים "קיים", עבור בדיקת אי ראשוניות בודקים "לכל". אלגוריתם זה צודק תמיד על לא ראשוניים ועלול לטעות עבור ראשוניים, הפוך ממילר-רבין.

אם כן, איך בודקים האם $ord(a) = n - 1$? הכפלה מרובה היא פעולה כבדה. אם היינו יודעים את הפירוק של $n - 1$ לגורמים ראשוניים אז היינו יכולים לבדוק ש- $a^{n-1} = 1$ ו- $a^{\frac{n-1}{q}} \neq 1$ לכל q ראשוני שהוא גורם של $n - 1$. שני התנאים האחרונים מתקיימים אמ"מ $ord(a) = n - 1$.

<u>אבחנה</u>: שאלת הראשוניות היא ב-$coNP$: נותנים עדות לפירוק למספר כדי להראות שהוא לא ראשוני.

<u>טענה</u>: שאלת הראשוניות היא ב- NP: עדות לכך היא ש- n ראשוני היא $a \in \mathbb{Z}_n^*$ המקיים את שני התנאים הנ"ל ופירוק של $n - 1$ לגורמים ראשוניים. העד צריך להכיל גם הוכחת ראשוניות שכל אחד מהגורמים בעדות הוא ראשוני. החלק בעדות לכל גורם k יהיה a משלו ולהראות שאותו a של גורם זה מקיים את התנאים. גודל העדות (בנפנופי ידיים) הוא פולי, ובדיקת הראשוניות צריכה להיעשות על כל אחד מהגורמים.

מיל-רבין ו-*RSA*:

נתון $n = p \cdot q$, p ו- q ראשוניים. מתקיים: $d \cdot e = 1 (\mathrm{mod}\, \phi(n))$. ואז: $(m^e)^d = m (\mathrm{mod}\, n)$. אם אנחנו יודעים את $\phi(n) = (p-1)(q-1)$ אז אנו יודעים את $n - \phi(n) + 1 = p + q$ ואז ניתן למצוא את p, q.

אם נתונים לנו זוגות $(e_1, d_1), \dots, (e_k, d_k)$, אנו יודעים ש-$\phi(n)$ מחלק את $e_i \cdot d_i - 1$. כנראה ש-$\phi(n) = \gcd\{e_i d_i - 1\}$. למה כנראה? בהסתברות נמוכה מאוד יש גורם נוסף שמשותף לכל הזוגות האלה, למשל11, אז בסוף נקבל $11 \cdot \phi(n)$.

אם נתון רק זוג אחד (d, e), כלומר רק כפולה אחת של $\phi(n)$. במקרה זה יש לנו $\alpha \cdot \phi(n)$ ו-α יכול להיות מאוד גדול. כאן נשתמש במשהו שדומה למבחן של מילר-רבין. נכתוב את המספר כך: $\alpha \cdot \phi(n) = 2^k \cdot r$ כאשר r אי-זוגי (k יכול להיות 0). לוקחים את הסדרה:

$$a_0 = a^r, a_1 = a^{2r}, a_2 = a^{4r}, \dots, a_k = a^{2^k r} = a^{\alpha \cdot \phi(n)} = 1$$

נחפש כעת i שעבורו $a_i \neq 1$ וגם $a_{i+1} = 1$ כלומר $a_i^2 = 1$ וגם $a_i \neq \pm 1$ (נסמן כעת $b := a_i$). אם $n | b^2 - 1 = \underbrace{(b+1)}_{=\alpha p} \underbrace{(b-1)}_{=\beta q}$ ואז: $p = \gcd(n, b+1)$, $q = \gcd(n, b-1)$.