יסודות הקריפטוגרפיה תרגול #5

ניזכר בפרוטוקול DH מהשיעור:

- ידועים: g, p
- אליס שולחת g^a
- בוב שולח g^b

הם משתמשים במפתח g^{ab}.

בניגוד להנחת השיעור, נניח כעת כי המאזין הוא אקטיבי ומשתלט על קו התקשורת בין אליס ובוב. הירי מחליף את g^a ב- $g^{a'}$, כנ"ל לגבי השני, ואז מעביר הודעות מאליס לבוב מוצפן ב-$g^{a'b}$ ומבוב לאליס מוצפן ב- $g^{ab'}$.

תקיפה זו נקראת תקיפת ***man in the middle***, ו-DH מאפשר לכל שני אנשים לתאם מפתח מבלי ידע מוקדם אחד על השני, ולכן אין שום דרך שאליס ובוב מדברים למעשה עם האיש באמצע ולא ישירות אחד עם השני.

פתרון:

אליס ובוב ישלחו תחילה את g^a, g^b אחד לשני מוצפן ע"י p כלומר $E_p(g^a), E_p(g^b)$. שיטה זו היא ***EKE*** – *Encrypted key exchange*. אם נניח ש-p ססמא גרועה, נניח בת ארבע ספרות, נרצה להגביל את התוקף כך שלא יוכל לעשות בדיקות מהי הסיסמא *offline*, אלא שיזדקק לדבר עם השרת/אחד הצדדים על כל ניסיון סיסמא – כי שיטה זו חושפת ניסיונות תקיפה (למשל ניסיון ניחוש קוד סודי לכרטיס בנקאי שלא מצליח כמה פעמים גורם לבליעת הכרטיס – מזוהה כניסיון תקיפה; לא ניתן לבצע ניסויים רבים *offline* כדי לגלות, חייבים ניסיון מקוון). בשיטת *EKE* התוקף מוגבל לניסיונות מקוונים, שכן לאחר מספר קבוע של ניסיונות ניתן לעלות על ניסונות התקיפה (גם סיסמא בת4 ספרות מספיקה).

נשים לב כי גם אם בטעות נחשף איכשו g^{ab}, עדיין אם יש לתוקף g^a, g^b משוערים (כי המקוריים מוצפנים), כיוון ש-a, b מקריים גם g^a, g^b מקריים ואין אינפורמציה להוציא מהם את g^a, g^b האמיתיים.

בעיית *Discrete-Log*:

ב-$\mathbb{Z}_p^*$ עבור $p = 2^n + 1$; נתונים g, p יוצר ונתון $x \in \mathbb{Z}_p^*$. רוצים לחשב $0 \le t \le 2^n - 1$ כך ש-$g^t = x \pmod p$ ביעילות. בגלל ש-g יוצר, אז מובטח כי קיים t כזה. נכתוב את t באופן הבא: $t = t_0 + 2t_1 + 4t_2 + 8t_3 + \cdots + 2^{n-1}t_{n-1}$. הזוגיות של t מעניינת כי $t_0 = 0$ אמ"מ x הוא שארית ריבועית מודולו p, וזאת אנו יודעים לחשב: $x^{\frac{p-1}{2}} = x^{2^{n-1}} = g^{t2^{n-1}} = g^{t_0 \cdot 2^{n-1}} \cdot g^{(\dots)\cdot 2^n}_{=1} \to \begin{cases} = 1, & t_0 = 0 \\ = g^{2^{n-1}} \neq 1, & t_0 = 1 \end{cases}$ - במקרה $t_0 = 0$ אז x הוא שארית ריבועית. במקום לעבוד עם x נעבוד עם $x' = \frac{x}{g^{t_0}} = g^{2t_1 + 4t_2 + \cdots + 2^{n-1}t_{n-1}}$. ואז: $\sqrt{x'}$ הוא שארית ריבועית מודולו p אמ"מ $t_1 = 0$. והרי:

$$\sqrt{x'} = g^{t_1 + 2t_2 + \cdots + 2^{n-2}t_{n-1}}$$

ואז ניתן להמשיך לעשות זאת על שאר הביטים. צריך לבדוק האם $\sqrt{x'}^{\frac{p-1}{2}} \overset{?}{=} 1$ כדי לבדוק האם הוא שארית ריבועית. אבל זה שקול לבדיקה האם $x'^{\frac{p-1}{4}} = 1$. זה דורש ש-$p - 1$ יתחלק בחזקה גדולה מאוד של 2 להמשך האיטרציות (כאן הגענו עד 4 בינתיים).

יעילות: כל העלאה בחזקה שעושים n פעמים שזה $\log p$ עושים $\log^3 p$ פעמים, סה"כ $O(\log^4 p)$ פעמים.