קריפטוגרפיה 2

הרצאה 3: PRG

Textbook: Katz and Lindell. Introduction to Modern Cryptography.

מרצה: אורי שטמר

נושאי ההרצאה:

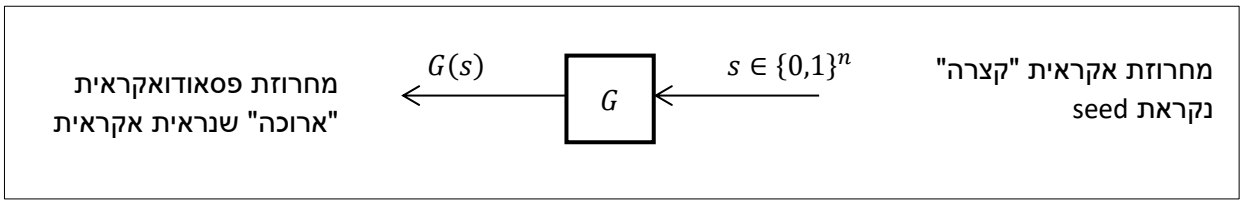
1. מהו גנרטור פסאודו אקראי (pseudorandom generator)?
2. איך בונים מערכת הצפנה במפתח סימטרי מתוך גנרטור פסאודו אקראי?
3. בטיחות כנגד הצפנות מרובות

נושא 1: מהו גנרטור פסאודו אקראי?

מוטיבציה: אקראיות היא משאב מוגבל. קשה באמת להשיג ביטים ממש אקראיים, כלומר מתפלגים בצורה אחידה ובאופן בלתי תלוי זה מזה.

הרעיון: ניקח מספר קטן של ביטים אקראיים "ונמתח" אותם למספר גדול יותר של ביטים "שיראו" אקראיים (לביטים כאלה נקרא "פסאודו אקראיים").

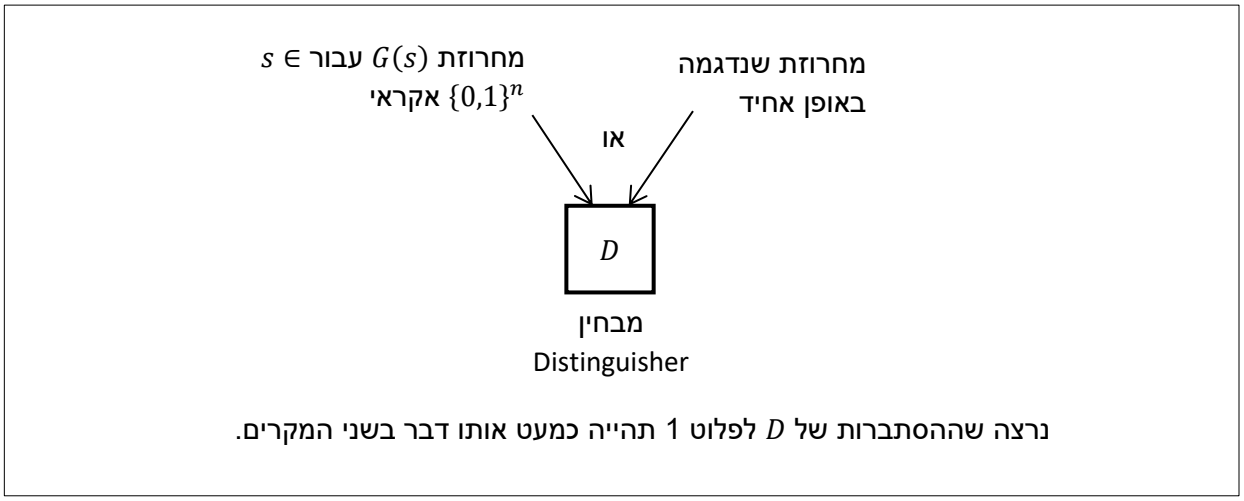
בציור:



מה זאת אומרת שהמחרוזת $G(s)$ נראית אקראית?? איך נגדיר?

נדרוש שאף אלגוריתם יעיל לא יכול להבחין בין $G(s)$ (עבור $s \in \{0,1\}^n$ שנדגם באקראי) לבין מחרוזת אקראית לחלוטין באותו האורך.

בציור:



נרצה שההסתברות של D לפלוט 1 תהייה כמעט אותו דבר בשני המקרים.

סימון: את ההתפלגות האחידה מעל מחרוזות באורך ℓ נסמן U_ℓ.

הגדרה: יהי $\ell(\cdot)$ פולינום ו- G אלגוריתם פולינומי (דטרמניסטי) כך שלכל n ולכל קלט $s \in \{0,1\}^n$ מתקיים $|G(s)| = \ell(n)$. נאמר ש- G הוא גנרטור (או יצרן) פסאודו אקראי אם מתקיים:

(1) הרחבה: לכל n מתקיים ש- $\ell(n) > n$

(2) פסאודואקראיות: לכל אלגוריתם (מבחין) פולינומי אקראי D קיימת פונקציה זניחה $negl$ כך שלכל n מתקיים:

$$\left| \Pr_{\substack{r\sim U_{\ell(n)} \\ D}}[D(r)=1] - \Pr_{\substack{s\sim U_n \\ D}}\left[D\left(G(s)\right)=1\right] \right| \leq negl(n)$$

תרגיל 1: נגדיר $G(s) = \left(s, (\oplus_{i=1}^{n} s_i)\right)$ כלומר G מחזיר את s ואח"כ את ה XOR של הביטים.
הוכח/הפרך: G יצרן פסאודו אקראי.

פתרון: G איננו יצרן פסאודו אקראי. כדי להוכיח את זה עלינו להראות מבחין יעיל D. נגדיר אלגוריתם D המקבל $n+1$ ביטים ובודק האם הביט ה $(n+1)$ הוא ה XOR של n הביטים הראשונים. אזי

$$\Pr_{r\sim U_{n+1}}[D(r)=1] = \frac{1}{2} \qquad \text{אבל} \qquad \Pr_{s\sim U_n}\left[D\left(G(s)\right)=1\right] = 1$$

מ.ש.ל.

תרגיל 2: עבור G יצרן פסאודו אקראי נגדיר

$$G'(\underbrace{s_0}_{\text{ביט}}, s) = \left(s_0, G(s)\right)$$

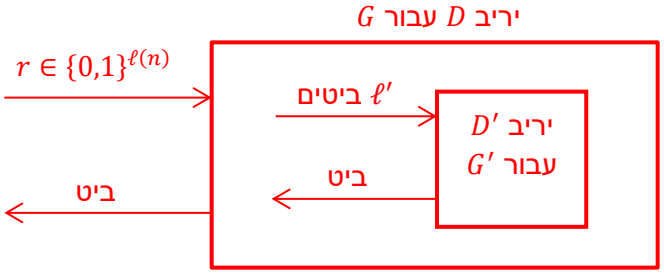
הוכח/הפרך: G' יצרן פסאודו אקראי.

פתרון: הוכחה. לכל n נסמן $\ell'(n) = |G'(n)|$. נבחין שמתקיים $\ell'(n) = 1 + \ell(n-1) > n$ ולכן G' מרחיב את הקלט שלו.

כעת נניח בשלילה ש- G' איננו מקיים את תכונה (2) בהגדרה של יצרן פסאודואקראי. כלומר קיים מבחין D' כך ש
$$\left|\Pr\left[D'\left(G'(s_0,s)\right)=1\right] - \Pr[D'(r)=1]\right| = \varepsilon(n)$$
עבור $\varepsilon(n)$ פונקציה לא זניחה.

נשתמש ב- D' כדי לבנות מבחין D ששובר את G וכך נקבל סתירה. כלומר ההוכחה היא על ידי רדוקציה.

בציור:
נבנה מבחין D
שמשתמש ב- D'
כקופסה שחורה



נגדיר מבחין D כך:

קלט: $r \in \{0,1\}^{\ell(n)}$
1. הגרל ביט אקראי s_0
2. החזר $D'(s_0, r)$

נשים לב שאם r אקראי אז s_0, r אקראי. לעומת זאת, אם r הוא פלט של $G(s)$ עבור $s \in \{0,1\}^n$ אקראי, אז $(s_0, r) = \big(s_0, G(s)\big)$ הוא פלט של $G'(s_0, s)$. כלומר,

$$\Pr_{\substack{r\sim U_{\ell(n)} \\ D}}[D(r)=1] = \Pr_{\substack{r\sim U_{\ell(n)} \\ s_0 \\ D'}}[D'(s_0,r)=1] = \Pr_{\substack{(s_0,r)\sim U_{\ell'(n+1)} \\ D'}}[D'(s_0,r)=1]$$

וגם

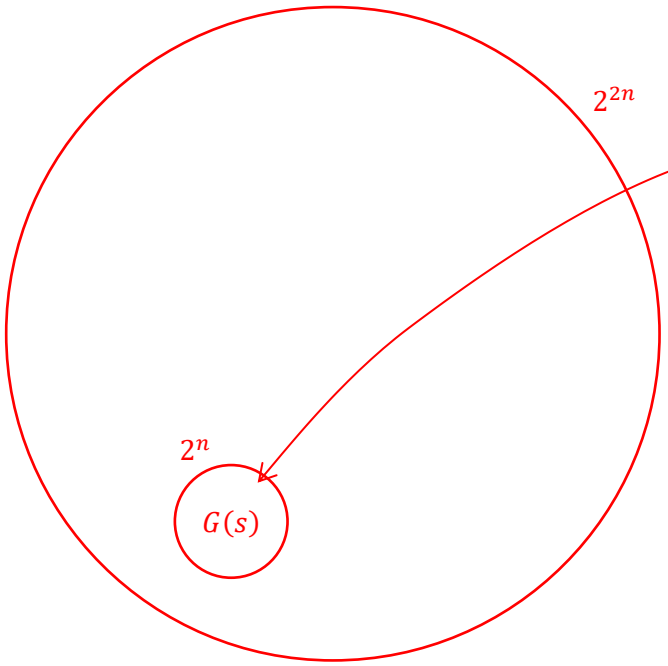
$$\Pr_{\substack{s\sim U_n \\ D}}\big[D\big(G(s)\big)=1\big] = \Pr_{\substack{s\sim U_n \\ s_0 \\ D'}}\big[D'\big(s_0, G(s)\big)=1\big] = \Pr_{\substack{(s_0,s)\sim U_{n+1} \\ D'}}\big[D'\big(G'(s_0,s)\big)=1\big]$$

כלומר D מבחין בהסתברות $\varepsilon(n+1)$ <u>לא זניחה</u> בין $r \sim U_{\ell(n)}$ לבין $G(s)$ עבור $s \sim U_n$. סתירה להנחה ש- G הוא יצרן פסאודו אקראי.
מ.ש.ל.

דגשים לגבי ההוכחה:
(1) התחלנו מיריב יעיל D' עבור G' וסימנו ב- $\varepsilon(n)$ את ההסתברות שהוא שובר את המערכת.
(2) בנינו יריב יעיל D עבור G. היריב D השתמש ב D' כקופסה שחורה, כלומר הריץ אותו בלי לנסות להבין איך הוא עובד. צריך להוכיח שאנחנו מפעילים את D' בתנאים שבהם הוא מצפה לעבוד.
(3) הראנו כי אם D' מצליח לשבור את G' בהסתברות לא זניחה אזי D מצליח לשבור את G בהסתברות לא זניחה.
(4) מההנחה שלא קיים אלגוריתם יעיל ששובר את G (בהסתברות לא זניחה) נסיק שלא קיים D' כנ"ל ששובר את G' (בהסתברות לא זניחה).

<u>תרגיל 3:</u> יהי G יצרן פסאודואקראי עם פונקצית הרחבה $\ell(n) = 2n$. הראו כי בעזרת אלגוריתם <u>לא מוגבל חישובית</u> ניתן להבחין (בהסתברות גבוהה) בין הפלט של $G(s)$ על $s \in \{0,1\}^n$ אקראי לבין $r \in \{0,1\}^{2n}$ אקראי.

<u>פתרון:</u> המחרוזת r נבחרת מתוך 2^{2n} מחרוזות ואילו המחרוזת $G(s)$ נבחרת מתוך 2^n מחרוזות.



אם נגריל מחרוזת באקראי מתוך $\{0,1\}^{2n}$ אז ההסתברות שהיא תיפול פה היא פיצפונת (ההסתברות היא $1/2^n$)

אם D אינו מוגבל חישובית אז הוא יכול להבחין כך:
בהינתן מחרוזת $r \in \{0,1\}^{2n}$:
- אם קיים s כך ש- $G(s) = r$ אז החזר 0
- אחרת החזר 1

נקבל ש $\Pr_{s\sim U_n}\big[D\big(G(s)\big)=1\big] = 0$

אבל $\Pr_{r\sim U_{2n}}[D(r)=1] = 1 - \frac{1}{2^n}$

מ.ש.ל.

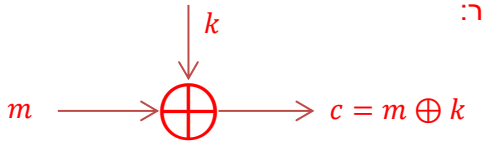
(כלומר מי שאינו מוגבל חישובית יכול לבצע את הבדיקה על ידי חיפוש ממצה...)

נושא 2: PRG ⟸ הצפנה סימטרית

תזכורת למערכת ההצפנה OTP:

- יצירת מפתח: הגרל $k \in \{0,1\}^n$
- הצפנה של הודעה $m \in \{0,1\}^n$: $Enc(m,k) = m \oplus k$

בציור:



- ראינו שמערכת OTP בטוחה. למעשה, ראינו כי כל יריב (אפילו כזה שאינו מוגבל חישובית) מנצח במשחק ההבחנה מול OTP בהסתברות בדיוק חצי.
- החיסרון של OTP הוא שאורך המפתח הוא כאורך ההודעה (זה חיסרון של כל מערכת הצפנה הבטוחה כנגד יריבים לא יעילים חישובית).

איך נוכל להשתמש ב PRG כדי לקבל מערכת הצפנה עם מפתח קצר יותר?

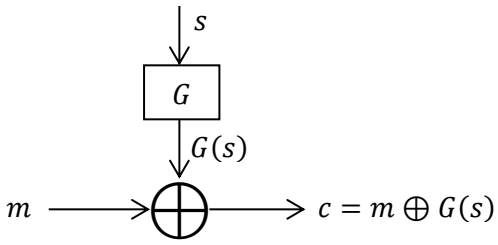
תהי $\ell: \mathbb{N} \to \mathbb{N}$ ויהי G גנרטור פסאודואקראי עם הרחבה $\ell(n)$. נגדיר את מערכת ההצפנה הבאה:

מערכת הצפנה Π (עם פרמטר בטיחות n):

- המפתח הוא $s \in \{0,1\}^n$
- ההצפנה של הודעה $m \in \{0,1\}^{\ell(n)}$: $Enc(m,s) = m \oplus G(s)$

נשים לב שכאן אורך המפתח הוא n ואורך ההודעה הוא $\ell(n) > n$
(אבל הבטיחות תהייה חישובית בלבד מכיוון שיריב שאינו מוגבל חישובית יכול לשבור את G).

בציור:



האינטואיציה: בהרבה מקרים אפשר להחליף מחרוזת אקראית במחרוזת פסאודואקראית

משפט: אם G הוא גנרטור פסאודואקראי עם הרחבה $\ell(n)$ אזי Π היא מערכת הצפנה EAV-בטוחה.

אינטואיציה להוכחת המשפט: אנחנו רוצים לבסס את הבטיחות של Π על הבטיחות של G.

מה אנחנו יודעים?

(1) עבור OTP, כל יריב מבחין בין הודעות בהסתברות בדיוק חצי

(2) עבור G, כל יריב יעיל מבחין בין מחרוזת אקראית r לבין $G(s)$ בהסתברות לכל היותר $\frac{1}{2} + \begin{pmatrix}\text{משהו}\\ \text{זניח}\end{pmatrix}$

מה אנחנו רוצים להראות? שכל יריב יעיל מבחין בין הצפנות של Π בהסתברות לכל היותר $\frac{1}{2} + \begin{pmatrix}\text{משהו}\\ \text{זניח}\end{pmatrix}$

איך נראה את זה? נניח שקיים יריב $\mathcal{A}$ שמנצח במשחק ההבחנה מול Π בהסתברות $\frac{1}{2}+\varepsilon(n)$ ונבנה ממנו יריב D לגנרטור G שמבחין בין r אקראי לבין $G(s)$ בהסתברות $\frac{1}{2}+\varepsilon(n)$. מכיוון שאנחנו יודעים ש- G בטוח, נסיק כי $\varepsilon(n)$ היא פונקציה זניחה.

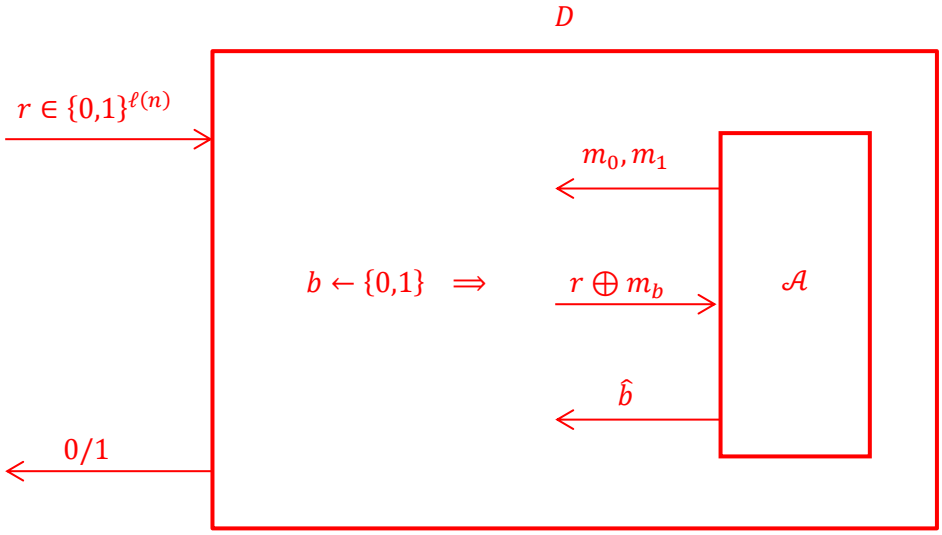
<u>הוכחה:</u> יהי $\mathcal{A}$ יריב פולינומי אקראי למשחק ההבחנה מול Π, המנצח בהסתברות $\frac{1}{2}+\varepsilon(n)$, ונניח בשלילה ש- ε היא <u>לא</u> פונקציה זניחה. נשתמש ב- $\mathcal{A}$ כדי לבנות מבחין D ל- G.

המבחין D:

קלט: $r \in \{0,1\}^{\ell(n)}$
(1) הרץ את $\mathcal{A}$ וקבל זוג מסרים m_0, m_1
(2) בחר ביט $b \in \{0,1\}$ באקראי ושלח ל- $\mathcal{A}$ את $m_b \oplus r$
(3) $\mathcal{A}$ מחזיר ביט $\hat{b}$
(4) D פולט 1 אם $b = \hat{b}$ ואחרת פולט 0

נשים לב שאם $\mathcal{A}$ פולינומי הסתברותי אז גם D פולינומי הסתברותי.

בציור:



D שבנינו אמור להבחין בין המקרה שבו $r \in \{0,1\}^{\ell(n)}$ נבחר באקראי לבין המקרה שבו $r = G(s)$ עבור $s \in \{0,1\}^n$ אקראי. נבדוק כל אחד משני המקרים:

<u>מקרה א:</u> r אקראי

אם $r \in \{0,1\}^{\ell(n)}$ אקראי, אזי $\mathcal{A}$ משחק במשחק ההבחנה מול OTP. במקרה זה אנו יודעים <u>שכל יריב</u> (ובפרט $\mathcal{A}$) סיכויי ההצלחה שלו הם <u>בדיוק</u> $1/2$. כלומר,

$$\Pr_{r\sim U_{\ell(n)}}[D(r)=1] = \Pr[\hat{b}=b] = \Pr\left[\begin{matrix}\mathcal{A}\text{ מנצח במשחק}\\ OTP\text{ ההבחנה כנגד}\end{matrix}\right] = \frac{1}{2}$$

<u>מקרה ב:</u> $r = G(s)$

אם $r = G(s)$ עבור $s \in \{0,1\}^n$ אקראי, אזי $\mathcal{A}$ משחק במשחק ההבחנה מול Π. במקרה זה סימנו את סיכויי ההצלחה שלו על ידי $\frac{1}{2} + \varepsilon(n)$. כלומר,

$$\Pr_{\substack{r=G(s)\\ s\sim U_n}}[D(r)=1] = \Pr\left[\begin{matrix}\text{מנצח במשחק } \mathcal{A}\\ \text{ההבחנה כנגד } \Pi\end{matrix}\right] = \frac{1}{2} + \varepsilon(n)$$

נסתכל על ההפרש

$$\left| \Pr_{r\sim U_{\ell(n)}}[D(r)=1] - \Pr_{\substack{r=G(s)\\ s\sim U_n}}[D(r)=1] \right| = \varepsilon(n)$$

לכן, מכיוון ש- G הוא יצרן פסאודואקראי, נקבל ש- $\varepsilon(n)$ חייבת להיות פונקציה זניחה.

מ.ש.ל.

<u>שאלה למחשבה (תראו את התשובה בתרגיל הבית):</u> במשפט האחרון הראינו שאם G גנרטור פסאודו-אקראי אז מערכת ההצפנה הסימטרית Π שבנינו בעזרתו היא EAV-בטוחה. האם גם הכיוון השני נכון? כלומר, נניח שאנחנו יודעים שמערכת ההצפנה Π שבנינו היא EAV-בטוחה. האם זה אומר ש- G הוא גנרטור פסאודו-אקראי?

נושא 3: בטיחות בהצפנות מרובות

עד היום דיברנו רק על הצפנה של מסר <u>אחד</u>. מה יקרה אם נרצה להצפין הרבה מסרים? איך נגדיר בטיחות כאן?

נשנה את משחק ההבחנה כדי להגדיר בטיחות במקרה של הרבה מסרים. נניח שיש לנו מערכת הצפנה $\Pi = (Gen, Enc, Dec)$. נגדיר את המשחק הבא:

1. היריב מקבל כקלט 1^n ופולט שני <u>וקטורים</u> של מסרים:

$$\vec{M}_0 = (m_0^1, m_0^2, \dots, m_0^t) \qquad \vec{M}_1 = (m_1^1, m_1^2, \dots, m_1^t)$$

כך שלכל $1 \le i \le t$ מתקיים $|m_0^i| = |m_1^i|$ (אנחנו צריכים את הדרישה הזאת כי מערכות ההצפנה שלנו לא מסתירות את אורך המסר).

2. המאתגר מפעיל את אלגוריתם Gen על 1^n לקבלת מפתח k, בוחר ביט $b \in \{0,1\}$ באקראי, ומחשב וקטור של הצפנות:

$$\vec{C} = \left(Enc(m_b^1, k), Enc(m_b^2, k), \dots, Enc(m_b^t, k)\right)$$

3. נמסר ליריב $\vec{C}$

4. היריב פולט $\hat{b} \in \{0,1\}$ ומנצח אם $\hat{b} = b$

<u>הגדרה:</u> מערכת הצפנה סימטרית Π <u>בטוחה כנגד יריב מאזין עבור מספר הודעות</u> אם לכל יריב פולינומי אקראי $\mathcal{A}$ קיימת פונקציה זניחה $negl$ כך שלכל n מתקיים

$$\Pr\left[\begin{matrix}\text{מנצח במשחק } \mathcal{A}\\ \text{הנ"ל מול } \Pi\end{matrix}\right] \le \frac{1}{2} + negl(n)$$

<u>שאלה למחשבה:</u> האם מערכת שהיא בטוחה להצפנת מסר אחד בטוחה גם כנגד הצפנה של מספר מסרים?

<u>תשובה:</u> לא בהכרח. היריב יכול לבחור $\vec{M}_0 = (m_0, m_0),\ \ \vec{M}_1 = (m_0 m_1)$ עבור $m_0 \neq m_1$. בכל מערכת הצפנה דטרמניסטית נקבל $C = (c_0, c_0)$ או $C = (c_0, c_1)$ וקל מאוד להבחין בין שני המקרים האלו.

<u>מסקנה:</u> מערכת תהייה בטוחה רק אם ניתן להצפין את אותו המסר בהצפנות שונות.

<u>משפט:</u> מערכת הצפנה שבה Enc הוא פונקציה דטרמניסטית של k (המפתח) ו- m (המסר) אינה בטוחה כנגד יריב הרואה מספר מסרים מוצפנים.

<u>שאלה למחשבה (נראה בהרצאה הבאה):</u> האם אפשר להשתמש ב PRG כדי לבנות מערכת הצפנה שתהייה בטוחה כנגד יריב מאזין עבור מספר הודעות?