תרגיל:

1. נתבונן בסביבות הדבקים הבאה.

גיר מפתחות במהרה הראשון חבר ק הפלגים אקראי

$q(\cdot)$ מדרגה $n-1$ ב $\mathbb{Z}_p[x]$ (כלומר נבחר

$\{0,\dots,p-1\} \ni a_0,\dots,a_{n-1}$)

מפתח: $q(x)$, p

$P = (\mathbb{Z}_p)^n$

$C = (\mathbb{Z}_p)^n$

הצפנה: כדי לצפן את הודעה $x \in \{0,\dots,p-1\}^n$

נחשב $y_i = x_i + q(i)$ מוד p

פענוח $x_i = y_i - q(i)$ מוד p

הנחיות אסור שיהיה משלמת

בתרגיל: נבנה באופן שכל שונה:

נניח ש $|P| = |C| = |K|$ הוא בעל חיתוך

משלמת, אם כל מפתח נבחר בהסתברות אחידה:

לכל x, y קיים מפתח יחיד כך ש $e_k(x) = y$

הראשית, נשים לב ש $P = C = K = (\mathbb{Z}_p)^n$

כי המפתח מכיל n מקדמים מתוך $\mathbb{Z}_p$.

בנוסף, נשים לב שלכל מפתח נבחר בהסתברות שווה

כמו כן, לכל $x \in P$ ולכל $y \in C$ קיים פולינום

יחיד כך ש $y = e_k(x)$ ובאופן מדויק x

ו y מגדירים n נקודות $(1, q(1)), \dots, (n, q(n))$

ו n נקודות מגדירות פולינום יחיד מדרגה $n-1$

2. נתבונן בהגדרה הבאה לסימון מלאי סגור הבסיס $\mathcal{B}$ שני הפעולות.

נאמר שלצופן יש סיפור מושלם לשני הפעולות אם לכל $x_1, x_2 \in P$ ולכל $y_1, y_2 \in C$:

$$Pr[x_1 \wedge x_2 \mid y_1 \wedge y_2] = Pr[x_1 \wedge x_2]$$

כאשר x_1 ו x_2 נבחרות בצורה בלתי תלויה.
הרעיון שאל בינן לבין מקרים הבדה בו.

<u>סתירה</u>: נניח שני הפעלות $x_1 \neq x_2$ כך ש
$Pr(x_1 \wedge x_2) \neq 0$

ונניח אבל שהבסיס $y_1 = y_2$, אז

$$Pr[x_1 \wedge x_2 \mid y_1 \wedge y_2] = 0$$

כי הבסיס הוא חח"ע

3. הרעיון בצורה פורמלית שאם נשנה את בינן הרי נגיע כן לכל אות נשתנש באפתח שונה, נקבל בינן בכל כיוונים מושלמים.

<u>סתירה</u>: מרגע לכל אות משתנשים באפתח שונה, מספיק להודיע סבור אות בודדת.
נשתנש במשפט שנון.
הנחה $|P| = |K| = |C| = 26$
כלומר, כל אותיות נבחרה בהסתב $\frac{1}{26}$ ולכל
זוג אותיות x, y קיים מפתח יחיד
שממפה את x ל y (הסבירות לה מלמד $k = y - x$)

ד. האם הסדרה הבאה בעלת סודות מושלמים?

המרחב P מורכב לדוגמא כל המילים באורך 26 מעל $\mathbb{Z}_{26}$ כך שכל אות במילה שייכת לקבוצה P שווה לכל התמורות של $\mathbb{Z}_{26}$.

K מורכב מכל $K=P$

אל הצפנה היא הרכבה של המפתח על הקוד הבלוקי

<u>פתרון</u>: כן נשתמש בנשמט שנון

<u>דוגמא</u>: $x=3,1,2$

$k=1,3,2$

בראש נניח לא שהרכבה של שני פרמוטציות היא פרמוטציה ולכן C מכילה את כל הפרמוטציות ולכן $|C|=|P|=|K|$

$y=2,1,3$

בנוסף כל מפתח נבחר בהסתברות שווה לכל $x\in P$ ולכל $y\in C$ קיים מפתח יחיד כך $e_k(x)=y$ וכל הפרמוטציה שממפה את x_i ל y_i לכל $i=1,2,\dots,26$

ולכן לפי שנון לצופן יש סודות מושלמים.

ב. הצפנה מוזרה $e_k(x): x_1+k_1, \dots, x_{26}+k_{26}$

בשביל התבוי הזאת מספיקות 26

<u>פתרון</u>: לכל נבחר מקרים $x\in P$ ו $y\in C$

כך $Pr[x|y]=Pr[x]$

נשפ"ר

$x = 0 \quad 12 \quad 25 \quad \overbrace{1 \quad 2 \quad 3 \quad \dots \quad 24}^{\text{אחר כל כך}}$

$y = 13 \quad 13 \quad \underbrace{0 \quad 0 \quad \dots \quad 0}_{\text{אפס 24}}$

כדי לבטל ל $x \in P$

נבחר ל $y \in C$: סבר

$x' = 13 \quad 0 \quad 1 \quad 2 \quad 3 \dots \quad 12 \quad 14 \quad 15 \dots \quad 25$

$k' = 0 \quad 13 \quad 25 \quad 24 \quad 23 \dots \quad 14 \quad 12 \quad 11 \dots \quad 1$

$y = 13 \quad 13 \quad 0 \quad 0 \quad 0 \quad \dots \quad 0$

ולכן $y \in C$.

$Pr[x|y] =$ כמה נראה

$= Pr[k = 13 \quad 1 \quad 1 \quad 25 \quad \dots \quad] = 0$

ולכן

$Pr[x|y] \neq Pr[x]$

בס"ד

פרק 3 - תרגילים - לפני כן שהבנה חיבת להיות הסתברותית

1. לצרכי ניסוי, הוחלט להשתמש ב נשק באמצעות באורך 48 בית ולהשתמש באותו מפתח בכל אוכלוסיה של מבנה פיסקל. נתחו את סיכוי ההצפה.

פתרון

כפי שמופיע, המנה ב נשק מתבצע בפונק באותו אופן שמתבצעת הצפנה. רק מס' מספר מפתחות הם. במקרה אנו מדברים שלא תת המפתחות נמצא הצפנה ומסנן מתבצעים באותו האופן בפונק במקרה כזה, ניתן לבצע התקפת מקסם אלו ניתן לבחור רק: בהינתן הצפנה c, נבחן את ההופעה ונקבל את התופעה המקורית m.

2. בפרקטיקה מומלץ בכל יום אולם שולחים אחת מ 10 הופעות אפשריות ולפיהן בוחר מבצע לחיצת פקלת נשמה (שרות יומי לראות).
נניח שאולם ובא יש מפה משותפת f היא פונק הצפנה טובה. כפי לדג את התופעה משתנים ב 4 בית ושאר הבית בכל נקבעים להיות 0.
אולם שולחים $f_k(m) = c$.
אוסקר ריגב לבעלי מקור אולם אחת לפני שבוחר מהבצע אותה בגב הוא יכול לקשור כאותה הבטי שלו קיים לפרטיקל שונה מהתקפה על אוסקר.

פתיון: בכל מקרה שאלים שלות אותה הועדה, ההצעה
היא כהה ולכן אם אוסקר רואה אותה אני
מקיפה בועדה לעתידית, בכסף הבאה שהוא
רואה אם אותה הועדה, הוא יקח את בונוס
לעתידית

הדרך הכי פשוטה להתנגד על כך, זה להצמיד את
הסקיפה בעניין ABC, כך שהצעות של אותה
הועדה יהיו שונות

פרק 4 - פונקציות חד־כיוון ! MAC

פונקציות חד־כיוון בלי עמיתה.

הגדרות כלליות לפונקציות חד־כיוון:

- Preimage
- second Preimage
- חסינות־אוספים

אפשר לשנות את כולן בצורה לא־יפה

הרעיון שהפונקציה סמיפה, כלומר אומר שאי־אפשר אלגוריתם יעיל שיצליח לשנות לתוקפים לשאלה כ בהסתברות 1

הגדרת כלליות לMAC:

לאלגוריתם יש עמיתה סודי אחרי כולם לחישוב MAC ליניאר אין עמיתה סודי, אבל כולם לשאילתות Q שאילתות לאורקל. בסוף צריך להוציא זוג (x,y) כך ש:

1. ...
2. ...

תרגילים:

1. תהי $E_k(\cdot)$ הצפנה בלוקים חשיפה.
הראה פונקציה hash הבאה כלליות בפני התנגשויות:
$h(x \| y) = E_x(y) \oplus E_y(x)$

פתרון: לכל

נניח $x \neq y$ ואז

$h(x\|x) = E_x(x) \oplus E_x(x) = 11..1$

$h(y\|y) = E_y(y) \oplus E_y(y) = 11..1$

$\Rightarrow$ $x\|x$! $y\|y$ מהוות התנגשות

2. יהי p ראשוני גדול ו $\alpha \in \mathbb{Z}_p^*$

הראה הפונקציה הבאה מקיימת בסיס התנגשויות

$$h(x) = \alpha^x \bmod p$$

<u>פתרון</u>: לכל

$$h(x+p-1) = \alpha^{x+p-1} \bmod p \equiv$$

$$\alpha^x \cdot \alpha^{p-1} \bmod p \equiv \alpha^x \bmod p$$

$$\Rightarrow h(x) = h(x+p-1)$$

יהי זוג $(x, x+p-1)$ מהווה התנגשות.

3. תהי $h: \{0,1\}^m \to \{0,1\}^n$ פונקציה חד כיוונית

מקיימת בסיס התנגשות. הראה הפונקציה הבאות

מקיימות בסיס התנגשות:

א. $g(x_1 \| x_2 \| x_3 \| x_4) = h((x_1 \oplus x_2) \| (x_3 \oplus x_4))$

<u>פתרון</u>: לכל

$$g(x_1 \| x_2 \| x_3 \| x_4) = g(x_2 \| x_1 \| x_4 \| x_3)$$

אם $x_1 \neq x_2$ זוג התנגשות.

ב. $g(x_1 \| x_2 \| x_3 \| x_4) = h(x_1 \| x_2) \oplus h(x_3 \| x_4)$

<u>פתרון</u>: לכל

$$g(x_1 \| x_2 \| x_3 \| x_4) = g(x_3 \| x_4 \| x_1 \| x_2)$$

אם $x_1 \neq x_3$ זוג התנגשות

6. תהי E הצפנת בלוקים עם גודל בלוק n
ותהי h פונקציה חד־חד־ערכית כלשהי בין התפלגויות על
גודל בלוק n. k היא סודית. את הצפנה
בעזרתה:

לכל הודעה m יקיים $|m| = n$, נחשב $y = E_k(m)$
" " " " $|m| > n$ " $y = E_k(h(m))$
(הניחו שאורך כל ההודעות $\leq n$)

בתרגיל: הסכימה לא באותה. נראה כיצד שרבלית ליצור גזל

היריב בוחר הודעה כלשהי $m \in \{0,1\}^n$ כאשר $n > k$
ומבקש מהאורקל שחלמה לו m. מקבל y.
מוציא כפלט זוג $(h(m), y)$.
נשים לב שהיריב לא בקש מהאורקל MAC לחלמה
ונשים לב ש y הוא MAC תקין של $h(m)$
לכן $(h(m), y)$ הוא זוג גזל
ב. הבנו תיקון לסכימה.

פתרון: בעזרת להכפיל את h ב כך $n < |m|$,
נפעיל אותו תמיד על כל $n = |m|$.

זה בפועל MAC מדוע

7 תצמדים - CBC-MAC: נשתמש את CBC-MAC כך
שהפלט יהיה - $y_1, y_2, \dots, y_l$ הוא הסכימה
לכן בטוחה

פתרון: לא. נראה כיצד שרבלית ליצור זוג גזל. הוראות: חב
היריב בוחר $m_1, m_2 \in \{0,1\}^n$, מבקש MAC של
$m_1 m_2$, מקבל y_1, y_2 כך ש $y_1 = E_k(m_1)$
$y_2 = E_k(m_2 \oplus y_1)$
מוציא את הזוג $(m_1, m_1 \oplus y_1, y_1, y_1)$. נראה
ש (y_1, y_1) הוא MAC תקין ל $(m_1, m_1 \oplus y_1)$:
$y_1 = E_k(m_1)$
$E_k(m_1 \oplus y_1 \oplus y_1) = E_k(m_1) = y_1$

4. הראו איך ניתן לשבור את RSA למפתחות אם משתמשים ב $n=p^2$ במקום $n=pq$

פתרון:

כידוע, אם $n=\prod_{i=1}^{m} p_i^{e_i}$

$$\phi(n)=\prod_{i=1}^{m}\left(p_i^{e_i}-p_i^{e_i-1}\right)$$

ולכן אם $n=p^2$ $\phi(n)=p^2-p$

$\Leftarrow$ כל מה שהיה צריך לעשות, זה למצוא a כך ש $ab\equiv 1 \mod (p^2-p)$.

8. כמה לקבל את בעלת הבסיס, הוצא לבחור a אקראי מתוך כל הסדר שהיקף הבנאי לא מגיל בפחות 3 בלי שיהם 1 והשאר אם ואז לחשב b מתאים. הדם אמור לחשב b מתאים? למה זה מבטיח את בעלת הבסיס? הדם הסבירה עפ"ן בחרה?

בתרגיל: ניתן לעצור גם b אחרי שבחרנו את a באופן אמן בפיקוח שחשבנו גם a אחרי בחירת b.

כי מעבר את הפעולה ~~מעלה סבה b~~

~~שאלה הפרמטר.~~

אולם הסבירה אינה בעיתה כלל.

מבין שפרור ורעורים באורך n, יש רק $\binom{n}{3}$

$\approx n^3$ אפשרויות ל a וכן מספר פולינום

עדין אפשר לעסות כזה מהם ולפיקוח גם הוא

נכון.

כי באלגוריתם לחלוקת הקבוצה מבנים יותר

עבור גם את הכל הקודמת הוא 1 מאשר

0 ולכן כבר שנם הבינו משמעם ל 1

יותר קטן, החישוב מתבצע יותר מהר

פרק 6

תזכורת דיפי הלמן

חבורה Z_p^* ו $\alpha \in Z_p^*$ יוצר

$\beta = \alpha^a \bmod p$ ו a אקראי

הצפנה $e_k(x) = (\alpha^k \bmod p,\ x\beta^k \bmod p)$

פענוח $d_k(y_1, y_2) = y_2 (y_1^a)^{-1} \pmod p$

תרגיל

1. תיש סון, מועמד ב. שאלה 4.

א. **פענוח** $d_k(y_1, y_2) = y_2 / (y_1^a)$

נראה שאם ניתן להבחין בין הצפנות של הודעות x_1, x_2, אפשר לפתור את בעיית DDH.

בהינתן יוצר α ושלשה (β, δ, γ) הלא של DDH, נשתמש בפתרון פוטנציאלי (α, β). נחשב $y = (\gamma, x_1 \cdot \delta)$ ונשתמש את הפתרון הפוטנציאלי ו y לשלוח שאלתון בין הצפנה של x_1 ו x_2. אם הוא מחזיר שזו הצפנה של x_1, נחזיר שזו שלשה חוקית של DDH. אם הוא מחזיר x_2 אז זו שלשה אקראית, נחזיר שזו לא שלשת DDH חוקית.

ב. **פענוח** טוב. אין הסברה לזה בכלל.

בהינתן זוג אחד של הודעה והצפנה של $x, (y_1, y_2)$ נחשב $y_2 (x^{-1}) \bmod p$ ונקבל את β^k.

בפתרון בהינתן הצפנה (y_1', y_2') של הודעה כלשהי נחשב $y_2 (\beta^k)^{-1}$ ונקבל את x'.

ג. **פענוח** אינו טוב כי יש לפתור קשה

2. אלס ובוב רוצים לממש פרוטוקול לקביעת מפתח משותף באופן הבא:

בוב בוחר מפתח $k \in \{0,1\}^n$ וסדרן אקראי $P_B \in \{0,1\}^n$ ושולח $M_1 = k \oplus P_B$ לאלס

אלס בוחרת סדרן אקראי P_A ושולחת $M_2 = M_1 \oplus P_A$ לבוב. בוב מחשב $M_3 = M_2 \oplus P_B$ ושולח לאלס

אלס מקבלת ומחשבת $k = M_3 \oplus P_A$.

א. הראו שאכן $k = M_3 \oplus P_A$

ב. נניח שאויב רואה את M_1, M_2, M_3. איך הוא יכול לגלות את k?

פתרון:

א. $M_3 \oplus P_A = M_2 \oplus P_B \oplus P_A = M_1 \oplus P_A \oplus P_B \oplus P_A =$
$= M_1 \oplus P_B = k \oplus P_B \oplus P_B = k$

ב. יחשב $M_3 \oplus M_2 = P_B$

ואז $M_1 \oplus P_B = k$

פרק 7 - חזקות

1. נניח שאלה חזקה של הרבה מספרים ראשוניים בחזקות גדולות (נניח כל הראשוניים עד 2^{20}). איך ניתן לחשב בחזקות אלו כדי לבדוק חזקה k אלים של הפקטור הראשוני?

<u>פתרון</u>

תהי m הפקטור שנרצה לבדוק שהוא חזקה ראשונית m לא יותר מ- 2^{20} אחרבה, אזי ניתן לפרק אותו לגורמים ראשוניים נניח m עד 100 ביטים (גם אחרים). כמו כן כל הראשונים בפירוק של m כבר נמצאו, וניתן לחשב בתוך הכלים k הנדרש כדי לבדוק חזקה של m

$$m = \prod_{i=1}^{l} p_i^{e_i}$$

כמו כן, אם σ_i חזקה של p_i, חזקה של m:

$$\prod_{i=1}^{l} \sigma_i^{e_i}$$

2. תרגילים 4, 5 בתרגיל

3. תרגיל 3 בחזקה הראשית