קריפטוגרפיה: תרגיל 6

לא להגשה

שאלה 1

נסתכל על הסכמה הבאה לחלוקת סוד t-מתוך-n. יהי p ראשוני כך ש- $p > n$. לחלק סוד $s \in Z_p$, המחלק מגריל t-1 איברים אקראיים $r_0, r_1, ..., r_{t-2}$ מתוך Z_p, מסתכל על הפולינום $Q(x) = (s \cdot x^{t-1} + \sum_{j=0}^{t-2} r_j \cdot x^j) \bmod p$ ונותן למשתתף i את החלק $Q(i)$. שימו לב כי הסוד הוא המקדם של x^{t-1}.

סעיף א

הראו כי כל קבוצה של משתתפים בגודל לפחות t יכולה לשחזר את הסוד בצורה יעילה מתוך החלקים שקיבלה.

סעיף ב

נסתכל על הפולינום $R(x) = (\sum_{j=0}^{t-2} r_j \cdot x^j) \bmod p$. הוכיחו כי אם משתתף i יודע מהו הסוד, אזי הוא יכול לחשב את $R(i)$ מתוך $Q(i)$.

סעיף ג

הוכיחו כי כל קבוצה בגודל t-1 לא מקבלת מידע על הסוד מתוך החלקים שלה, כלומר, בהינתן החלקים כל סוד $s \in Z_p$ אפשרי.

שאלה 2

יהיו p,q ו- $N=pq$ כך ש- $p < q$. כמו כן, יהיו $0 \le x_1 < x_2 < ... < x_t < p$ ו- $y_1, y_2, ..., y_t \in \mathbf{Z}_N$.

סעיף א

הוכיחו כי קיים פולינום Q מעל $\mathbf{Z}_N$ מדרגה לכל היותר t-1 כך ש- $Q(x_i) = y_i$ עבור $1 \le i \le t$.

סעיף ב

יהי Q פולינום מעל $\mathbf{Z}_N$ כאשר $Q(x) = \sum_{j=0}^{t-1} a_j x^j$. נגדיר $b_j = a_j \bmod p$ עבור $0 \le j \le t-1$ ו- $R(x) = \sum_{j=0}^{t-1} b_j x^j$. הסבירו מדוע $Q(z) \equiv R(z) (\bmod p)$ לכל $z \in \mathbf{Z}_p$.

סעיף ג

יהיו $p > x_t > ... > x_2 > x_1 \ge 0$ ו- $y_1, y_2, ..., y_t \in \mathbf{Z}_N$. הוכיחו כי קיים פולינום יחיד R מעל $\mathbf{Z}_p$ מדרגה לכל היותר $t-1$ כך ש- $R(x_i) \equiv y_i (\bmod p)$ עבור $1 \le i \le t$. איפה השתמשתם בכך ש- $x_t < p$?

סעיף ד

הוכיחו בעזרת משפט השאריות הסיני כי קיים פולינום יחיד Q מעל $\mathbf{Z}_N$ מדרגה לכל היותר t-1 כך ש- $Q(x_i) = y_i$ עבור $1 \le i \le t$.

סעיף ה

יהיו מעל n,t שלמים חיוביים כך ש- $2 \le t \le n < p < q$. נממש את הסכמה של שמיר מעל $\mathbf{Z}_N$. כלומר כדי לחלק סוד $s \in \mathbf{Z}_N$, נגריל פולינום אקראי מעל $\mathbf{Z}_N$ מדרגה לכל היותר $t-1$ כך ש- $Q(0)=s$ והחלק של המשתמש ה- i הוא $Q(i)$. הוכיחו כי זוהי סכמה t-מתוך-n לחלוקת סוד.

שאלה 3

שאלה זו עוסקת בפרוטוקול ל-Oblivious Transfer המתבסס על הנחת ההכרעה של Diffie ו-Hellman.

יהי p ראשוני, ויהי g יוצר של $\mathbf{Z}_p^*$. שלשת DH היא שלשה $\langle A,B,C\rangle \in \left(\mathbf{Z}_p^*\right)^3$ אם קיימים $a,b \in \mathbf{Z}_{p-1}$ כך ש- $A \equiv g^a \pmod p$, $B \equiv g^b \pmod p$ ו- $C \equiv g^{ab} \pmod p$.

<u>הנחת ההכרעה של Diffie ו-Hellman (להלן הנחת DDH):</u>

לא קיים אלגוריתם יעיל שבהינתן $\langle A,B,C\rangle \in \left(\mathbf{Z}_p^*\right)^3$ מכריע האם הקלט הוא שלשת DH.

סעיף א

נתונות שתי שלשות DH הבאות: $\langle A,B_1,C_1\rangle$ ו- $\langle A,B_2,C_2\rangle$. הראו כי $\langle A,B_1B_2,C_1C_2\rangle$ היא שלשת DH.

סעיף ב

נתונה שלשת DH $\langle A,B_1,C_1\rangle$. מאידך, ידוע כי $\langle A,B_2,C_2\rangle$ אינה שלשת DH. הוכיחו כי $\langle A,B_1B_2,C_1C_2\rangle$ אינה שלשת DH.

סעיף ג

אליס מחזיקה $B,C \in \mathbf{Z}_p^*$ ו- $a \in \mathbf{Z}_{p-1}$. תארו כיצד אליס יכולה לחשב בצורה יעילה האם $\langle g^a,B,C\rangle$ היא שלשת DH.

נזכיר את הגדרת פרוטוקול Oblivious Transfer:

קלט לאליס: $i \in \{0,1\}$. קלט לבוב: $y_0,y_1 \in \{0,1\}$.

דרישות:

נכונות: בסיום הפרוטוקול אליס תדע את y_i.

בטיחות 1: אליס לא תלמד דבר על y_{1-i}.

בטיחות 2: בוב לא ילמד דבר על i.

הוצע הפרוטוקול הבא עבור Oblivious Transfer:

1. אליס מגרילה $a,b_{1-i} \in \mathbf{Z}_{p-1}$, ומחשבת את השלשה $\langle A,B_{1-i},C_{1-i}\rangle$ כאשר $A=g^a$, $B_{1-i}=g^{b_{1-i}}$ ו- $C_{1-i}=g^{ab_{1-i}}$.
2. אליס מגרילה $x,b_i \in \mathbf{Z}_{p-1}$, ומחשבת את השלשה $\langle A,B_i,C_i\rangle$ כאשר $A=g^a$, $B_i=g^{b_i}$ ו- $C_i=g^x$, כאשר $x \not\equiv ab_i \pmod{p-1}$.
3. אליס שולחת את השלשות $\langle A,B_0,C_0\rangle$ ו- $\langle A,B_1,C_1\rangle$ לבוב.
4. בוב מחשב $B=B_0^{y_0}B_1^{y_1} \bmod p$ ו- $C=C_0^{y_0}C_1^{y_1} \bmod p$.
5. בוב שולח את $\langle B,C\rangle$ לאליס.
6. אליס בודקת האם $\langle A,B,C\rangle$ היא שלשת DH. אם כן, היא קובעת $y_i=0$. אחרת, היא קובעת $y_i=1$.

סעיף ד

הוכיחו את נכונות הפרוטוקול, כלומר, שהביט שאליס מחשבת הוא אכן y_i.

סעיף ה

הסבירו מדוע בוב לא לומד מידע על i.

סעיף ו

הפרוטוקול הנ"ל אינו עונה על דרישת בטיחות 1. הראו כיצד אליס יכולה לחשב בצורה יעילה את y_0 ו- y_1.

סעיף ז

שנו את הפרוטוקול הנ"ל כך שיקיים גם דרישת בטיחות 1. הסבירו מדוע הפרוטוקול שבניתם מקיים את כל הדרישות..