עמוס ביימל 13.5.02

# קריפטוגרפיה: תרגיל 4

הגשה: יום ב' 27/05/02 ב- 18:00 בתא הדואר שלי (126).

## שאלה 1

יהיו $p$ ו- $q$ ראשוניים אי-זוגיים כך ש- $p=2q+1$.

**סעיף א**

יהי $a \in \mathbb{Z}_p^*$ כך ש- $a \neq \pm 1 \pmod p$. הוכיחו כי אם $a$ אינו יוצר של $\mathbb{Z}_p^*$, אזי $a$- הוא יוצר של $\mathbb{Z}_p^*$.

**סעיף ב**

הראו אלגוריתם דטרמיניסטי יעיל המוצא יוצר של $\mathbb{Z}_p^*$. מה סיבוכיות האלגוריתם שתיארתם?

## שאלה 2

יהיו $(p,g,b)$ ו- $(p,g,B)$ מפתח פרטי וציבורי בהתאמה עבור מערכת ההצפנה של ElGamal, כאשר $B \equiv g^b \pmod p$. בנוסף יהיו $M_1,M_2 \in \mathbb{Z}_p^*$ שתי הודעות. עבור $j$=1,2, הצפנו את $M_j$ בעזרת מחרוזת אקראית $a_j$ לקריפטוגרמה $(A_j , C_j)$ כאשר $A_j \leftarrow g^{a_j} \pmod p$ ו- $C_j \leftarrow B^{a_j} M \pmod p$. הוכיחו כי $(A_1 \cdot A_2, C_1 \cdot C_2)$ היא הצפנה של ההודעה $M_1 \cdot M_2$, כאשר כל הכפלים הם ב- $\mathbb{Z}_p^*$.

**סעיף ב**

הראו שמערכת ההצפנה של ElGamal אינה עמידה בפני התקפת קריפטוגרמה נבחרת.

## שאלה 3

בשאלה זו $p$ הוא ראשוני גדול, ו- $g$ הוא יוצר של $\mathbb{Z}_p^*$.

**סעיף א**

יהיו $a,b \in \{0,....,p-1\}$ ו- $K \equiv g^{ab} \pmod p$. הוכיחו כי $K$ הוא שארית ריבועית מודולו $p$ אם ורק אם $a$ או $b$ זוגיים. (שימו לב כי יתכן ש- $ab \geq p-1$).

**סעיף ב**

האם המפתח הנוצר בפרוטוקול של Diffie & Hellman להחלפת מפתחות מתפלג בצורה אחידה על $\mathbb{Z}_p^*$? הוכיחו תשובתכם.

**סעיף ג**

הוכיחו כי מאזין יכול לבדוק בצורה יעילה אם $K \equiv g^{ab} \pmod p$, המפתח הנוצר בפרוטוקול של Diffie & Hellman, הוא שארית ריבועית כאשר המאזין יודע מהם $p, g, A \equiv g^a \pmod p$ ו- $B \equiv g^b \pmod p$.

**סעיף ד**

הוכיחו כי מאזין יכול לבדוק בצורה יעילה אם הודעה המוצפנת בשיטת ElGamal היא שארית ריבועית כאשר המאזין יודע מהו המפתח הציבורי ומהי הקריפטוגרמה.

# שאלה 4

## סעיף א

בשאלה זו נסתכל על מערכת החתימה של ElGamal כאשר מפתח הוידוא הוא $(p,g,B)$. תהיינה $m_1, m_2$ הודעות ו- $(\gamma_1,\delta_1)$ , $(\gamma_2,\delta_2)$ חתימות על $m_1, m_2$ בהתאמה. איב הצליחה לחשב $a$ כך ש- $\gamma_1 \equiv g^a \gamma_2 \pmod p$. הראו איך איב יכולה לחשב בצורה יעילה את מפתח החתימה הפרטי מתוך $p, g, m_1, m_2, \gamma_1, \delta_1, \gamma_2, \delta_2$ ו- $a$.
<u>הערה</u>: הניחו של- $(\gamma_1\delta_2 - \gamma_2\delta_1)$ קיים הופכי מודולו $p$-1.

## סעיף ב

נתון כי בוב חתם על שתי הודעות בשיטת ElGamal כאשר בשני המקרים השתמש באותו מפתח פרטי ובאותו $k$.
הראו איך איב יכולה לחשב בצורה יעילה את מפתח החתימה הפרטי מתוך שתי ההודעות, שתי החתימות והמפתח הציבורי.

# *שאלה 5*

בשאלה זו נסתכל על מערכת חתימה הדומה למערכת החתימה של ElGamal. אלגוריתם יצירת המפתחות הוא בדיוק כמו באלגוריתם של ElGamal:

1. יהי $p$ ראשוני גדול ו- $g$ יוצר של $\mathbb{Z}_p^*$.
2. בוב מגריל $b \in \mathbb{Z}_{p-1}^*$ ומחשב $B \leftarrow g^b \mod p$.
3. מפתח החתימה הוא $(p,g,b)$ ומפתח הוידוא הוא $(p,g,B)$.

## אלגוריתם הוידוא:

חתימה על מסמך $M \in \mathbb{Z}_p^*$ היא זוג $(\gamma,\delta)$ כך ש- $B^\delta \gamma^\gamma \equiv g^M \pmod p$.

### סעיף א

הראו איך בוב יכול לחתום ביעילות על כל מסמך $M \in \mathbb{Z}_p^*$.

### סעיף ב

הראו כי המערכת אינה עמידה בפני זיוף קיומי.