מבוא להצפנה

תוכן עניינים בסוף...

חלק I: רקע

1. מושגים בסיסיים

הגדרה 1.1. "מחלק את": עבור $a,b\in\mathbb{Z}$ - $b\mid a$ אם קיים $k\in\mathbb{Z}$ כך ש-$a\cdot k=b$, למשל: $2\mid 8$, $7\mid 35$ וכו...

הגדרה 1.2. מחלק מקסימלי משותף של שני מספרים $a,b\in\mathbb{N}$ מוגדר להיות המספר הגדול ביותר $n\in\mathbb{N}$ אשר מקיים: $n\mid a\wedge n\mid b$ ומסומן: $\gcd(a,b)$,

למשל: $\gcd(18,12)=6$ כי 6 הוא המספר הגדול ביותר אשר מקיים: $6\mid 18\wedge 6\mid 12$.

הערה 1.3. $\gcd(a,b)=\gcd(b,a)$.

הגדרה 1.4. **מספר ראשוני** הוא מספר $p\in\mathbb{N}$ כך שלכל $a\neq p$ $\gcd(a,p)=1$ - או לכל $1<a<p$: $a\nmid p$.

הגדרה 1.5. **מספר פריק** הוא מספר שאינו מספר ראשוני (הגדרה 1.4)

הגדרה 1.6. **מספרים זרים:** עבור $a,b\in\mathbb{N}$ אם $\gcd(a,b)=1$ אזי אומרים כי a ו-b הם זרים.

הגדרה 1.7. עבור קבוצה סופית A: $|A|$ תוגדר כמספר האיברים ב-A.

2. פונקציית אוילר

פונקציית אוילר היא פונקציה $\varphi:\mathbb{N}\to\mathbb{N}$ אשר מוגדרת באופן הבא:

$$\varphi(n)=\left|\left\{a\middle|\gcd(a,n)=1\right\}\right|$$

כלומר זוהי פונקציה שמחזירה את כמות המספרים הזרים (הגדרה 1.6) למספר $n\in\mathbb{N}$.
למשל: $\varphi(10)=4$ כי המספרים שזרים ל-10 הם: $\{1,3,7,9\}$.

2.1 נוסחה לחישוב פונקציית אוילר

ישנן שתי נוסחאות שדרכן ניתן לחשוב את פונקציית אוילר:

משפט 2.1. ניתן להציג כל מספר טבעי באמצעות מכפלה של מספרים ראשוניים: $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.

$$\boldsymbol{\varphi(n) = \prod_{p_i|n} \left(1 - \frac{1}{p_i}\right)}$$

כאשר p_i הוא ראשוני שמחלק את n. (ויכולים להיות כמה כאלה).
וכמו-כן ניתן לחשב את פונקציית אוילר באמצעות הנוסחה הבאה:

$$\boldsymbol{\varphi(n) = \prod_{p_i|n} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right)}$$

דוגמה 2.2. ניקח את $n = 25 = 5^2 \cdot 2^1$ אזי:

$$\varphi(25) = \left(5^2 - 5^1\right)\left(2^1 - 2^0\right) = 20 \cdot 1 = 20$$

ליאונרד אוילר

הערה 2.3. אם p ראשוני אזי $\varphi(p) = p - 1$.

3. הקבוצות $\mathbb{Z}_n$ ו-$\mathbb{Z}_n^*$

הגדרה 3.1. הקבוצה $\mathbb{Z}_n$ היא הקבוצה $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$
או:

$$\mathbb{Z}_n = \left\{k \middle| k \in \mathbb{N},\ 0 \le k \le n-1\right\}$$

הגדרה 3.2. הקבוצה $\mathbb{Z}_n^*$ היא הקבוצה אשר מכילה את כל המספרים אשר זרים ל-n:

$$\mathbb{Z}_n^* = \left\{k \middle| k \in \mathbb{N},\ \gcd(a, n) = 1\right\}$$

הערה 3.3. $\varphi(n) = \left|\mathbb{Z}_n^*\right|$.

משפט 3.4. אם p ראשוני אזי $\varphi(p) = \left|\mathbb{Z}_p^*\right| = p - 1$ (כל המספרים $k \in \mathbb{N}$: $0 < k < p$).

3.1 הסימן $\pmod n \equiv$

הרעיון במשוואה מהצורה $a \equiv b \pmod n$ היא ש-$a = b$ ב-$\mathbb{Z}_n$, למשל: ניקח את $\mathbb{Z}_{18}$, כלומר $n = 18$, אזי:

$$19 \equiv 1 \pmod{18}$$

כי אין לנו 19 ב-$\mathbb{Z}_{18}$, אבל זה אומר שהגענו ל-0 (18) והמשכנו עוד 1.
וזה נכון גם לגבי מספרים שליליים:

$$-3 \equiv 15 \pmod{18}$$

3.2 איברים הפיכים ב-$\mathbb{Z}_n$

הגדרה 3.5. עבור איבר בקבוצה $a \in \mathbb{Z}_n$, נאמר כי קיים לו אביר הופכי אם קיים $b \in \mathbb{Z}_n$ כך ש-$a \cdot b \equiv 1 \pmod n$.
ל-b קוראים **האיבר ההופכי של a**, והוא מסומן ע"י: $\boldsymbol{a^{-1}}$.

הערה 3.6. בקבוצה $\mathbb{Z}_n^*$ נמצאים כל האיברים ההופכיים ל-n, כלומר, לכל $a \in \mathbb{Z}_n^*$ קיים $b \in \mathbb{Z}_n^*$ כך ש-$a \cdot b \equiv 1 \pmod n$.

משפט 3.7. אם p ראשוני אזי לכל $a \in \{1, \ldots, p-1\}$ קיים איבר הופכי.

הערה 3.8. אם $a \notin \mathbb{Z}_n^*$ אזי לא קיים ל-a איבר הופכי b.

4. משוואת מהצורה $ax \equiv b \pmod n$

הגדרה 4.1. עבור $a, b, n \in \mathbb{N}$: $ax \equiv b \pmod n$ פירושו: $n \mid (ax - b)$.

4.1 פתרון משוואות מהצורה $ax \equiv b \pmod n$

נפתור משוואות מהצורה $ax \equiv b \pmod n$ באופן הבא:
נסמן: $d = \gcd(a, n)$.

- אם $d = 1$ אזי ישנו פתרון יחיד שהוא: $x = a^{-1}b \pmod n$.
- אם $d > 1$, אזי יש שתי אפשרויות:
  - $d \nmid c$: $ax \not\equiv b \pmod n$ (אין פתרון למשוואה).
  - $d \mid c$: אזי למשווה $\frac{a}{d}x \equiv \frac{b}{b} \pmod{\frac{n}{d}}$ יש פתרון אחד מודולו $\frac{n}{d}$, אבל למשוואה $ax \equiv b \pmod n$ ישנן d פתרונות:

$$\left\{ \boldsymbol{x_0 + k \cdot \frac{n}{d}} \middle| \boldsymbol{k} \in \mathbb{N},\ \boldsymbol{0 \le k \le d - 1} \right\}$$

חלק II: הצפנה סימטרית

בהצפנה סימטרית הרעיון הוא שיש לנו מפתח משותף לשני הצדדים (לעומת הצפנה א-סימטרית ששמה לכל צד יש את המפתח שלו).

5. הצפנה חד-אלפבתית

בהצפנה חד-אלפבתית אנחנו מצפינים כל אות בנפרד, לעומת הצפנה רב-אלפבתית (בעמוד 7) ששמה אנחנו מצפינים בלוקים של אותיות.

5.1 צפני הזזה

בצפני הזזה אנחנו מזיזים את האותיות ע"י פונקציה כלשהי שתוגדר בהמשך (כי ישנם כמה אופנים).

5.1.1 סימונים

ישנו האלף-בית שמכיל n אותיות.

צורת רישום 5.1. P = מרחב הטקסט המקורי.

צורת רישום 5.2. C = מרחב הטקסט המוצפן.

צורת רישום 5.3. K = מרחב המפתחות.

$$P = C = K = \mathbb{Z}_n$$

$e\left(x\right)$ - זוהי פונקציית ההצפנה.
$d\left(x\right)$ - זוהי פונקציית הפענוח.

5.1.2 צופן הזזה כללי

פונקציית הצפנה: $\boldsymbol{e_k\left(x\right) = x + k \mod n}$

פונקציית פיענוח: $\boldsymbol{d_k\left(y\right) = y - k \mod n}$

כאשר x, y אילו אותיות בא"ב.
זהו צופן הצפנה פשוט שוב אנחנו פשוט עושים הזזה לאותיות.

5.1.3 צופן קיסר

דוגמה לצופן הזזה כללי הוא **צופן קיסר** שבו $k = 3$.

הצופן הטריוויאלי במקרה של הצפנה זאת, הצופן הטריוויאלי הוא כאשר $k = 0$.
אזי $e_k\left(x\right) = d_x\left(x\right) = x$.

5.1.4 התקפות על צופן הזזה

- אפשר באמצעות כוח גס. זה קל מאוד כי מספר המפתחות קטן מאוד ($|\mathbb{Z}_n|$) .
- ואם אנחנו יודעים את טקסט המקור, מספיק למצוא זוג אותיות (x,y) כך ש-y $e_k(x)=y$ ואז ניתן בקלות למצוא את המפתחות:

$$y \equiv x+k \pmod n \Rightarrow k \equiv y-x \pmod n$$

5.2 צופן החלפה

בצופן החלפה אנחנו מבצעים תמורה על כול האותיות. כלומר זוהי פונקציה:

$$\sigma : \mathbb{Z}_n \to \mathbb{Z}_n$$

ולכן מספר המפתחות הוא: $|\mathbb{Z}_n|!$.

5.2.1 התקפות על צופן החלפה

ניתן לתקוף את הצופן בקלות ע"י בדיקת תדירות של אותיות, ואם זה מספיק, ניתן לבדוק ע"פ צמדים, כלומר, ע"פ נפיצות של צמדי אותיות. למשל באנגלית: th, er. וכו'...

5.3 צופן אפיני

צפן אפיני הוא צופן טיפה יותר מורכב, אשר: $|\mathbb{Z}_n| = P = C$, אבל לעומת זאת $k = |\mathbb{Z}_n^*| \cdot |\mathbb{Z}_n|$.

$$\begin{aligned} \text{פונקציית הצפנה: } \quad & \boldsymbol{e_k(x) = ax+b \mod n} \\ \text{פונקציית פיענוח: } \quad & \boldsymbol{d_k(y) = a^{-1}(y-b) \mod n} \end{aligned}$$

כאשר: $a \in \mathbb{Z}_n^*$ ו-$b \in \mathbb{Z}_n$.

5.3.1 פענוח הצופן

הפעם בשביל הפענוח אנחנו זקוקים לשני אותיות מטקסט המקור ומהצופן כדי לפענח (וגם כאן, אם הטקסט מספיק ארוך, ניתן להשתמש בתדירות האותיות).
הסיבה לכך היא שיש לנו שני נעלמים (a,b) ולשם כך אנחנו צריכים שתי משוואות.
אם מדובר למשל על המרחב כמו ב-5.3.2 ונתון לנו כי $c \to t$ אזי המשוואה היא:

$$2a+b = 19 \pmod{26}$$

ובאופן כללי יותר:
נניח כי הפונקציה $\psi(A)$ מחזירה עבור A בא"ב את הערך המספרי שלו (למשל, ב-5.3.2: $\psi(d)=3$).
אזי, עבור A, C בא"ב: אם נתון לנו כי $A \to C$ אזי המשוואה תהיה:

$$\psi(A)\, a + b \equiv \psi(C)$$

5.3.2 דוגמאות לפענוח

בשתי הדוגמאות יהיה מדובר על ה-abc ולכן נדבר על $\mathbb{Z}_{26}$ כאשר בטקסט המקור C:
$0 \mapsto a, 1 \mapsto b, \ldots, 25 \mapsto z$.

דוגמה פשוטה נתחיל מדוגמה פשוטה: $gj \to ns$, כלומר:

$$\begin{cases} 6a+b \equiv 13 \pmod{26} & (1) \\ 9a+b \equiv 18 \pmod{26} & (2) \end{cases}$$

נחסר: $(1)-(2)$ ומה שנקבל הוא:

$$3a \equiv 5 \pmod{26}$$

וכעת נפתור את המשוואה ע"פ חלק 4.1:
$\gcd(3,26)=1$ ולכן יש פתרון אחד.
ההופכי של ב-$\mathbb{Z}_{26}$, ויש לו הופכי כי $3 \in \mathbb{Z}_{26}^{*}$, הוא 9 ולכן נכפול ב-9 ונקבל:

$$a = 19$$

כעת נציב, למשל ב-(1) ונקבל את b: $6 \cdot 19 + b \equiv 13 \pmod{26} \Leftarrow b=3$.
ולכן פונקציית ההצפנה היא: $e(x)=19x+3$,
ואילו פונקציית הפענוח היא: $d(y)=11(y-3)$.

דוגמה מורכבת יותר נעשה עוד דוגמה, רק שהפעם יהיה לנו "מכשול" בדרך...
נסתכל על: $gk \to nl$, כלומר: $e(10)=11$, $e(6)=13$, ולכן:

$$\begin{cases} 6a+b \equiv 13 \pmod{26} & (1) \\ 10a+b \equiv 11 \pmod{26} & (2) \end{cases}$$

כעת נעשה $(2)-(1)$ ונקבל:

$$22a \equiv 2 \pmod{26}$$

וישנה בעיה - $\gcd(22,26)=2 \neq 1$.
לכן, מה שנעשה הוא שנחלק את כל המשוואה ב-2 ונקבל:

$$11a \equiv 1 \pmod{13}$$

ההופכי של 11 ב-$\mathbb{Z}_{26}$ הוא 19 ולכן: $a=19$.
נציב באחת המשוואות, למשל ב-(1) ונקבל: $b=3$.
ופונקציית ההצפנה היא: $e(x)=19x+3$,
ופונקציית הפענוח היא: $d(y)=11(y-3)$.

6. הצפנה רב-אלפבתית

אם בהצפנה חד-אלפבתית הצפנו אות-אות, כאן אנחנו נצפין בבלוקים. כלומר, נצפין כל קבוצה של אותיות (בלוק) באותו אופן ולא אות-אות.

בחלק זה $\alpha, \beta, \gamma, \ldots$ יהיו מספרים ב-$\mathbb{N}$ או ב-$\mathbb{R}$.

6.1 צופן ויג'נר (Vigenere)

עובדים עם א"ב בגודל n. במקרה שלנו זה יהיה כמו ב-5.3.2 ונעבוד עם $\mathbb{Z}_{26}$.

- בוחרים מפתח באורך α, למשל: $[k,e,y] \leftrightarrow [10,4,24]$.
- השיטת ההצפנה עובדת כך:
  - מחלקים את טקסט המקור לבלוקים בגודל α.
  - על האות מספר i בבלוק עושים הזזה ב-k_i (כלומר, מוספים לה k_i).

חשוב לשים לב כי בדיקת תדירות האותיות אינה עוזרת במקרה כזה כיוון שכל אות מוצפנת באופן שונה. אבל אם בודקים לפי האות במקום ה-α בכל בלוק (בהנחה שאנחנו יודעים את אורך המפתח) אזי אפשר באמצעות כך להתחיל לפענח את הצופן.

6.1.1 דוגמה

ניקח את המפתח ממקודם: $[k,e,y] \leftrightarrow [10,4,24]$

וכעת נבצע הצפנה, למשל:

המילה שאותה נצפין	d	l	r	o	w	o	l	l	e	h
כמה נוסיף לכל אות	10	24	4	10	24	4	10	24	4	10
הטקסט המוצפן	n	j	v	y	u	s	v	j	i	r

כי למשל: $h = 7 \Rightarrow 7 + 10 = 17 = r$.

6.1.2 פיענוח הצופן

כדי לפענח את הצופן ישנם שני דברים שצריך לעשות:

1. למצוא את גודל המפתח.
2. למצוא את אותיות המפתח.

ישנן שתי שיטות לפענוח הצופן. אם אחת לא מספיק טובה ניתן להשתמש בשנייה.

6.1.3 מציאת אורך המפתח ע"י סיבוב הטקסט

מציאת התאמות ע"י סיבוב

אנחנו שמים את הטקסט מעל עצמו ומסובבים אותו ב-α.

למשל, אם טקסט המקור הוא: $abac$ אזי:

השורה הראשונה $\alpha = \ldots$ אומרת בכמה הזזנו את הטקסט ביחס לעצמו.

השורה השנייה - $abac$ - היא הטקסט.

השורה השלישית - היא הטקסט המוזז.

$\alpha = 1$	$\alpha = 2$	$\alpha = 3$
$abac$	$ab\underline{a}c$	$abac$
$caba$	$c\underline{a}b$	ca

נשים לב ששינה התאמה אחת כאשר $\alpha = 2$ (באות השלישית משמאל: a)

הרעיון הוא למצוא את ה-α שעבורו יש הכי הרבה התאמות (בדרך כלל במקום הזה תהיה קפיצה משמעותית במספר, בהנחה שמדובר בטקסט שהוא מספיק ארוך).

ואז ניתן לפענח בדרכים שמתוארות כאן: 6.1.5.

6.1.4 מציאת אורך המפתח ע"י מכפלה וקטורית

נסמן את את וקטור התדירויות של האותיות בטקסט המוצפן ב-$\mathscr{V}_0$ שזה הווקטור המקורי ללא הזזה, ב-$\mathscr{V}_1$ את הוקטור בהזזה ציקלית של 1 ימינה, כלומר, אם $\mathscr{V}_0 = [1, 2, 3, 4]$ אזי $\mathscr{V}_1 = [4, 1, 2, 3]$, $\mathscr{V}_2 = [3, 4, 1, 2]$ וכו'...

עבור $\alpha, \beta \in \mathbb{Z}_n$, כאשר n זה גודל הא"ב ו-$\alpha \neq \beta$ ההסתברות להתאמה היא:

$$\boxed{\mathscr{V}_\alpha \bullet \mathscr{V}_\beta = \sum_{i \in \mathbb{Z}_n} \left(\mathscr{V}_\alpha\left[i\right] \cdot \mathscr{V}_\beta\left[i\right]\right)}$$

ניקח את הערך **המקסימלי** של $\mathscr{V}_\alpha \bullet \mathscr{V}_\beta$ וזה יהיה כאשר או ש-$\alpha = \beta$ [בלתי אפשרי במקרה שלנו] או כאשר האותיות מוצפנות לפי אותה הצפנה (כלומר שההזזה ימינה היא לפי אורך המפתח או כפולה שלו).

נשים לב כי לשני הווקטורים ישנם את אותם רכיבים אך בסדר שונה.

חשוב לזכור ששתי השיטות האחרונות הינן הסתברותיות, כלומר, הם מאפשרות לנו לדעת בהסתברות גבוהה מה אורך המפתח אך לא מבטיחות לנו בוודאות שזהו אכן אורכו.

6.1.5 פענוח מילת המפתח

שיטה ראשונה:

השיטה הראשונה היא לפי תדירות האותיות.

ניקח את האות הראשונה בכל בלוק ונבדוק תדירות.

האות עם התדירות הכי גבוהה היא ככל הנראה e. (ומספיקה אות אחת כזאת כדי לדעת בכמה הזזנו...).

ככה נעשה לאות השנייה בכל בלוק וכו'...

אבל השיטה הזאת לא תמיד עובדת כי לפעמים נגלה שהאות השנייה בתדירות היא למשל k מה שאומר שככל הנראה פענחנו לא נכון (ואז גם לפענוח כולו לא תהיה משמעות).

לשם כך יש שיטה אחרת:
שעובדת ע"פ ההסתברות לקבל אות מסוימת.

הערה חשובה:

בשביל השיטה הזאת אנחנו צריכים שיהיה לנו וקטור ההסתברות של תדירות האותיות בא"ב שלנו באופן כללי.

ניקח את האות הראשונה בכל בלוק ונבנה וקטור תדירויות, באופן הבא:

כיצד בונים וקטור תדירויות:

נסמן: Σ = הא"ב שלנו (קבוצה לא ריקה וסופית של סימנים).
$|\Sigma| = n =$ מספר האותיות ב-א"ב שלנו, ועבור $\mathcal{A} \in \Sigma$ נסמן ב-$\phi\left(\mathcal{A}\right)$ את מספר המופעים של $\mathcal{A}$ בטקסט מסוים.
אזי עבור טקסט כלשהו, וקטור התדירויות יהיה:

$$\mathscr{U} = \left[\frac{\phi\left(\mathcal{A}\right)}{n}\middle|\mathcal{A} \in \Sigma\right]$$

חשוב לזכור שאם סוכמים את כל אברי הווקטור צריך לקבל 1.

אם $\mathscr{U}$ הוא וקטור התדירויות עבור טקסט מסוים, אזי נסמן ב-$\mathscr{V}_0$ את וקטור התדירויות של הא"ב בכללי ו-$\mathscr{V}_\alpha$ עבור $\alpha \in \mathbb{N}$ הוא הזזה ציקלית של הוקטור ב-α ימינה (כפי שתואר ב-6.1.4).
כעת מה שעלינו למצוא הוא:

$$\max\left\{\beta\middle|\beta = \mathscr{V}_\alpha \bullet \mathscr{U}\,,\ \alpha \in \mathbb{Z}_n\right\}$$

אחרי שנמצא את אותו ערך β מקסימלי אזי נמצא בהתאמה את אותו α שעבורו $\mathscr{V}_\alpha \bullet \mathscr{U}$ הוא מקסימלי, וה-α הזה זאת האות שאותה אנחנו מחפשים.
למשל, אם נעשה זאת על האות הראשונה בכל בלוק ונראה כי $\alpha = 0$ אזי האות הראשונה היא a.
ואם $\alpha = 2$ אזי נדע כי האות הראשונה היא c...
וכך הלאה.
השיטה הזאת בעיקרון יותר מוצלחת השיטה הקודמת.

7. צופן היל

צופן היל (Hill Cipher) הוא צופן שעובד על הצפנה של בלוקים באמצעות מטריצות.
כאשר מחלקים טקסט המקור לבלוקים בגודל $n \in \mathbb{N}$.

7.1 הצפנה

בשביל להצפין את טקסט המקור אנחנו צריכים מטריצה $M \in M_{n\times n}(\mathbb{Z}_m)$ **הפיכה** בגודל $n \times n$ (כאשר n זה גודל הבלוקים).
כאשר המספרים בתאי המטריצה הם במספרים ב-$\mathbb{Z}_m$ כאשר m הוא גודל הא"ב וכל מספר מסמל אות בא"ב.
למשל, נסתכל על ה-$abcd...$ (האותיות הלטיניות) כאשר $a=0, b=1, \dots, z=25$ אזי כל אברי המטריצה K יהיו ב-$\mathbb{Z}_{26}$, ונניח כי $n=2$ אזי המטריצה יכולה להיות:

$$M = \begin{bmatrix} 1 & 2 \\ 7 & 13 \end{bmatrix}$$

ונניח כי טקסט המקור שלנו הוא:
$rabbit$
אזי נחלק אותו לבלוקים של בגודל 2 $(ra|bb|it)$ ונכפול כל בלוק במטריצה, למשל, עבור הבלוק הראשון:

$$M \cdot \begin{bmatrix} r \\ a \end{bmatrix} = M \cdot \begin{bmatrix} 17 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 7 & 13 \end{bmatrix} \cdot \begin{bmatrix} 17 \\ 1 \end{bmatrix} = \begin{bmatrix} 19 \\ 2 \end{bmatrix} = tb$$

והתוצאה בסוף תהיה: $tbgour$.

7.2 פענוח

לשם פענוח אנחנו צריכים את M^{-1} (ואת גודל הבלוקים כמובן...).
במקרה שלנו:

$$M^{-1} = \begin{bmatrix} 13 & 2 \\ 7 & 25 \end{bmatrix}$$

ובשביל לפענח פשוט נחלק את הטקסט המוצפן לבלוקים בגודל 2 $(tb|go|ur)$ ונכפול אותם במטריצה M^{-1} כדי לקבל את את הטקסט המקורי.
כלומר, במקרה שלנו נתחיל מ-tb:

$$\begin{bmatrix} 13 & 2 \\ 7 & 25 \end{bmatrix} \cdot \begin{bmatrix} t \\ b \end{bmatrix} = \begin{bmatrix} 13 & 2 \\ 7 & 25 \end{bmatrix} \cdot \begin{bmatrix} 19 \\ 2 \end{bmatrix} = \begin{bmatrix} 17 \\ 1 \end{bmatrix} = \begin{bmatrix} r \\ a \end{bmatrix} = ra$$

וכך הלאה עד שנקבל בסוף: $rabbit$.

7.3 מציאת מטריצת ההצפנה

נניח ואנחנו לא יודעים מהי M, כיצד נוכל למצוא אותה?

הערה 7.1. אנחנו צריכים לדעת מה גודל הבלוקים, אם הוא לא נתון לנו אזי פשוט צריך לנסות גדלים שונים עד שנצליח...

אנחנו יודעים כי $rabb \to tbgo$ ולכן נבנה שתי מטריצות:

$$P = \begin{bmatrix} r & b \\ a & b \end{bmatrix}, C = \begin{bmatrix} t & g \\ b & o \end{bmatrix}$$

ואנחנו יודעים כי $M \cdot P = C$ ולכן:

$$M = C \cdot P^{-1}$$

הערה 7.2. יכול להיות שהמטריצה P אינה הפיכה. במצב כזה, נצטרך למצוא טקסט אחר שממנו נוכל לייצר את המטריצות הנ"ל (4 אותיות של הטקסט המקורי ו-4 אותיות המקבילות להן בטקסט המוצפן).

חלק III: הצפנות מודולו

8. חיבור מודולו 2 וקסור

$\mathbb{Z}_2 = \{0,1\}$ (ע"פ הגדרה 3.1, בעמוד 2).

עבור $x, y \in \mathbb{Z}_2$:

$$x + y \pmod 2 = x - y \pmod 2 = x \oplus y$$

והדבר נכון עבור m משתנים $x_1, \ldots, x_k \in \mathbb{Z}_2$:

$$\left(\sum_{1 \le i \le m} x_i\right) \bmod 2 = \bigoplus_{1 \le i \le m} x_i$$

הגדרה 8.1. ביט זוהי יחידה מאורך אחד אשר ערכה הוא ב-$\mathbb{Z}_2$, כלומר - ב-$\{0,1\}$.

9. הצפנות זרם

בהצפנות זרם אנחנו מצפינים כל ביט בנפרד (בניגוד להצפנת בלוקים).
טקסט המקור p, המפתח k והטקסט המוצפן c - כולם אוסף של ביטים באותו אורך m.
פונקציית ההצפנה:
לכל $1 \leq i \leq m$:

$$c_i = e(p_i) = p_i \oplus k_i = p_i + k_i \tag{1}$$

פונקציית הפענוח:
לכל $1 \leq i \leq m$:

$$p_i = d(c_i) = c_i \oplus k_i = c_i + k_i \tag{2}$$

כאשר:

p_i	זאת סיבית מטקסט המקור
k_i	זאת סיבית מהמפתח
c_i	זאת סיבית מהטקסט המוצפן

בכל הצפנות הזרם הבאות: פנקס חד-פעמי מחוללי סיביות אקראית ו-אוגר הזזה לינארי פונקציות ההצפנה (1) והפענוח (2) הן זהות.
כעת השאלה העיקרית היא **כיצד אנחנו יוצרים את המפתח?** כלומר, באיזו דרך הכי כדאי לנו ליצור מפתח.

9.1 פנקס חד-פעמי (OTP)

פנקס חד-פעמי זאת הצפנה מאוד חזקה וטובה (אפילו מושלמת!), הסיבה: משתמשים במפתח רק **פעם אחת** וזהו.
הפנקס מכיל סדרה אקראית של סיביות $k_0, k_1, k_2 \dots, k_m \in \mathbb{Z}_2$.

הערה 9.1. בגלל האקראיות של הסיביות בפנקס, הטקסט המוצפן לא יכול לגלות לנו שום דבר על טקסט המקור.

הערה 9.2. שימש בעיקר לתקשורת מחשבים באינטרנט להעברת מידע.

9.2 מחוללי סיביות אקראיות

9.2.1 $TNRG$

$TNRG$ - True Random Number Generator - זהו מחולל סיביות שאי אפשר לשחזר כיוון שהוא מבוסס על תופעות פיזיקליות.

9.2.2 $PRNG$

$PRNG$ - Pseudo Random Number Generator - זוהי סדרה של סיביות הנוצרת על-ידי חישוב ברקורסיה, למשל:

$$s_0 = 12$$
$$s_{i+1} = 115 s_i + 19 \bmod 3^{12}$$

הפתרונות הללו יותר קלים לשימוש מהפנקס החד-פעמי אבל אין בטיחות מושלמת כי הם לא אקראיים...

9.3 אוגר הזזה ליניארי $LFSR$

כאן מדובר בנוסחה שהרעיון שלה הוא לייצר "פסודו-אקראיות" - כלומר, משהו שיראה אקראי. מקובל להשתמש בצופן זה במקומות כמו טלוויזיה בכבלים - אשר דורשות מהירות גבוהה אך פחות בטיחות. הרעיון הוא שישנה נוסחת נסיגה, למשל:

$$z_{n+5} = z_2 + z_4 \mod 2$$

9.3.1 נוסחת הנסיגה

עבור נוסחת הנסיגה יש לנו m ערכים:
$z_1, \ldots, z_m$ ערכים התחלתיים
ו-$c_0, \ldots, c_{m-1}$ מקדמים.
(כל הנתונים הם כמובן ב-$\mathbb{Z}_2$)

$$Z_{m+n} = c_0 z_n + c_1 z_{n+1} + \cdots + c_{m-1} z_{n+m-1} \mod 2$$

הסיבה שבגללה אנחנו מתחילים ב-z_n היא שאנחנו מחשבים את הסיביות הבאות בסדרה.

9.3.2 תכונות של הצופן

הוא מאוד מהיר. אבל עם בטיחות נמוכה: עבור מפתח באורך m צריך $2m$ סיביות כדי לאתר את נוסחת הנסיגה (את הדרך נראה בהמשך).

הערה 9.3. מדובר במשהו מחזורי. כלומר, בגלל שיש נוסחת נסיגה, אזי היא יכולה לייצר לנו מחזור עד $2^m - 1$ ביטים (כלומר, אחרי זה - הסיביות כבר יתחילו לחזור על עצמן: $\underbrace{100110\ldots}_{2^m-1}\underbrace{100110\ldots}_{2^m-1}$

- כמובן שהמחזוריות יכולה להיות קטנה יותר.

9.3.3 מציאת נוסחת הנסיגה

לשם מציאת נוסחת הנסיגה אנחנו צריכים חלק מההודעה המקורית + חלק מהטקסט המוצפן או חלק מהסדרה שהאוגר יוצר.
הסיבה לכך היא שכמו שראינו בחיבור מודולו 2 ובנוסחה להצפנת זרם (1) אם נתונה לנו סיבית מטקסט המקור, למשל p_i וסיבית מהטקסט המוצפן c_i אזי כדי להגיע אליה חיברנו אליה סיבית מהמפתח k_i (שאותה כרגע אנחנו לא יודעים), אבל:

$$p_i + k_i = c_i$$
$$\Updownarrow$$
$$k_i = c_i - p_i = c_i + p_i$$

וכך נוכל לעשות לשאר הסיביות הנתונות.
כעת, כפי שנכתב בהערה 9.3 מדובר במשהו מחזורי. לכן אחרי שיש לנו את מספר סיביות של המפתח נוכל לנסות לשחזר את נוסחת הנסיגה וככה נוכל למצוא את המפתח באיזה אורך שנרצה.

9.3.4 מבנה נוסחת הנסיגה

בשביל להבין איך היא עובדת נסתכל על דוגמה פשוטה:

$$z_{n+3} = z_n + z_{n+2}$$

חשוב לזכור שאנחנו מתחילים מ-0, כלומר, הספרה במקום הראשון היא הספרה ה-0 והספרה במקום השני היא הספרה ה-1 וכך הלאה...
וכמובן - **כל החיבורים הם** $\mathrm{mod}2$**!**

במקרה הנ"ל: $m = 3$. כלומר, אנחנו נוכל למצוא את הסיבית הרביעית ואילך, ולכן אנחנו צריכים שיהיו לנו 3 סיביות בתור התחלה לפחות (אפשר גם יותר כמובן, אבל 3 זה המינימום). המקדמים הם: $c_0 = 1,\ c_1 = 0,\ c_1 = 1$. נניח והספרות שנתונות לנו הן: 010, אזי הספרה הרביעית, z_{n+3} היא הספרה של הסכום של $z_n + z_{n+2}$ - כלומר סכום הספרה הראשונה והשלישית:
הטקסט הכחול הוא הספרות שמצאנו באמצעות נוסחת הנסיגה, והספרות עם הקו התחתון אלו הספרות שאותן אנחנו מחברים:
עבור $n = 0$, נוכל למצוא את הספרה z_3 (כלומר, הספרה במקום הרביעי).
$z_3 = z_0 + z_2$:

$$\underline{0}1\underline{0} \longrightarrow 010\mathbf{0}$$

עבור $n = 1$:
$z_4 = z_1 + z_3$:

$$0\underline{1}0\underline{\mathbf{0}} \longrightarrow 010\mathbf{01}$$

עבור $n = 2$:
$z_5 = z_2 + z_4$:

$$01\underline{0}\mathbf{0}\underline{\mathbf{1}} \longrightarrow 010\mathbf{011}$$

וכך הלאה....
וכמובן שיכולים להיות יותר משני מחוברים, למשל:
$Z_{n+6} = z_{n+2} + z_{n+4} + z_{n+5}$

9.3.5 מציאת נוסחת הנסיגה

כמו שהוזכר למעלה - זאת הנוסחה הכללית:

$$Z_{m+n} = c_0 z_n + c_1 z_{n+1} + \cdots + c_{m-1} z_{n+m-1} \bmod 2$$

בהינתן סדרת ביטים, המטרה שלנו היא למצוא את m ולמצוא את המקדמים: $c_0,\dots,c_{m-1}$
עבור m מסוים, הדרך לפתור היא באמצעות משוואות:

$$\underbrace{\begin{pmatrix} z_1 & z_2 & \cdots & z_m \\ z_2 & z_3 & \cdots & z_{m+1} \\ \vdots & \vdots & \ddots & \vdots \\ z_m & z_{m+1} & \cdots & z_{2m-1} \end{pmatrix}}_{M} \cdot \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{m-1} \end{pmatrix} = \begin{pmatrix} z_{m+1} \\ z_{m+2} \\ \vdots \\ z_{2m} \end{pmatrix}$$

כלומר, אם סדרת הסיביות שלנו היא: $abcdefghi$ אזי:
עבור $m=2$:

$$\underbrace{\begin{pmatrix} a & b \\ b & c \end{pmatrix}}_{M} \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} = \begin{pmatrix} c \\ d \end{pmatrix}$$

עבור $m=3$:

$$\underbrace{\begin{pmatrix} a & b & c \\ b & c & d \\ c & d & e \end{pmatrix}}_{M} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} d \\ e \\ f \end{pmatrix}$$

וכך הלאה.
כמובן שיש הבדל בין c (אחד הביטים) ל-$c_0, c_1, \dots$ שאלו המקדמים.
כל פעם מנסים m אחר עד שמוצאים את נוסחת הנסיגה שנותנת לנו את סדרת הספרות שיש לנו.

עבור כל m:

1. אנחנו מחשבים את הדטרמיננטה של המטריצה השמאלית $\det(M) \bmod 2$ - אם $\det(M) \neq 0$ אז יש פתרון וממשיכים ל-2.
אחרת - עוברים ל-$m+1$.

2. פותרים את מערכת המשוואות ומקבלים את נוסחת הנסיגה וממשיכים לייצר ספרות על-פיה.

2.1. אם הגענו לסדרה שהייתה נתונה לנו במקור - סיימנו!

2.2. אחרת - עוברים ל-$m+1$.

9.3.6 דוגמה

נניח ונתונה לנו הסדרה הבאה: 1001001
אזי, בגלל שיש רצף של שני אפסים, אנחנו יודעים בוודאות כי $m>2$ (ובאופן כללי - אם יש לנו k אפסים בסדרה הנתונה, אזי $k<m$ בהכרח).
$m=3$:

$$\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}\begin{pmatrix}c_0\\c_1\\c_2\end{pmatrix}=\begin{pmatrix}1\\0\\0\end{pmatrix}$$

$\det(M)=1$ ולכן יש פתרון למשוואות:

$$c_0=1$$
$$c_1=0$$
$$c_2=0$$

(הכפלנו את וקטור המקדמים בכל שורה במטריצה, למשל, עבור השורה הראשונה: $c_0\cdot 1+c_1\cdot 0+c_2\cdot 0$).
ונוסחת הנסיגה שקיבלנו היא:

$$z_{n+3}=z_n$$

ועכשיו פותרים כמו שראינו כאן (9.3.4).
מה שנקבל הוא:

$$1001\rightarrow 10010\rightarrow 100100\rightarrow 1001001$$

ואכן קיבלנו את הספרות שבהתחלה. מכאן שזאת נוסחת הנסיגה.
אם היינו מקבלים למשל ספרות אחרות ממה שנתון לנו, או ש-$\det(M)=1$ - אזי היינו ממשיכים ל-$m+1$.

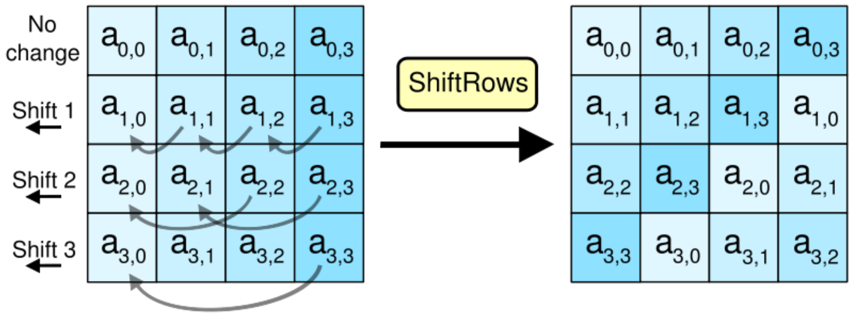
10. הצפנת בלוקים

הרעיון בהצפנת בלוקים דומה להצפנת זרם, רק שכאן במקום להצפין ביט-ביט אנחנו מצפינים בלוקים של ביטים, מה משמאוד משפיע על התוצאה.

10.1 AES

הצפנת AES - Advanced Encryption Standart - זוהי שיטת הצפנה נפוצה וחזקה שעובדת על בלוקים בגודל 128 **סיביות**. המפתח הוא באחד הגדלים הבאים:
$128, 192, 256$.
הצפנת ה-AES כוללת ארבעה שלבים:
ראשית כל מחלקים את הנתונים לחלקים של 16 ביטים, כל 16 ביטים נמצאים בתוך מטריצה 4×4.

1. תיבות החלפת בתים - כל ביט מוחלף בבית אחר ע"פ טבלה מסוימת.
2. סיבוב המטריצה - המטריצה אחרי ההחלפה מסובבת: השורה הראשונה נשארת כמו שהיא, בשורה השנייה - כל תא זז מקום אחד ימני, בשורה השלישית כל תא זז שני תאים שמאלה ובשורה השלישית כל תא זז שלושה תאים שמאלה:



3. שינוי עמודות המטריצה - כל עמודה עוברת כפל במטריצה מסדר 4×4 ומומרת לביטים חדשים.
4. תוספת של המפתח - לכל סיבית יש מפתח הנבנה מהמפתח הכללי אשר עובד על כל עמודה בנפרד.

10.2 הצפנת סדרה של צפני בלוקים

מקודם ב-AES ראינו כיצד ניתן להצפין בלוק, אבל מה קורה שיש לנו סדרה של בלוקים? בדיוק בשביל זה באה סדרת ההצפנות הבאה.

חלק IV:
RSA

בשביל להבין את אלגוריתם ה-RSA (Rivest–Shamir–Adleman) וכיצד הוא עובד נצטרך תחילה להכיר שיטות לבדיקה האם מספר הוא ראשוני או פריק.

11. בדיקת האם מספר n הוא פריק

כמובן שמדובר רק על מספרים ב-$\mathbb{N}$.

11.1 משפט אוילר

יהי $n \in \mathbb{N}$ ויהי $a \in \mathbb{Z}_n^*$ (כלומר: a, n הם מספרים זרים, ולכן $\gcd(a,n) = 1$).
אזי:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

כאשר $\varphi(n)$ זאת פונקציית אוילר.

11.2 המשפט הקטן של פרמה

זהו מקרה פרטי של משפט אוילר שבו n ראשוני, ואז:
$\varphi(n) = n - 1$, ולכן, לכל $1 \leq a < n$:

$$\boxed{a^{n-1} \equiv 1 \pmod{n}}$$

עכשיו, אפשר לומר ש"פתרנו את הבעיה", כי בשביל לדעת אם $p \in \mathbb{N}$ הוא ראשוני, פשוט ניקח מספר כלשהו $1 < a < p$ ונבדוק האם:

$$a^{p-1} \equiv 1 \pmod{p}$$

אם כן - הוא ראשוני (1.4), אם לא - הוא פריק (1.5).
אבל נמצאו מספרים שהם אינם ראשוניים ושעבורם מתקיים משפט פרמה. אלו נקראים **מספרי קרמייקל**
לכן משפט פרמה לא מספיק לנו וצריך בדיקה אחרת.

11.3 אלגוריתם רבין-מילר

11.3.1 הרעיון הכללי

עבור $n \in \mathbb{N}$, מחפשים עד לפריקות n -
אם מוצאים עד כזה (או שמוצאים שישנו, אבל לא מוצאים את העד עצמו) - אזי המספר בוודאות פריק.
אם לא מוצאים עד לפריקות - אז מכריזים כי המספר ראשוני (אבל זה נכון בהסתברות $< \frac{3}{4}$).

האלגוריתם עצמו מתחלק לשני אלגוריתמים:
הראשון - עבור $a < n$ - האם a הוא עד לפריקות?
השני - האם n הוא ראשוני או פריק.

11.3.2 מציאת עד לפריקות על בסיס a

כפי שראינו מקודם עבור a, n זרים לא מספיק לבדוק האם $a^{n-1} \equiv 1 \pmod n$ (משפט פרמה), לכן מה שצריך לעשות הוא:
למצוא r, j כך ש: $n - 1 = r \cdot 2^j$ (למשל, עבור $n = 29$ אזי $n - 1 = 28$ ולכן: $r = 7, j = 2$ כי $28 = 7 \cdot 2^2$).

אלגוריתם 1 האם a הוא עד לפריקות n

קלט: זוג מספרים טבעיים a, n כך ש-$n > a$.
פלט: האם a עד לפריקות n ואם כן וניתן למצוא את המחלק - אזי האלגוריתם מחזיר גם אותו.

1. מוצאים r, j כך ש: $n - 1 = r \cdot 2^j$.
2. $b_0 = a^r \pmod n$.
3. אם $b_0 \equiv \pm 1 \pmod n$ - אזי החזר כי n כנראה ראשוני (כל השלבים הבאים באלגוריתם ייתנו את אותה תוצאה, ולכן אין טעם להמשיך).
4. עבור $i = 1$ עד $i = j - 1$:
   4.1. $b_i = b_{i-1}^2 \pmod n$.
   4.2. $b_i \equiv 1 \pmod n$ - החזר כי המספר n פריק ואת b_{i-1} בתור העד לפריקות.
   4.3. $b_i \equiv -1 \pmod n$ - החזר כי המספר n כנראה ראשוני.
5. החזר כי n פריק (ללא עד). (כי מה שקורה הוא שהגענו למצב ש-$a^{r \cdot 2^j} = a^{n-1} \not\equiv 1 \pmod n$ ולכן ע"פ פרמה המספר אינו ראשוני).

11.3.3 אלגוריתם רבין-מילר

נגדיר את האלגוריתם הקודם (האם a הוא עד לפריקות n) בתור $W(a, n)$.

אלגוריתם 2 אלגוריתם רבין-מילר

קלט: מספר טבעי n.
פלט: האם המספר הוא ראשוני, ואם האלגוריתם מוצא גם עד לפריקות.

1. הגרל מספר $1 < a < n$ (לא חייב להיות מוגרל, יכול להיות שנרצה לבחור את a).
2. בדוק האם $W(a,n)$ אומר כי n פריק.
   2.1. אם כן - החזר כי n פריק (ואם ישנו גם את העד לפריקות).
   2.2. אחרת - חזור ל-1 או סיים והחזר כי המספר כנראה ראשוני.

ברגע שהאלגוריתם מחזיר לנו עד w, אזי $\gcd(w,n) \neq 1$ וכך ניתן לפרק את n.

12. אלגוריתם ה-RSA

אלגוריתם ההצפנה RSA עובד בצורה אסימטרית, כלומר לכל אחד מהצדדים יש את המפתח שלו.

12.1 בניית המפתח

מוצאים שני מספרים ראושניים (עדיף גדולים), ומחשבים את:

1. $n = p \cdot q$.
2. $\varphi(n) = (p-1)\cdot(q-1)$ (כאשר $\varphi(n)$ זאת פונקציית אוילר).
3. מוצאים e כך ש-$1 < e < \varphi(n)$ ו-$e, \varphi(n)$ זרים, כלומר, $\gcd(e, \varphi(n)) = 1$.
4. מחשבים: $d = e^{-1} \pmod{\varphi(n)}$.

המפתח הציבורי: $K_{pub} = (n,e)$ (את זה אנחנו **מפרסמים**).
המפתח הפרטי: $K_{pr} = d$ (את זה אנחנו **שומרים בסוד**).

12.2 הצפנה ההודעה

נניח וההודעה שאנחנו רוצים להצפין היא x, כאשר $1 < x < n$, אזי:

$$y = E(x) = x^e \pmod{n}$$

נזכיר: אם אפרת רוצה לשלוח את ההודעה x לבני, אזי היא מסתכל על המפתח הציבורי שלו (n,e) וכך מצפינה את x.

12.3 פענוח ההודעה

בני רוצה לפענח את ההודעה שאפרת שלחה לו (y), לשם כל מה שהוא צריך לעשות זה:

$$D(y) = y^d \pmod{n} = x$$

12.3.1 פענוח בעזרת משפט השאריות הסיני

מתחילים בכמה חישובים של הכנות:
אנחנו רוצים לחשב את $x^d \pmod{n}$ כאשר $n = p \cdot q$.
מחשבים:

1. עבור p:
   1.1. $M_p \equiv q \cdot \left(q^{-1} \pmod{p}\right)$.
   1.2. $d_p \equiv d \pmod{p-1}$.
   1.3. $x_p \equiv x \pmod{p}$.
   1.4. $y_p \equiv x_p^{d_p} \pmod{p}$.
2. עבור q:
   2.1. $M_q \equiv p \cdot \left(p^{-1} \pmod{q}\right)$.
   2.2. $d_q \equiv d \pmod{q-1}$.
   2.3. $x_q \equiv x \pmod{q}$.
   2.4. $y_q \equiv x_q^{d_q} \pmod{q}$.

ואז מחשבים:

$$\boxed{x^d \equiv y_p \cdot M_p + y_q \cdot M_q \pmod{n}}$$

12.4 כלים שעוזרים לנו בביצוע החישובים

בשביל שנוכל לעשות את החישובים ביעילות ישנם שני אלגוריתמים (העלה בחזקה וחישוב הופכי) שהחישוב שלהם יותר מהיר וקל.

12.4.1 אלגוריתם להעלאה בחזקה

המון פעמים נרצה לחשב את $a^b \pmod{n}$, אבל הבעיה שהעלה בחזקה יכול לקחת המון זמן, לשם כך יש את האלגוריתם הבא:

אלגוריתם 3 אלגוריתם העלאה בחזקה

קלט: $x, c, n \in \mathbb{N}$.
פלט: $x^c \pmod{n}$.

1. ממירים את c (החזקה) לצורה בינארית, כאשר c_t זאת הספרה הכי שמאלית ו-c_0 זאת הספרה הכי ימנית.
2. $z = 1$.
3. עבור $i = t$ עד $i = 0$:
   3.1. $z^2 \pmod{n} \to z$.
   3.2. אם $c_i = 1$ אזי $z \cdot x \pmod{n} \to z$
4. החזר את z וסיים.

דוגמה 12.1. נחשב את $3^{10} \bmod 5$:
10 בבינארית זה **1010**
ולכן:
נחשב את $3^{1010} \bmod 5$:
לכן, אנחנו נחשב את ההעלאה בחזקה בהתאם לספרות בסדר הבא: $\overrightarrow{1010}$.
בהתחלה $z=1$, נעלה אותו בריבוע ונקבל: $z=1$, ואז נכפול ב-3 ונקבל: $z=3$.
לאחר מכן יש לנו רק 0, ולכן: $z=3^2 \bmod 5 = 4$.
לאחר מכן יש לנו 1 - לכן נעלה את z בריבוע: $z=4^2 \bmod 5 = 1$ ואז נכפיל ב-3. קיבלנו 3.
לבסוף יש לנו 0 - לכן נעלה את זה z בריבוע: $z=3^2 \bmod 5 = 4$,
וזאת התוצאה הסופית: $\mathbf{3^{10} \bmod 5 = 4}$.

הערה 12.2. נעדיף מספרים כמו 3 $(11)_2$ או 17 $(10001)_2$ שיש בהם מעט אחדות כך שהם דורשים מעט פעמים כפל (שלב 3.2).

12.4.2 חישוב ההופכי

כמו שראינו, בבניית המפתח עלינו לחשב את ההופכי.

חלוקה עם מנה ושארית נניח כי יש לנו שני מספרים: $x,n \in \mathbb{N}$ כך ש-$x<n$ ואנחנו רוצים "לחלק" את n ב-x אזי ניתן לרשום את זה באופן הבא:

$$n = qx + r$$

כאשר q - זאת המנה.
ו-r - זאת השארית $(0 \le r \le n-1)$.

דוגמה 12.3. נחלק 14 ב-3: $14 = 4 \cdot \underline{3} + 2$, אזי המנה היא 4 והשארית היא 2.

דוגמה 12.4. נחלק 22 ב-21: $22 = 1 \cdot \underline{21} + 0$, המנה היא 1 והשארית היא 0.

האלגוריתם המורחב של אוקלידס למציאת gcd עבור שני מספרים $a,b \in \mathbb{N}$ נרצה לחשב את $\gcd(a,b)$ לשם כך יש לנו את האלגוריתם הבא:

אלגוריתם 4 האלגוריתם המורחב של אוקלידס לחישוב ה-gcd

קלט: $a,b \in \mathbb{N}$ (ונניח כי $a>b$).
פלט: $d = \gcd(a,b)$.

1. חלק את a ב-b עם שארית כך ש: $a = q \cdot b + r$.
2. כל עוד $r>0$:
   2.1. $a \to b$.
   2.2. $b \to r$.
   2.3. חזור ל-1.
3. החזר את b.

מקדמי בז'ו אם $d=\gcd(a,b)$ אזי קיימים שני מספרים $s,t\in\mathbb{Z}$ כך ש-d $= s\cdot a+t\cdot b$. s,t נקראים **מקדמי בז'ו**.
בשביל להבין איך למצוא אותם נצטרך להפעיל על שני מספרים כלשהם את האלגוריתם המורחב של אוקלידס.
ניקח $a=22, b=17$.

i	a	b	q_i		
0	22	17	1	$22=1\cdot 17+5$	
1	17	5	3	$17=3\cdot 5+2$	
2	5	2	2	$5=2\cdot 2+1$	
3	2	1	0		

ונחזיר את 1 כי באיטרציה מספר 3: $b=1, r_3=0$, ולכן נעצור ונחזיר אותו.
כעת נשים לב לסדרה של המנה: q_i: $1,3,2$.
ניתן לחשב את מקדמי בז'ו ע"פ הנוסחאות הבאות:
מחשבים: $s_0,s_1,\ldots,s_m$ ואת $t_0,t_2,\ldots,t_m$.
עבור $2\le i\le m$

$$s_0=0,\ s_1=1, s_i=-q_{i-1}\cdot s_{i-1}+s_{i-2}$$
$$t_0=1,\ t_1=0, t_i=-q_{i-1}\cdot t_{i-1}+t_{i-2}$$

ולבסוף:

$$\boxed{\boldsymbol{s_m a+t_m b=r_m=\gcd(a,b)}}$$

כאשר s_m,t_m אלו הם מקדמי בזו ובאמצעותם ניתן למצוא את האיבר ההופכי.
כיצד?
נניח ואנחנו רוצים למצוא את ההופכי של $3 \pmod 7$ (וישנו הופכי כי $\gcd(3,7)=1$), אזי מה שנעשה הוא שנפעל מתואר למעלה:
נקבל משוואה:

$$s\cdot 3+t\cdot 7=1$$

כאשר s,t הם מקדמי בז'ו.

$$s\cdot 3=1-t\cdot 7$$

ולכן ה-s הוא ההופכי של 3 ב-$\mathbb{Z}_7$.

13. התקפות על RSA

אנחנו יודעים ש-n הוא מכפלה של שני ראשונים: p,q, כלומר:

$$n=p\cdot q$$

לכן, המטרה שלנו היא למצוא את שני המספרים הראשוניים הללו.
ראשית כל אנחנו יכולים להשתמש בבדיקת ראשוניות: בדיקת האם מספר n הוא פריק (בעמוד 17)
כדי לדעת האם מדובר במספר ראשוני.
בהנחה שמצאנו שהוא אינו ראשוני - ישנן מספר דרכים למצוא את p,q.

13.1 פירוק לגורמים

13.1.1 הפירוק של פרמה

אם $n=x^2-y^2$ אזי יש לנו פירוק: $n=(x+y)(x-y)$.
לכן אנחנו מחפשים x כך ש-y הוא מספר שלם כאשר $y=\sqrt{x^2-n}$.
מתחילים מ-$x=\lceil\sqrt{n}\rceil$ וכל פעם מעלים את x ב-1.

אלגוריתם 5 אלגוריתם הפירוק של פרמה

קלט: $n\in\mathbb{N}_+$.
פלט: $x,y\in\mathbb{N}_+$ כך ש: $(x+y)(x-y)=n$.

1. חשב את $x=\lceil\sqrt{n}\rceil$.
2. כל עוד $\sqrt{x^2-n}$ אינו שלם:
   2.1. $x+1\to x$
3. $y=\sqrt{x^2-n}$.
4. החזר: $(x+y),(x-y)$ וסיים.

13.1.2 $p-1$ של פולארד

הרעיון:
אנחנו יודעים כי אם p ראשוני, אזי לכל $a\in\mathbb{Z}_p$: $a^{p-1}\equiv 1$, לכל m כך שלכל m כך ש-$m \mid p-1$:
$a^m\equiv 1$.

דוגמה 13.1. נסתכל על $p=7$, ו-$p-1=6$ אזי:

$$3^6\equiv 1 \pmod 7 \Rightarrow 3^{18}\equiv 1 \pmod 7$$

ו-$6 \mid 18$.

כעת אם $p-1$ מתחלק לראשוניים קטנים למשל: אם $p=71$ אזי $p-1=70=2\cdot 5\cdot 7$.
ולכן: $p-1 \mid 7!$.
לכן, עבור k לא גדול: $p-1 \mid k!$ ו-$a^{k!}\equiv 1 \pmod p$
כעת, אם $a^{k!}\not\equiv 1 \pmod n$ אזי ניתן למצוא ככה את אחד הגורמים של n: $\gcd\left(a^{k!}-1,n\right)=p$
והצלחנו לפרק את n!

אלגוריתם 6 אלגוריתם $p-1$ של פולארד

קלט: $n \in \mathbb{N}_+$ וחסם B.
פלט: פירוק של n.

1. $a = 2$.
2. עבור $k = 2$ עד B:
   2.1. $a^k \pmod{n} \to a$ (מחשבים את $a^{k!} \pmod{n}$).
   2.2. $\gcd(a-1, n) \to d$.
   2.3. אם $1 < d < n$ החזר את d וסיים (מצאנו גורם של n).
3. החזר "כישלון בפרוק n" וסיים.

מסקנה 13.2. צריך לבחור p, q כך ש-$p-1, q-1$ יש לפחות גורם ראשוני אחד גדול.

13.1.3 אלגוריתם "רו" (ρ) של פולארד

הרעיון:
מגדירים סדרה פסודו-אקראית $x_{i+1} = g(x_i)$ של מספרים מודולו n.
בגלל עקרון שובך היונים הסדרה חייבת להיות מחזורית מודולו n ועבור מודולו אחד הגורמים של n היא צריכה להיות בעלת מחזור קטן יותר, כלומר באיזושהי נקודה (עבור איזשהו מספר) הסדרה תצטרך לחזור על עצמה כמו האות היוונית ρ (רו).
בשלב k מחשבים את x_k ואת x_{2k}, ברגע שנקבל:

$$x_{2k} \equiv x_k \pmod{p}$$

כש-p הוא גורם של n אזי נקבל: $\gcd(|x_{2k} - x_k|, n) = p$ וקיבלנו גורם של n.

אלגוריתם 7 אלגוריתם "רו" ρ של פולארד

קלט: $n \in \mathbb{N}_+$ ו-$x_0 \in \mathbb{N}_+$ ערך התחלתי. פולינום $g(x)$ (שבד"כ הוא שווה ל-$g(x) = x^2 + 1$) .
פלט: אחד הגורמים של n.

1. $1 \to d$, $x_0 \to y$, $x \to x_0$.
2. כל עוד $d = 1$:
   2.1. $g(x) \bmod n \to x$.
   2.2. $g(g(x)) \bmod n \to y$.
   2.3. $\gcd(|x-y|, n) \to d$.
3. אם $d = n$ החזר "כישלון" וסיים. אחרת החזר את d וסיים.

13.1.4 אלגוריתם "בסיס גורמים" ("נפה ריבועית")

הרעיון נניח כי קיימים a, b כך ש:

$$a^2 \equiv b^2 \pmod{n}$$

אבל $a \not\equiv b \pmod n$, אזי אנחנו יודעים כי $n \mid \left(a^2-b^2\right)$ (ע"פ ההגדרה) אבל $n \nmid (a \pm b)$ אז איך כן מפרקים את n?
באופן בסיסי הרעיון הוא כזה (כל החישובים הם מודולו n):

$$a^2 = 2^3 \cdot 3 \cdot 5^2$$
$$b^2 = 2 \cdot 3 \cdot 5^4$$
$$\Updownarrow$$
$$(a \cdot b)^2 = 2^4 \cdot 3^2 \cdot 5^6 = \left(\overbrace{2^2 \cdot 3 \cdot 5^3}^{c}\right)^2$$

אזי $\gcd(n, ab-c)$ הוא גורם של n. המטרה להגיע למצב כזה.
מה שחשוב זה ש: **זה לא יהיה אותו מספר בריבוע** (כלומר, שנכפול מספר גורמים ולא את הגורם בעצמו) **ושכל החזקות יהיו זוגיות**.

איך מוצאים את a, b?

1. בוחרים מספר קטן B (חסם לראשוניים).
2. מחפשים מספרים m_i שהם קצת יותר גדולים מ-$\sqrt{n}$ ו-$m_i^2 \pmod n$ מתפרק לראשוניים $p_1, \ldots, p_k \leq B$.
3. מכפילים כמה מהפירוקים הללו (למשל a^2, b^2 כמו בדוגמה למעלה) כדי לקבל שיוויון בין ריבועים (c^2 בדוגמה למעלה).
4. $\gcd(n, ab-c) \neq 1$ והוא מחלק את n.

הערה 13.3. אלו יכולים להיות כמובן יותר משני מספרים, ואז במקרה כזה, נוכל לכפול יותר משני מספרים כדי להגיע למצב שבו כל החזקות זוגיות כדי שנוכל להוציא שורש.

חלק V:
חתימות דיגיטליות

14. הרעיון הכללי של החתימה

חתימה דיגיטלית <u>**אינה**</u> חלק מהמסמך.

חשוב שיהיה בלתי אפשרי להשתמש באותה חתימה על מסמך אחר.
וכמובן - שיהיה אפשר לבדוק את אמיתותה.

14.1 למה מיועדת החתימה?

החתימה מיועדת לכך שניתן יהיה לוודא בוודאות ש:

1. ההודעה לא השתנתה בדרך (מכל מיני סיבות).
2. השולח זה אכן מי שאנחנו חושבים שהוא.

ככה קשה לזייף את ההודעה או את המקור (השולח) שלה.

15. חתימה דיגיטלית מבוססת RSA

כמו בחלק של בניית המפתח ב-RSA גם כאן:

$$n = p \cdot q, \quad e \cdot d \equiv 1 \bmod \varphi(n)$$

חתימת ההודעה $x \in \mathbb{Z}_n$:

$$y = \operatorname{sig}_K(x) \equiv x^d \pmod n$$

כאשר הטקסט החתום הוא הזוג: (x, y).
בדיקה:

$$\operatorname{ver}_K(x, y) = True \iff x \equiv y^e \pmod n$$

15.1 התקפות על חתימות RSA

15.1.1 רמות שונות של התקפות על חתימות

1. התקפה עם מפתח בלבד: איב (התוקפת) מכירה רק את המפתח הציבורי ולכן את אלגוריתם הבדיקה (התקפה הכי פשוטה).
2. התקפת הודעות מוכרות: לאיב יש כמה הודעות חתומות על ידי אפרת (ולכן קל לה יותר יהיה לזייף חתימה, דוגמה בהמשך).
3. התקפת הודעות נבחרות: איב מקבלת כמה חתימות של אפרת על כמה הודעות שהיא (איב) בוחרת, וככה יותר קל לה לתקוף.

15.1.2 מטרות של ההתקפות

להתקפות שציינו למעלה יש מספר מטרות:

1. פיצוח מלא: איב (התוקפת) מצליחה לגלות את המפתח הסודי של אפרת ולכן יכולה לחתום במקומה וכך אי אפשר יהיה לדעת מי חתמה - אפרת או איב.
2. זיוף סלקטיבי: איב מצליחה לחתום בהצלחה על הודעה שנבחרה מראש על-ידי מישהו אחר.
3. איב מצליחה ליצור הודעה עם חתימה תקנית (זה לא אומר בהכרח שלהודעה יש משמעות, אבל בבדיקת האמיתות, תהיה תוצאה חיובית).

15.1.3 דוגמה לזיוף קיומי

זיוף קיומי עם מפתח בלבד:
איב בוחרת חתימה y ומחשבת את $x \equiv y^e \pmod{n}$ - כך יוצא ש-y היא חתימה תקנית של x (ל-x לא בהכרח יש משמעות).

15.1.4 דוגמה לזיוף סלקטיבי

כך ניתן לזייף חתימה על הודעה סלקטיבית x:
איב רוצה לזייף את החתימה להודעה x, לשם כך היא מוצאת $x_1, x_2 \in \mathbb{Z}_n$ כך ש-$x \equiv x_1 \cdot x_2 \pmod{n}$ ומבקשת מאפרת לחתום על שתי ההודעות x_1, x_2.
אם איב תכפיל את שתי החתימות - היא תקבל חתימה תקנית של x.

16. חתימות דיגיטליות מבוססות פונקציות גיבוב

16.1 פונקציות גיבוב

הגדרה 16.1. פונקציית גיבוב קריפטוגרפית h היא פונקציה שלוקחת קלט באורך כלשהו ומחזירה פלט באורך קבוע.
ישנן כמה דברים נוספים שחשוב לקחת בחשבון:

1. עבור הודעה נתונה m - קל לחשב את הפלט $h(m)$.
2. אבל, מצד שני - קשה יהיה למצוא הודעה m כך שהפלט שלה יהיה $h(m)$ (במילים אחרות: אם נתון לנו $h(m)$, קשה מאוד לדעת מהי m). בנוסף, מדובר בפונקציה חד-כיוונית[1].
3. קשה למצוא שתי הודעות עם אותו פלט תחת פונקציית הגיבוב.

16.2 התקפת יום ההולדת

16.2.1 פרדוקס יום ההולדת

ישנם 23 אנשים בחדר, מה ההסתברות שאין לאף שניים מהם יום הולדת באותו יום היא:

$$\prod_{i=1}^{22}\left(1-\frac{i}{365}\right)=0.495$$

כלומר, הסיכוי שלשניים מתוך 23 האנשים יש יום הולדת באותו יום היא גדולה מ-$\frac{1}{2}$!
ובאופן כללי יותר:
נניח כי שתי קבוצות של r אנשים בוחרים איבר מאוסף של N איברים. , אזי הסיכוי שמישהו מהקבוצה הראשונה יבחר משהו כמו מישהו מהקבוצה השנייה הוא בערך:

$$\boxed{1-e^{\frac{-r^2}{N}}}$$

[1] כלומר, פונקציה שאין אפשרות לדעת מה היה הקלט היות ומספר קלטים יכולים להחזיר את אותה תוצאה, למשל: $h(m) = h \bmod 7$, במקרה כזה, אם למשל $h(m) = 3$ לא נוכל לדעת מה הייתה n (אבל בניגוד ל-2, לא קשה למצוא m כך ש-$h(m) = 3$).

ואם למשל מדובר על ימי הולדת, ועל שתי קבוצות בנות 30 איש כל אחת, אזי הסיכוי שלמישהו מהקבוצה הראשונה תהיה אותה יום הולדת כמו למישהו בקבוצה השנייה היא:

$$1-e^{\frac{-30^2}{365}}=0.915$$

16.2.2 שימוש בפונקציות גיבוב

אם לפלט של פונקציות גיבוב יש n סיביות, אזי ישנם $2^n=N$ פלטים אפשריים.
לכן, עבור שני אוספים של בערך $\sqrt{N}$ פלטים, ההסתברות שיהיו שני פלטים זהים (אחד בכל אוסף) היא בערך: $1-e^{-1}\approx 0.6$.

דוגמה 16.2. אפרת חתמה על חוזה עם הילי (החוזה הטוב), אבל הילי רוצה לרמות את אפרת ולגרום לה לחתום על חוזה מזויף (החוזה הרע).
נניח כי אורך הפלט של פונקציית הגיבוב הוא 50סיביות, לכן מספר הפלטים האפשריים הוא 2^{50}.
הילי מכינה 2^{30} גרסאות שונות של החוזה הטוב ו-2^{30} של החוזה הרע. היא מחשבת את הפלט שלהם תחת פונקציית הגיבוב.
ע"פ מה שראינו למעלה, ההסתברות שהילי תקבל חוזה טוב וחוזה רע עם אותו הפלט היא:

$$1-e^{\frac{-2^{60}}{2^{50}}}=1-e^{-2^{10}}\approx 1$$

כלומר, ברגע שהילי תקבל שני חוזים כאלו היא תוכל לגרום לאפרת לחתום על החוזה המזויף וזה יראה כאילו היא חתמה על אותו חוזה.

<u>מה אפרת יכולה לעשות?</u>
כל מיני דברים, למשל:

1. ברגע האחרון אפרת יכולה לבקש שינוי קטן בחוזה, ואז להילי יהיה קשה מאוד למצוא חוזה רע עם אותו הפלט (סעיף 3).
2. אפרת יכולה לשמור עותק של המסמך שעליו היא חתמה כדי להוכיח שהחתימה שלה היא חתימה תקינה לחוזה (וככה היא תראה את התקינות של החתימה שלה על העותק שלה, וככה יהיה יותר קשה לזייף כי יראו שני חוזים שונים שלשניהם החתימה תקפה).

17. סוגים מיוחדים של חתימות דיגיטליות

עד עכשיו דיברנו על חתימות באופן כללי ועל הצורך בהן. עכשיו נדון על סוגים מיוחדים של חתימות.

17.1 חתימה חד-פעמית (למפורט)

מתבססת על פונקציה חד-כיוונית (למשל, פונקצית גיבוב קריפטוגרפית): $F:X\to Y$.
הרעיון:
חותמים על כל סיבית בנפרד.
לכל סיבית i בוחרים שני מפתחות סודיים $K_{i,0},K_{i,1}\in X$ ולכל אחד מהמפתחות קובעים ערך ציבורי: $f\left(K_{i,0}\right),f\left(K_{i,1}\right)\in Y$.
אם הסיבית ה-i-ית שווה ל-0 אזי החתימה של הסיבית ה-i היא $K_{i,0}$ ואם היא 1 אזי החתימה שלה היא $K_{i,1}$.

דוגמה 17.1. נניח כי הפונקציה החד-כיוונית f היא $f(x) = 2^x \bmod 17$ [2]:

$y_{1,0} = f(x_{1,0}) = 16$	$x_{1,0} = 12$
$y_{1,1} = f(x_{1,1}) = 9$	$x_{1,1} = 7$
$y_{2,0} = f(x_{2,0}) = 15$	$x_{2,0} = 13$
$y_{2,1} = f(x_{2,1}) = 2$	$x_{2,1} = 9$
$y_{3,0} = f(x_{3,0}) = 1$	$x_{3,0} = 8$
$y_{3,1} = f(x_{3,1}) = 13$	$x_{3,1} = 14$

הרעיון הוא כזה: לכל ביט אנחנו מצמידים שני מפתחות - אחד למקרה שהוא 0 והשני למקרה שהוא 1. עוברים על ההודעה סיבית-סיבית ומצפינים בהתאם. כאן למשל, הטבלה חולקה לפי צבעים: השורות הכחולות - לסיבית הראשונה, השורות הירוקות - לסיבית השנייה, והאדומות לשלישית.
נסתכל על הצפנת ההודעה הבאה:

$$101$$

הסיבית הראשונה, מוצפנת בהתאם לשורות הכחולות והיות והיא 1 אזי: הולכים להיכן שיש 1: $x_{1,1}$, ולכן:

$$f(x_{1,1} = 7) = 9$$

ואז ממשיכים לסיבית הבאה שהיא 0. היות ומדובר בסיבית השנייה אזי נלך לשורות הירוקות ושמה לשורה הראשונה $x_{2,0}$ (אם הסיבית השנייה הייתה 1 היינו הולכים לשורה השנייה $x_{2,1}$):

$$f(x_{2,0} = 13) = 15$$

ובסוף נלך לשורה השנייה כי הסיבית השלישית היא 1:

$$f(x_{3,1} = 14) = 13$$

ולכן, החתימה להודעה היא:

$$(9, 15, 13)$$

דוגמה 17.2. ניקח את אותה פונקציה וטבלה כמו בדוגמה הקודמת. אם היינו רוצים לחתום את ההודעה: 011, אזי החתימה שלה הייתה:

$$(16, 2, 13)$$

[2] זאת דוגמה ממש פשוטה, אבל היא ממחישה את הרעיון.

בדיקת הנכונות היא מאוד פשוטה:
נתונה לנו הטבלה, לכן מה שצריך לבדוק זה את איך חותמים את ההודעה לפי הטבלה הנתונה לנו.
כלומר, אם נתונה לנו ההודעה 101 והחתימה $(9, 15, 13)$ - אזי נדע כי החתימה תקינה, אך אם לעומת זאת עבור ההודעה 011 נבל אותה עם החתימה $(15, 2, 13)$ - נדע כי החתימה פגומה ולא נוכל לסמוך על מקור ההודעה.

יתרונות:

- קשה מאוד לזייף חתימה כזאת כיוון שמאוד קשה לחשב את פונקציית המקור החד-כיוונית.
- נחשב כעמיד נגד מחשבים קוונטיים.

חסרונות:

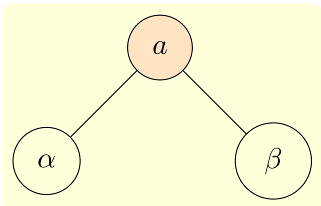
- המפתח מאוד ארוך: שתי זוגות למפתח הפרטי ($x_{i,\{0,1\}}$) ושתי זוגות למפתח הציבורי ($y_{i,\{0,1\}}$).
- לא בטיחותי עם משתמשים באותו מפתח כדי לחתום על יותר מהודעה אחת (כלומר, אם חותמים גם על 1011 ועל 0110 אזי ניתן לדעת גם מה החתימה על 1111) לכן חשוב להשתמש בחתימה הזאת באופן חד-פעמי.

שיפורים:

- במקום לחתום על הודעה אפשר לחתום על הגיבוב שלה (למשל, במקרה של $SHA-256$ צריך "רק" 512 מפתחות פרטיים ו-512 מתפתחות ציבוריים.
- אפשר להכניס 2^N מפתחות בעץ גיבוב של מרקל.

17.1.1 עץ מרקל

עץ הגיבוב של מרקל (Merkle) הוא עץ בינארי (כלומר, לכל קודקוד בעץ, מלבד העלים, יש שני ילדים[3].
המידע שמוחזק בעלים אלו התוצאות של פונקציית הגיבוב וכל קודקוד מעליהן מכיל את השירשור שלהן, כלומר - חיבור של שני הקודקודים שלו.
באופן כללי:

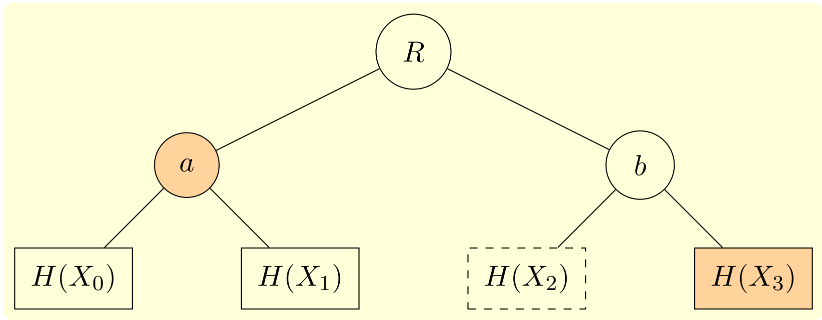


קודקוד a מכיל בתוכו את $\alpha + \beta$ או כמו שאנחנו נסמן זאת:

צורת רישום 17.3. שירשור של a ו-b מסומן: $a \| b$ ופירושו $a + b$.

בעץ מרקל בעלים ישנם את ערכי פונקציית הגיבוב וכל קודקוד מעליהם מכיל את השירשור שלהם.
למשל:

[3] זה רק במקרה שלנו. ישנים עצי מרקל יותר מורכבים.



הרעיון שאנחנו מצפינים דרך עלה אחד (במקרה שלנו - $H(X_2)$) וצריכים לספק, מלבד שורש העץ את הדרך שבה ניתן לסכום את הקודקודים ולהגיע לשורש העץ.
המידע שנשלח הוא שורש העץ, כלומר, הקודקוד הכי עליון + הקודקודים שדרכם ניתן לחשב את R.
במקרה שלנו זה את: $H(X_3)$ ואת a (את b כבר נוכל לחשב אוטומטית, ע"י כך שנוכל לחבר את $H(X_2)$ ואותו), ובהינתן לנו את R נוכל לראות האם דרך שירשורים נוכל להגיע אליו.

17.2 חתימה עיוורת

חתימה עיוורת היא חתימה שבה החותם אינו רואה את ההודעה, אבל החתימה היא לצורך אישור בלבד.
לדוגמה - עושים הצבעה אלקטרונית, אם יש לכם זכות הצבעה, מישהו יצטרך לחתום על ההצבעה שלכם (כדי לאשר שזה אכן אתם וההצבעה תקינה), אבל הוא לא יוכל לראות מה הצבעתם. זאת **חתימה עיוורת**.

17.2.1 חתימה עיוורת של שאום (מבוססת RSA)

אפרת רוצה שבנימין יחתום על ההודעה m בצורה עיוורת.
(n, e) - זה המפתח הציבורי של בנימין ו-d זה המפתח הפרטי שלו.
אליס בוחרת k אקראי $1 < k < n$ ומחשבת את:

$$t = mk^e \pmod n$$

זוהי בעצם ה"מעטפה", ככה שבנימין לא יוכל לקרוא את ההודעה.
בנימין חוצם על t (אין לו מושג מהי ההודעה m):

$$t^d = (mk^e)^d \pmod n$$

אפרת כמובן אינה יודעת מהו d, אבל היא מחשבת את החתימה באמצעות:
(תזכורת: $e \cdot d \equiv 1 \pmod n$).

$$s = \frac{t^d}{k} = \frac{(mk^e)^d}{k} = \frac{m^d \cancel{k^{ed}}}{\cancel{k}} = m^d \pmod n$$

כעת בנימין יכול לראות כי החתימה היא אכן שלו (כי הוא יודע מהו d), ומצד שני הוא <u>אינו</u> יכול לדעת מהי m.

הערה 17.4. זה נכון גם לגבי מספר הודעות. הוא יכול לחתום על כמה הודעות ואין הוא יכול לדעת על איזו הודעה הוא חתם עם איזו חתימה, היות ואין קשר בין ההודעה לחתימה.

17.3 חתימה שלא ניתן להכחישה

17.3.1 הרעיון

האלגוריתם של שאום לחתימה שאינה ניתן להכחישה.
הרעיון כאן מחלוק לשניים:

1. בדיקת החתימה נעשית בשיתוף פעולה עם החותם (אחרת לא ניתן לאמת אותה). לכן אם בחותמת רגילה היה ניתן לשכפל ולשלוח אותה לכמה מקורות וכל מקור היה יכול לבדוק את אמינותה, כאן אם זה שחתם רוצה שרק מקורות מסוימים יאשרו אותה הוא יכול (במקורות האחרים הוא לא ישתף פעולה).

2. מצד שני - החותם לא יכול להכחיש את החתימה שלו. אם החתימה תקינה - החותם אינו יכול להכחיש זאת.

17.3.2 אופן החתימה

נתונים לנו: p - מספר ראשוני ו-g יוצר של $\mathbb{Z}_p^*$.
ההודעה היא m.
המפתח הפרטי של אפרת הינו: $1 < x < p-1$.
היא חותמת על ההודעה באופן הבא: $z \equiv m^x \pmod p$.
<u>פרוטוקול אישור החתימה ע"י בנימין:</u>
בנימין בוחר שני מספרים אקראיים: $1 < a, b < p-1$ ושולח לאפרת את $c = m^a g^b \pmod p$.
מצב העניינים הוא שבנימין אינו יודע מהו x ואפרת אינה יודעת מהם a, b.
אפרת בוחרת מספר אקראי $1 < q < p-1$ ושולחת לבנימין את $s_1 = cg^q$ ואת $s_2 = s_1^x$.
נשים לב כי s_1 שאפרת שולחת לבנימין מתבסס על c ו-s_2 מתבסס על s_1 - כלומר: כל מה שאפרת שולחת לבנימין מתבסס על ה-c שהוא שלח לה.
<u>שלב הגילוי:</u>
כעת אפרת ובנימין חושפים את המשתנים הפרטיים שלהם ומאמתים את המידע שכל אחד שלח.
בנימין מגלה את a, b.
אפרת בודקת כי אכן $c = m^a g^b$ (אחרי שהיא מקבלת את a, b מבנימין היא בודקת שהוא חישב את c כמו שצריך).
אפרת מגלה את q.
בנימין בודק כי אכן $s_1 = cg^q$ וכי $s_2 = z^a y^{b+q}$.

ניתן להגיע למסקנה כי $s_2 = z^a y^{b+q}$ (אם מציבים במקום s_1^x את $(cg^q)^x$ ואז מציבים במקום c את $m^a g^b$ וכו'...), אבל מה שחשוב שאומנם $s_2 = s_1^x$ - אבל אם בנימין לא מרמה עם a, b אזי אחרי שאפרת מגלה לו את q - <u>הוא יכול לחשב את s_2 באמצעות a, b, q בלבד (ללא צורך ב-x)</u>.
אבל כל זה בתנאי שהוא לא רימה בשליחת c....

מה מיוחד בחתימה הזאת?
שבלי ההשתתפות של אפרת החתימה אינה שווה.
אם בנימין מראה את **כל** התקשורת למישהו אחר, אזי זה לא נחשב לבאמת תקין כי בנימין יכול לבחור את a, b, q ולחשב את s_1, s_2 בלי בעיות.
הוא היחיד שיודע שהוא בחר את a, b ואפרת בחרה את q (ממש כמו בהוכחה באפס ידיעה).

17.3.3 הכחשה

נניח כי אפרת רוצה לשכנע את בנימין כי החתימה אינה תקינה, כלומר: $z \not\equiv m^x \pmod p$.
מה שקורה הוא שהיא ובנימין מסכימים על איזשהו k שמגדיר את האמינות של האלגוריתם: אם החתימה תקנית, אזי הסיכוי שאפרת תצליח לשכנע את בנימין שהיא לא תקנית היא: $\frac{1}{k+1}$.
<u>הפרוטוקול:</u>

1. בנימין בוחר $0 \leq s \leq k$ ו-$1 < b < p$ באופן אקראי ושולח לאפרת את:

$$v_1 = m^s g^b$$
$$v_2 = z^s y^b$$

המספרים b, s סודיים בשלב הזה והם מוסתרים בחזקות. אם החתימה תקינית, אזי:

$$v_2 = z^s y^b = (m^x)^s (g^x)^b = \left(m^s g^b\right)^x = v_1 \pmod p$$

(התהליך מאוד דומה לבדיקה, רק ש-s (במקום a) חייב להיות בין 0 ל-k, והמספרים v_1, v_2 מקבילים ל-s_1, s_2 רק שכאן $q = 0$.

2. אפרת מחשבת את $v_1^x \pmod p$ ואת $v_1^x v_2^{-1} \pmod p$. <u>אם החתימה תקינה היא אמורה לקבל: $v_1^x v_2^{-1} \equiv 1 \pmod p$</u>. (היות ו-$m^x \equiv z \pmod p$).

3. אם החתימה אכן **<u>לא</u>** תקינה, אפרת יכולה להשוות את $v_1^x v_2^{-1}$ ל-$\left(m^x z^{-1}\right)^i$ עבור $i \in \{1, \ldots, p-1\}$ כדי למצוא את ה-i כך ש:

$$\left(m^x z^{-1}\right)^i = v_1^x v_2^{-1}$$

וזה יהיה הערך s.

3.1. מצד שני - אם החתימה אכן תקינה, היא לא תוכל למצוא את s כי לכל i: $\left(m^x z^{-1}\right)^i = v_1^x v_2^{-1} = 1 \pmod p$ ולכן היא חייבת לבחור i אקראי. (זה מצב שבו היא רוצה להכחיש את החתימה למרות שהיא חתמה, או שהיא רוצה להוכיח כי החתימה שלה אינה תקינה למרות שהיא תקינה).

4. אפרת מתחייבת ל-i: היא בוחרת r אקראי ושולחת $h(r, i)$ לבנימין.
h זאת פונקציית גיבוב כלשהי. הסיבה שהיא שולחת את i "מוסווה" בפונקציית גיבוב יחד עם r היא שככה היא לא מגלה את i שלה למקרה שבנימין מרמה (כלומר, היא תקינה למרות שבנימין טוען שלא). אם החתימה <u>אינה</u> תקינה - אזי ישנו i שמאשש זאת ואפרת לא רוצה לגלות מהו לבנימין.

5. בנימין מגלה את b.

6. אפרת בודקת כי אכן b הוא המספר הסודי של בנימין, כלומר, היא בודקת שניתן לחשב איתו את v_1, v_2 ושולחת לבנימין את r.

7. בנימין בודק כי: $h(r, i) = h(r, s)$ (אם החתימה <u>אינה</u> תקינה - אזי ישנו i כך שהוא יתן את התוצאה כמו של s ואם השוויון מתקיים סימן שאפרת עלתה עליו).

אם אכן חלק 7 מתקיים ו-$h(r, i) = h(s, i)$ אזי זה אומר כי $z \not\equiv m^x \pmod p$ וכי החתימה אינה תקינה.
אם אכן החתימה תקנית (ולמרות זאת אפרת רוצה להכחישה), אזי כל i יתאים, לכן הסיכוי שלה למצוא את ה-i הנכון (שיהיה שווה ל-s הוא: $\frac{1}{k+1}$ היות ו-$0 \leq s \leq k$.

חלק VI:
שורשים ריבועיים

18. הגדרה

הגדרה 18.1 עבור $n \in \mathbb{N}_+$, אומרים על s שהוא שורש ריבועי, אם קיים $x \in \mathbb{Z}_n$ כך ש:

$$\boxed{x^2 \equiv s \pmod{n}}$$

דוגמה 18.2 עבור $\mathbb{Z}_n$: 1 תמיד יהיה השורש הריבועי של עצמו: $1^2 \equiv 1 \pmod{n}$.

דוגמה 18.3 אם ניקח את $\mathbb{Z}_7$ לדוגמה, אזי $4^2 \equiv 2 \pmod{7}$ ולכן 4 הוא שורש ריבועי של 2 ב-$\mathbb{Z}_7$.

19. כיצד מחשבים שורש ריבועי מודלו p ראשוני

הנחה 19.1 p הוא מספר ראשוני כך ש-$p \equiv 3 \pmod{4}$ (אחרת השיטה לא תעבוד!).

אנחנו רוצים למצוא את השורש הריבועי של b, כלומר: למצוא s כך ש:

$$s^2 = b \pmod{p}$$

1. מקרה ראשון: $b \pmod{p} \equiv 0 \pmod{p}$ - במקרה זה: ישנו רק שורש אחד והוא 0.
2. מקרה שני: נקבל איזשהו $s \not\equiv 0 \pmod{p}$, ואז מה שנבדוק הוא האם $s^2 \equiv b \pmod{p}$.
   2.1. אם כן: אזי $\pm s$ הם שורשים של b.
   2.2. אחרת: ל-b אין שורשים.

הערה 19.2 אם p ראשוני אזי:

1. ל-0 ישנו רק שורש ריבועי אחד.
2. ל-$\frac{p-1}{2}$ איברים <u>יש</u> שני שורשים ריבועיים.
3. ל-$\frac{p-1}{2}$ איברים <u>אין</u> שורשים ריבועיים.

19.1 מציאת שורש ראשוני מודולו p

אם $p\equiv 3 \pmod 4$: יהי $b\in\mathbb{Z}_n$. נחשב: $x\equiv b^{\frac{p+1}{4}}$.
אם b הוא ריבוע מודולו p, אז: $b\equiv x^2 \pmod p$.
אם b <u>אינו</u> ריבוע מודולו p, אז: $-b\equiv x^2 \pmod p$.

19.2 דוגמאות

19.2.1 $\mathbb{Z}_{11}$

$\mathbb{Z}_{11}, b=5$

דוגמה 19.3. ניקח $p=11$:

ראשית כל נבדוק: $11\equiv 3 \pmod 4$ ✓.
נרצה לחשב את השורש הריבועי של 5:

$$5^{\frac{11+1}{4}}\equiv 5^3\equiv 4 \pmod{11}$$

ועכשיו נבדוק:
האם $4^2\equiv 5 \pmod{11}$? ✓. (בודקים אם 4^2 נותן 5).
ולכן: $4,7\,(=-4)$ הם שורשים ריבועיים של 5 ב-$\mathbb{Z}_{11}$

$\mathbb{Z}_{11}, b=6$

דוגמה 19.4. $p=11$.

נרצה לחשב את השורש הריבועי של 6:

$$6^{\frac{11+1}{4}}\equiv 6^3\equiv 7 \pmod{11}$$

ועכשיו נבדוק:
האם $6^2\equiv 7 \pmod{11}$? ✗.
ולכן ל-6 אין שורשים ריבועיים ב-$\mathbb{Z}_{11}$...

אם באופן כללי נסתכל על $\mathbb{Z}_{11}$:

x	0	1	2	3	4	5	6	7	8	9	10
x^2	0	1	4	9	5	3	3	5	9	4	1

וניתן לראות שבשורה התחתית (x^2) מופיעים לנו רק המספרים $\{0,1,4,5,9\}$ - אלו המספרים היחידים שנוכל למצוא להם שורשים, עבור השאר לא נוכל למצוא. (לכן לא מצאנו ל-6).

20. חישוב שורש ריבועי עבור $n=p\cdot q$

במקרה הקודם חישבנו שורש ריבועי עבור מספר ראשוני p, כעת נרצה לחשב עבור מספר שהוא מכפלה של שני ראשוניים $n=p\cdot q$.

משפט 20.1. אם $x^2 \equiv b \pmod{pq}$ אזי:

$$x^2 \equiv b \pmod{p}$$
$$x^2 \equiv b \pmod{q}$$

משפט 20.2. (כיוון שני):
נניח וקיימים x_p, x_q כך ש$x_p^2 \equiv b \pmod{p}$ ו-$x_q^2 \equiv b \pmod{q}$, אזי ע"פ משפט השאריות הסיני:
קיים <u>יחיד</u> $x \in \mathbb{Z}_n$ כך ש-$x \equiv x_p \pmod{p}$ וגם $x \equiv x_q \pmod{q}$, ואז:

$$x^2 \equiv b \pmod{p}$$
$$x^2 \equiv b \pmod{q}$$
$$\Updownarrow$$
$$x^2 \equiv b \pmod{n}$$

מסקנה 20.3. b הוא ריבוע מודולו n $\iff$ b הוא ריבוע מודולו p ומודולו q.

מסקנה 20.4. לכל זוג $(x_p, x_q) \in \mathbb{Z}_p \times \mathbb{Z}_q$ של שורשים ריבועיים של b (כלומר: $x^2 = b$) מודולו p, q מתאים שורש ריבועי $x \in \mathbb{Z}_n$ מודולו n.

מספר השורשים מודולו n שווה למספר השורשים מודולו p $\times$ מספר השורשים מודולו q.

20.1 מספר השורשים

הנחה 20.5. b הוא ריבוע מודולו n. (כלומר, קיים $x \in \mathbb{Z}_n$ כך ש-$x^2 = b$).

20.1.1 $\gcd(b,n) = 1$

אזי ישנם שני <u>ארבעה</u> שורשים ריבועיים: $\pm x_p \pmod{p}$, $\pm x_q \pmod{q}$ ולכן ישנם ארבעה שורשים מודולו $n = p \cdot q$.

20.1.2 $\gcd(b,n) = p$ (או q)

אזי ישנו שורש אחד 0 מודולו p ושני שורשים: $\pm x_q = \pmod{q}$ - ולכן ישנם שני שורשים מודולו n.
אם מדובר על q אזי צריך להחליף בין האותיות $q \iff p$.

20.1.3 $\gcd(b,n) = n$

ישנו שורש יחיד מודולו n והוא 0.

20.1.4 דוגמה $\mathbb{Z}_{15}$

לשם הדגמה ניקח את $\mathbb{Z}_{15}$:

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
x^2	0	1	4	9	1	10	6	4	4	6	10	1	9	4	1

דוגמה 20.6. ניקח לדוגמה את $x^2 = b = 4$

אזי $\gcd(15,4) = 1$ ולכן ישנם ארבעה שורשים: $2, 7, 8, 13$.[4]

דוגמה 20.7. עבור $x^2 = b = 6$ ישנם שני שורשים:
$\gcd(15,6) = 3$ ו-3 הוא אחד מהראשוניים המחלקים את 15 ($3 \cdot 5 =$).
לכן, עבור 3 השורש יהיה 0 (ואכן $6 \equiv 0 \pmod 3$) ועבור 5 ישנו לנו שני שורשים: $6, 9$.

דוגמה 20.8. עבור $x^2 = b = 10$ ישנם שני שורשים:
$\gcd(15,10) = 5$ שהוא אחד מהראשוניים המחלקים את 15.
$10 \equiv 0 \pmod 5$ ושני השורשים הם: $5, 10$.

דוגמה 20.9. דוגמה נוספת וחשובה היא דוגמה שבה **אין שורשים ריבועיים בכלל**: מספיק שלאחד מהמספרים הראשוניים שמרכיבים את n אין שורשים ריבועיים, אזי אין בכלל. למשל: $x^2 = b = 7$. $7 \equiv 2 \pmod 5$, ול-2 אין שורשים ריבועיים מודולו 5, ולכן ל-$b = 7$ אין שורשים ריבועיים מודולו 15....

20.2 חישוב שורש ריבועי מודולו $n = p \cdot q$

נתסכל על $\mathbb{Z}_{15}$ ועל $b = 6$ אזי נחפש שורשים מודולו 3 ומודולו 5.
מודולו 3:

$$6 \equiv 0 \pmod 3$$

מודולו 5:

$$6 \equiv 1 \equiv (\pm 1)^2$$

ולכן השורשים $1, 4\,(\equiv -1)$
ולכן יהיה לנו שתי משוואות שנצטרך לחשב באמצעות משפט השאריות הסיני:

$$x \equiv 0 \pmod 3 \wedge x \equiv 1 \pmod 5$$
$$x \equiv 0 \pmod 3 \wedge x \equiv 4 \pmod 5$$

וכך נקבל את שני השורשים הנדרשים.

הערה 20.10. אם מכירים את הפירוק של n יודעים כיצד למצוא את כל השורשים הריבועיים מודולו n.

הערה 20.11. אם מכירים 4 שורשים של b מסוים, שזר ל-n, אזי ניתן לפרק את n כי יש לנו:

$$x^2 \equiv y^2 \equiv b$$

כאשר $x \neq \pm y \pmod n$ ואז: $\gcd(x-y, n)$ הוא גורם לא טריוויאלי של n.

[4] לא נכנסתי כאן לאילו שורשים הם של p ואילו שורשים הם של q כדי לא לסבך.

חלק VII:
הוכחה באפס ידיעה

21. הרעיון הכללי

הרעיון בהוכחות באפס ידיעה הוא כזה:
אפרת רוצה להוכיח לבנימין שהיא יודעת סוד מסוים, בתנאים הבאים:

- אפרת (שהיא המוכיחה) אינה מגלה שום מידע על הסוד שלה (כלומר, היא רוצה שבנימין, זה שמוודא את זה שהיא יודעת את הסוד, ידע רק אם היא יודעת אותו או לא אך שום מידע על הסוד) .
- משקיף מהצד אינו מקבל אף מידע על הסוד של פגי, וגם הוא אינו יודע אם היא יודעת אותו או לא...

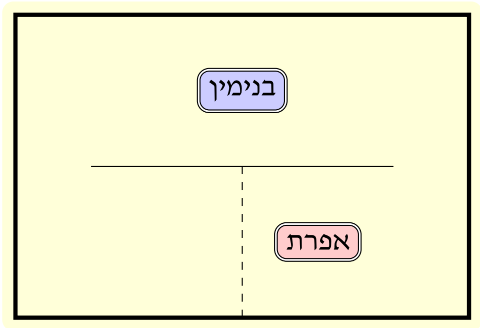
השאלה היא:

איך בנימין יכול לדעת אם אפרת יודעת את הסוד או לא?

איך הוא יוכל לדעת אם היא יודעת או לא את הסוד מבלי לגלות מהו הסוד. כלומר, הוא צריך לשאול לשאול את אפשרת שאלה כך שהתשובה של אפרת תאמר לו אם היא יודעת את הסוד או לא מבלי לגלות לו את הסוד.

21.1 דוגמה כללית

נניח את שאפרת רוצה לשכנע את בנימין שהסוד שלה הוא שהיא יכולה לעבור דרך קירות, אבל - אם בנימין יראה איך היא עוברת הוא ידע את הסוד.
לכן הם צריכים לחשוב על דרך שבה בנימין יוכל לדעת אם היא יכולה לעבור דרך קירות מבלי שהוא יראה אותה עוברת (או שכל אחד אחר יראה).
הם עושים את הדבר הבא:



בשביל להוכיח לבנימין שהיא אכן יכולה לעבור דרך קירות אפרת צריכה לעבור דרך הקיר המקווקו (שנניח שהוא אינו שונה מכל קיר אחר).
זה הולך כך:
אפרת נמצאת מאחורי הקיר הלא-מקווקו באחד הצדדים (באיור למעלה, היא נמצאת בצד שמאל של בנימין).
בנימין אומר לאפרת **"ימין"** או **"שמאל"**, ואפרת צריכה לצאת מהצד הזה (נניח כי מדובר על שמאל/ימין שלו).
אם היא יודעת את הסוד - אין שום בעיה - לא משנה איזה צד בנימין יגיד, היא תמיד תוכל לצאת מהצד הזה.
אם היא אינה יודעת הסוד - אז בהסתברות $\frac{1}{2}$ היא תצא מהצד שבנימין יגיד.

חשוב לזכור:

- בנימין יכול לדעת אם אפרת יודעת את הסוד בהסתברות $\frac{1}{2}$ מבלי לדעת כלום על הסוד ולכן זה נקרא אפס ידיעה - כי בנימין יכול לדעת אם היא יודעת את הסוד או לא עם **אפס ידיעה** על הסוד עצמו.
- כל מי שצופה מהמקום של בנימין (או שהוא אינו יכול לראות מה יש מעבר לקיר) - לא יוכל לדעת אם אפרת יודעת את הסוד או לא.
- מצד שני - אותו אחד שצופה מהצד - לא יוכל לדעת בוודאות שאפרת מכירה את הסוד היות ויכול להיות שהיא ובנימין תיאמו מההתחלה איזה צד בנימין יגיד כל פעם...

22. דוגמאות

הדבר שימושי מאוד במדעי המחשב ולהלן כמה דוגמאות:

22.1 אפס ידיעה בשורשים ריבועיים

נגדיר: $n = p \cdot q$ כאשר p, q מספרים ראשוניים.
יהי b ריבוע מודולו n שהוא זר ל-n (כמו בדוגמה 20.6).
הסוד: הסוד של אפרת הוא שורש ריבועי s של b ואפרת אינה רוצה לגלות לבנימין את s.
הפרוטוקול:

1. אפרת בוחרת מספר אקראי r_1 שזר ל-s ומחשבת $r_2 = s \cdot r_1^{-1}$ כך ש: $r_1 \cdot r_2 = s \pmod n$.
2. אפרת מחשבת $a_i \equiv r_i^2 \pmod n$ עבור $i = \{1,2\}$ ושולחת את a_1, a_2 לבנימין.
3. בנימין בודק כי אכן $a_1 \cdot a_2 \equiv b \pmod n$ ובוחר אחד מהם - a_i.

4. אפרת שולחת לו את r_i ובנימין בודק כי הוא אכן שורש ריבועי של a_i.
5. חוזרים על התהליך עד שבנימין משוכנע.

אם אפרת אינה מכירה באמת שורש ריבועי של b, היא יכולה לבחור r_1 ולחשב:

$$a_1 \equiv r_1^2 \pmod n$$
$$a_2 \equiv b \cdot a_1^{-1} \pmod n$$

כשבנימין יבדוק, אכן $a_1 \cdot a_2 \equiv b \pmod n$ אבל אם הוא יבקש את השורש הריבועי של a_2 היא לא תוכל לתת לו אתו.
אם היא כן יודעת את s אזי היא מסתירה אותו באמצעות ומסתירה אותו באמצעות a_1, a_2. בנימין יוכל לדעת מהו b אבל לא מהו s (ויש 4 כאלה).

22.2 אפס ידיעה באיזומורפיזם של גרפים

22.2.1 חזרה קצרה על מושג האיזומורפיזם

צורת רישום 22.1. יהי גרף G, $V(G)$ הינה קבוצת הקודקודים של הגרף G.

צורת רישום 22.2. יהי גרף G, עבור קודקודים $u, v \in V(G)$ אשר הם שכנים - $\{u, v\}$ הינה קשת ב-G

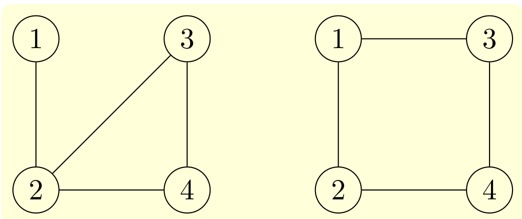
הגדרה 22.3. גרפים G_1, G_2 נקראים <u>גרפים איזומורפים</u> אם קיימת פונקציה חח"ע ועל: $f : V(G_1) \to V(G_2)$ כך שיתקיים:

$$\{u, v\} \in G_1 \iff \{f(u), f(v)\} \in G_2$$

כלומר, f "מעבירה" את כל הקודקודים של G_1 ל-G_2, לכל קודקוד ב-G_1 f מתאימה קודקוד ב-G_2, וכל קשת שהייתה ב-G_1 נשמרת גם ב-G_2.

צורת רישום 22.4. אם גרפים G_1, G_2 הינם איזומורפים, אזי מסמנים זאת ב-$G_1 \simeq G_2$.

דוגמה לגרפים שהם אינם איזומורפים:



(לא קיימת אף פונקציה f שמקיימת את הגדרה 22.3).

22.2.2 הפרוטוקול

הסוד: אפרת רוצה להוכיח לבנימין שהיא יודעת שהגרפים G_1, G_2 הם איזומורפים. היא מכירה f שעונה על ההגדרה.

1. אפרת בונה גרף חדש: H שהוא איזומורפי ל-G_1 ומחשבת את $H \simeq G_1$ וגם היא מחשבת את $G_2 \simeq H$ (אם הגרפים איזומורפים אזי היא בהכרח יכולה לחשב את שניהם). לפונקציה של איזומורפיזם $H \simeq G_1$ היא קוראת h_1 ול-$H \simeq G_2$ היא קוראת h_2.
2. היא שולחת לבנימין את G_1, G_2, H ובנימין מבקש את h_1 או h_2.
3. אם היא יודעת שהגרפים איזומורפים (ולכן היא יודעת מה האיזומורפיזם) לא תהיה לה בעיה לתת את h_i (היא גם יכולה בקלות לחשב את h_2 אם היא לא חישבה: $h_2 = h_1 \circ f^{-1}$).

22.3 הטלת מטבע בטלפון

הרעיון כאן הוא שיש הטלת מטבע באמצעות אינפורמציה, כלומר, לא ניתן לראות את ההטלה אבל ניתן להעביר אינפורמציה שהיא אכן קרתה (למשל בטלפון).
בנימין הוא זה ש"יצור" את המטבע ואילו אפרת היא זו שתטיל אותו.

1. אפרת בוחרת שני מספרים ראשוניים גדולים p,q כך ש-$p,q\equiv 3 \pmod 4$ ושולחת לבנימין את $n=p\cdot q$.
2. בנימין בוחר a אקראי ומחשב את $a^2\equiv b \pmod n$ (כעת ניתן לומר שבנימין "יצר" את המטבע, מכיוון שבד"כ יהיה יותר משורש אחד - אפרת לא תוכל לדעת מה היה ה-a שבנימין בחר).
3. אפרת מחשבת את השורשים הריבועיים של b: $\pm x, \pm y$ (ואם b אינו ריבוע היא יכולה להאשים את בנימין שהוא רימה ולא נתן לה אפשרויות להטלה...). היא בוחרת אחד מהם, את x או את y (נסמן את זה ב-α) ושולחת לבנימין (כאן בדיוק מתבצעת הטלת המטבע, היא לא יודעת מה היה השורש המקורי אבל היא צריכה לנחש כשאר יש התפלגות אחידה של $\frac{1}{2}$, כלומר, היא צריכה להטיל מטבע הוגן).
4. בנימין בודק כי מה שאפרת שלחה לו, α, מקיים: $\alpha^2\equiv \pm a \pmod n$.
   4.1. אם $\alpha^2\equiv \pm a \pmod n$ - אזי בנימין מודיע לה כי היא ניצחה. (כי היא הצליחה למצוא את השורש שלו עד כי סימן).
   4.2. אחרת: בנימין מודיע לה כי הפסידה. (היא בחרה את השורש השני).
5. אם אפרת ניצחה, בנימין מבקש ממנה את הפירוק כדי לבדוק שהיא לא רימתה.

הבעיה: בנימין יכול להפסיד בכוונה.

חלק VIII: הלוג הדיסקרטי

23. בעיית הלוג הדיסקרטי

23.1 מהו $\log_a(b)$?

לוגריתם זה ההפך מחזקה:

$$\log_a(c)=b \iff a^b=c$$

דוגמה 23.1. $2^4=16$ ולכן $\log_2(16)=4$ (כאשר 2 זה בסיס הלוג)

דוגמה 23.2. $2^3=8$ ולכן $\log_2(8)=3$.

דוגמה 23.3. $3^2=9$ ולכן $\log_3(9)=2$.

23.1.1 סימונים

צורת רישום 23.4. ניתן לסמן את הלוג כ-$\log_a(c) = b$, או: $L_a(c) = b$.

23.2 לוג דיסקרטי

ניתן לתאר את הלוג גם באופן דיסקרטי. למשל, ניקח את $\mathbb{Z}_7$:

$$3^2 \equiv 2 \pmod 7$$

ולכן: $\log_3(2) = 2 \pmod 7$.

23.3 בעיית הלוג הדיסקרטי

תהי G חבורה ציקלית ויהי a יוצר של G:

$$a^k = b$$

a, b נתונים לנו, אך איך ניתן לחשב את k?
זאת בעיית הלוג הדיסקרטי. עבור $\mathbb{Z}_p^*$ כאשר p ראשוני ממש גדול - זה מאוד קשה!!

הערה 23.5. הסיבה שבגלל בוחרים a שהוא יוצר של G היא שזה מקשה מאוד על חישוב הלוג (אחרת יותר כל לחשב אותו כי הוא לא יוצר את כל החבורה G, אבל לא ניכנס לזה כאן... זה קשור לכך).

23.3.1 איך מוצאים יוצר בחבורה ציקלית מסדר n?

משפט 23.6. a יוצר של החבורה הציקלית אסס $a^{\frac{n}{p}} \neq 1 \pmod n$ לכל $p \mid n$ ראשוני.

דוגמה 23.7. ניקח את $\mathbb{Z}_{23}^*$. $|\mathbb{Z}_{23}^*| = 23 - 1 = 22 = 2 \cdot 11$.
לכן נבדוק מה הוא ה-a הראשון שעבורו $a^{\frac{22}{11}} = a^2 \neq 1 \pmod{23}$
<u>**וגם**</u> $a^{\frac{22}{2}} = a^{11} \neq 1 \pmod{23}$.

a	$a^2 \pmod{23}$	$a^2 \pmod{23}$	יוצר?
2	1	4	✗
3	1	9	✗
4	1	16	✗
5	22	2	✓

ל-5 **בשתי** העמודות אין 1 ולכן הוא יוצר של $\mathbb{Z}_{23}^*$.

23.4 קביעת מפתח של דיפי-הלמן

יהי p ראשוני התאים ללוג דיסקרטי 1024 סיביות ויהי $1 < \alpha < p - 1$.
קיבתע המפתח בין אפרת לבנימין:

1. אפרת בוחרת $1 < a < p - 1$ ושולחת את $\alpha^a \pmod p$ לבנימין.
2. בנימין בוחר $1 < b < p - 1$ ושולח את $\alpha^b \pmod p$ לאפרת.

המפתח הסודי המשותף של אפרת ובנימין הוא: $\boldsymbol{\alpha^{ab} \pmod p}$, כלומר:
אם אפרת רוצה להגיע למפתח היא צריכה לחשב את $\left(\alpha^b\right)^a$ (ואת α^b יש לה מבנימין).
אם בנימין רוצה להגיע למפתח הוא צריך לחשב את $\left(\alpha^a\right)^b$ (ואת α^a יש לו מאפרת).

23.4.1 בעיית האיש באמצע

בעיית האיש באמצע (Man in The Middle), הית התקפה שבה יכול להיות מישהו באמצע, באמצע ערוץ התקשורת ולשלוח מספרים שונים לאפרת ובנימין, למשל:
הוא רואה שאפרת שלחה לבנימין את α^a והוא שולח לה בחזרה את α^c (ואילו אפרת חושבת כמובן שבנימין הוא זה ששלח לה את זה).
וככה אותו דבר בדיוק אותה אחת יכולה לשלוח מספר כלשהו לבנימין והוא יחשוב שאפרת שלחה לו את זה...

23.5 הצפנת אל-גמאל

קביעת המפתח של אפרת:

- p ראשוני המתאים ללוג הדיסקרטי (1024 סיביות).
- α יוצר של $\mathbb{Z}_p^*$.
- $1 < a < p-1$. $\beta = \alpha^a \pmod p$.

המפתח הציבורי של אפרת הינו (p, α, β) ואותו היא מפרסמת והמפתח הפרטי הינו a.
כעת, אם בנימין רוצה לשלוח לאפרת את ההודעה x הוא מצפין אותה באופן הבא:

- הוא בוחר k: $1 < k < p-1$.
- הוא מחשב: $(y_1, y_2) = \left(\alpha^k \pmod p, x \cdot \beta^k \pmod p\right)$ ושולח את (y_1, y_2) לאפרת.

אם אפרת רוצה לדעת מהי ההודעה שהוצפנה (x) היא מפענחת אותה באופן הבא:

$$x \equiv y_2 \left(y_1^a\right)^{-1} \pmod p$$

הערה 23.8. הקשר בין אל-גמאל לדיפי-הלמן הוא שהצפנת אל-גמאל כוללת את הפרוטוקול של דיפי הלמן (23.4), אבל באופן חד פעמי:
אפרת בוחרת את a ומפרסמת את $\beta = \alpha^a \pmod p$ ובנימין עושה דבר דומה עם k.

23.6 חתימת אל-גמאל

נתונים:

- p ראשוני גדול.
- α יוצר של $\mathbb{Z}_p^*$.
- a: $1 < a < p-1$, $\beta = \alpha^a \pmod p$.
- מפתח ציבורי (p, α, β) ומפתח פרטי: a.

חתימה על ההודעה x:

1. אפרת בוחרת k זר ל-$p-1$ ($\gcd(k,p-1)=1$).
2. אפרת מחשבת את $\gamma=\alpha^k \pmod p$, ואת $\delta=(x-a\gamma)\cdot k^{-1} \pmod{p-1}$.
3. החתימה היא: (γ,δ).

חשוב לזכור:

γ - הוא מודולו p.
δ - הוא מודולו $p-1$.

בדיקת החתימה (כלומר, כך נוודא שהחתימה אינה מזויפת):
אם:

$$\boxed{\beta^\gamma\cdot\gamma^\delta\equiv\alpha^x \pmod p}$$

אזי החתימה תקינה.

23.6.1 נכונות הבדיקה

היות ו: $\delta=(x-a\gamma)\cdot k^{-1} \pmod{p-1}$, אזי:

$$\delta=(x-a\gamma)\cdot k^{-1} \pmod{p-1}$$
$$\Downarrow$$
$$k\delta=x-a\gamma \pmod{p-1}$$
$$\Downarrow$$
$$x=k\delta+a\gamma \pmod{p-1}$$

כמו-כן: $\gamma=\alpha^k \pmod p$, ולכן:

$$\gamma^\delta\cdot\beta^\gamma=\left(\alpha^k\right)^\delta\cdot(\alpha^a)^\gamma=\alpha^{\overbrace{k\delta+a\gamma}^{x}}$$
$$\Downarrow$$
$$\gamma^\delta\cdot\beta^\gamma=\alpha^x$$

ולכן אם קיבלנו את השוויון הנ"ל סימן שהחתימה לא זויפה.

24. התקפות על הלוג הדיסקרטי

24.1 התקפת "Baby Steps - Giant Steps"

התקפה מסוג "איזון זמן/זיכרון".
<u>נתון:</u>
G - חבורה ציקלית מסדר n.
α - יוצר של G.
β: $\beta=\alpha^x$.
המטרה:

למצוא מהו x...

הרעיון:
לכתוב את x באופן הבא:

$$\boldsymbol{x = jm + i}$$
$$m = \lceil \sqrt{n} \rceil$$
$$0 \le i, j < m$$

ואז: $\beta\left(\alpha^{-m}\right) = \alpha^i$.
מה שעושים הוא שמחשבים את כל האפשרויות עבור α^i ומחפשים $\beta\left(\alpha^{-m}\right)^j$ שנותן את אותה תוצאה.
כזכור: $i < \sqrt{n}$ ולכן אנחנו בעצם לא עוברים על כל האפשרויות.

אלגוריתם 8 אלגוריתם Baby Steps - Giant Steps

1. לכל $0 \le i < m$ מחשבים α^i ומאחסנים את הזוג $\left(i, \alpha^i\right)$ בטבלה.
2. מחשבים את α^{-m}.
3. $\beta \to y$. (תזכורת: $\beta = \alpha^x$).
4. לכל $0 \le j < m$:
   4.1. בודקים אם y מופיע באחד המקומות בחלק השני (הימני) של הטבלה.
   4.2. אם כן: מחזירים את $mj + i$.
   4.3. אחרת: $y \cdot \alpha^{-m} \to y$

הערה 24.1. האלגוריתם מתאים לכל חבורה ציקלית.

הערה 24.2. אין צורך לדעת בדיוק את סדר החבורה, אפשרת לעבור עם חסם מליעל (בחלק של עקומות אליפטיות).

הערה 24.3. רצוי להשתמש בחבורות שסדרן ראשוני (אחרת יש את אלגוריתם פוליג הלמן, אשר יעיל יותר).

הערה 24.4. זמן ריצה/זיכרון: $O\left(\sqrt{n}\right)$.

24.2 התקפת אינדקס קלקולוס

24.2.1 שלב ההכנה

קובעים חסם מסוים B.
עבור ערכים שונים של $1 \le k < p - 2$ מפרקים לגורמים את: $\alpha^k \pmod p$ ושומרים על הפירוקים שבהם מופיעים **רק** הראשוניים שהם קטנים מהחסם הנבחר B.
אם לוקחים את הלוג של כל הפירוקים הללו, ניתן לקבל מערכת משוואות מודלו $p-1$ שבהם מופיעים $L_\alpha(q)$ עבור המספרים הראשוניים הקטנים מ-B.

24.2.2 חישוב הלוג הדיסקרטי

מחפשים r כך ש-$\beta\alpha^r$ מתפרק בראשוניים קטנים מודולו n ומשתמים בשלב המקדים (מערכת המשוואות) כדי לחשב את $L_\alpha(\beta)$.

24.2.3 דוגמה

ניקח $p = 17$ ו-$\alpha = 3$. מה שאנחנו רוצים לחשב הוא את:

$$3^x \equiv 8 \pmod{17}$$

כלומר, את $L_3(8)$.
המטרה היא למצוא את x:

$$3^1 \equiv 3 \pmod{17} \Rightarrow \boldsymbol{1 = L_3(3) \pmod{16}}$$

הסבר:
מצד שמאל - אנחנו יודעים כי $3^1 \equiv 3 \pmod{17}$.
מצד ימין - אנחנו מתסכלים על החזקות, ולכן זה קודם כל $\ldots = 1$ ואז בשפה של $L_3(\square)$, אנחנו צריכים לקבל 1 ו-$L_3(3) = 1$ ולכן $\square = 1$.

$$3^6 \equiv 15 = 3 \cdot 5 \pmod{17}$$

ואם שוב נסתכל על החזקות נקבל: $\boldsymbol{6 = L_3(3) + L_3(5) \pmod{16}}$.
כעת אם יהיה לנו מצב כמו:

$$3^2 \equiv 9 \pmod{17}$$

אזי נקבל: $2 = 2 \cdot L_3(3) \pmod{16}$ וזה בגלל ש-$3^2 = 9$ ולכן זה 2 כפול החזקה של 3^1 (תזכורת: אנחנו מדברים על החלק של החזקות).
אם ניקח את שתי המשוואות המודגשות נקבל:

$$\boxed{1 = L_3(3)}$$
$$6 = \underbrace{L_3(3)}_{=1} + L_3(5) \Rightarrow \boxed{5 = L_3(5)}$$

כעת נעבור לשלב השני חישוב הלוג הדיסקרטי:
אם ניקח $r = 12$ נקבל ש:

$$8 \cdot 3^{12} \equiv 15 = 3 \cdot 5 \pmod{17}$$

ולכן: אם נסתכל על החזקות נקבל:

$$L_3(8) + 12 \cdot L_3(3) = L_3(3) + L_3(5)$$

נסתכל על מה שנמצא בתוך המסגרות ונציב:

$$L_3\left(8\right)+12\cdot1=1+5$$
$$\Downarrow$$
$$L_3\left(8\right)=-6\equiv10\pmod{16}$$

ואכן: $3^{10}\equiv8\pmod{17}$ ☺.

24.3 אלגוריתם פוליג-הלמן

יהי n סדר החבורה, ויהי:

$$n=\prod_i P_i^{a_i}$$

הפירוק לראשוניים של n.

1. מחשבים את הלוג הדיסקרטי מודולו $p_i^{a_i}$ לכל i.
2. מחשבים את הלוג הדיסקרטי מודולו n בעזרת משפט השאריות הסיני.

מסקנה 24.5. חשוב ש-n לא יתפרק לראשוניים קטנים.

24.4 חתימת DSA

דומה מאוד לחתימת אל-גמאל, רק שבוחרים p מהצורה $p=2q+1$ כש-q ראשוני.
עובדים מודולו p אבל עם α מסדר q (במקום ש-α יהיה יוצר של החבורה). לכן החזקות הן מודולו q.
היתרון: הלוג הדיסקרטי חזק יותר.

חלק IX:
חלוקת סוד

25. הרעיון הכללי

הרעיון הכללי בחלוקת סוד הוא כזה:
יש לנו קבוצה בת n אנשים ואנחנו רוצים לחלוק ביניהם סוד באופן הבא:

- אף אחד אינו יודע את הסוד (לבד).

- רק תת-קבוצה בגודל k אנשים $(1 < k < n)$ תוכל לדעת את הסוד. כל תת-קבוצה בגודל שהוא קטן מ-k לא תוכל להסיק שום אינפורמציה עליו.
- אלו יכולות להיות תת-קבוצות בגודל שונה אם מגדירים זאת מראש.

למשל: אנחנו לא רוצים להרשות מורשה חתימה יחיד כדי שלא יהיה שימוש לא הולם.

26. סכמת סף

הגדרה 26.1. נניח ויש לנו קבוצה בת n איברים ואנחנו רוצים לדעת כמה תת-קבוצות שונות יש לה מגודל k (כאשר $k < n$), אזי התשובה היא:

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$$

הגדרה 26.2. יהיו $k, n \in \mathbb{N}_+$ כך ש-$k \leq n$. **סכמת סף** (k, n) היא שיטה לחלוקה של סוד M ב-n חלקים כך שניתן עם כל k חלקים (תת-קבוצה של n) לשחזר את הסוד M, אבל עם $k-1$ לא ניתן לקבל שום מידע על הסוד (כלומר, כל ערך אפשרי של M אפשרי באותה מידה).

26.1 דוגמת המדענים

נניח כי 10 מדענים עובדים ביחד. שומרים את החומר של הצוות בכספת שניתן לפתוח רק בנוכחות של 4 מדענים (או יותר). זוהי סכמת סף של $(4, 10)$.

1. כמה מנעולים צריך? (ככה שפחות מ-4 מדענים לא יוכלו לפתוח את הכספת - ברגע שארבעה).
2. כמה מפתחות נותנים לכל מדען?

התשובה (לשאלה 1) : אנחנו רוצים כי עבור כל 3 מדענים יהיו להם מפתחות ל-3 מנעולים שונים (כך שזה לא מספיק כדי לפתוח את הכספת), לכן אנחנו צריכים את כמות האפשרויות ל-3 מנעולים שונים מתוך 10, או במילים אחרות: $\binom{10}{3}$.
$120 = \frac{10!}{3!7!} = \binom{10}{3}$, לכן, מה שנעשה הוא שנשים 120 מנעולים ונמספר אותם מ-1 עד 120.
עכשיו נשאלה השאלה כמה מפתחות לכל מדען (שאלה 2):
נסתכל על המדען נועם. נועם יודע שהוא צריך עוד שלושה מדענים כדי לפתוח את הכספת, כלומר, הוא צריך לקבל את המפתח למנעול שיהיה חסר ל-3 מדענים כלשהם (וע"פ הכללים - תמיד יהיה חסר להם מנעול, ולא משנה אילו שלושה מדענים אלו, ברגע שנועם יצטרף אליהם - הם יוכלו לפתוח את הכספת).
לכן, עבור כל קבוצה בת 3 מדענים שהיא לא כוללת את נועם (סה"כ ישנם 9 מדענים בלי נועם) צריך שיהיה לכל אחד מהם מספר מנעולים שלא יגיע לכל ב-120.כלומר:

$$\binom{9}{3} = \frac{9!}{3!6!} = 84$$

כלומר, לכל מדען יהיו 84 מפתחות שונים!
המשמעות היא שנוכל לסדר זאת כך שלכל מדען נוכל לתת 84 מפתחות שונים כך שלכל שלושה לא יהיו אף פעם את כל 120 המפתחות, אבל כל מדען רביעי שיצטרף - ישלים להם את החסר ל-120מפתחות.

דוגמה 26.3. דוגמה מאוד פשוטה עם מספרים קטנים:
נניח כי יש לנו 4 מדענים ואנחנו רוצים שכל שניים יוכלו לפתוח את הכספת, אזי אנחנו צריכים: $4 = \binom{4}{1}$ מנעולים.
כמה מפתחות ניתן לכל מדען? $3 = \binom{3}{1}$.
מדען א' - $\{1,2,3\}$, מדען ב' - $\{1,2,4\}$, מדען ג' - $\{2,3,4\}$, מדען ד' - $\{1,4,3\}$.

26.2 סכמת סף (n,n)

יהי $N\in\mathbb{N}_+$ כך ש-$M<N$ (M זאת ההודעה).
בוחרים $a_1,a_2,\ldots,a_{n-1}\in\mathbb{Z}_N$ אקראיים ויהי:

$$a_n=M-\left(\sum_{i=1}^{n-1}a_i\right)\pmod N=M-a_1-a_2-\cdots-a_{n-1}\pmod N$$

עובדה 26.4. כדי לשחזר את M צריך את כל המספרים. אם מכירים רק חלק מהם לא מקבלים שום מידע מכיוון שכל ערך של M אפשרי באותה מידה. (גם אם יודעים את כולם חוץ מאחד אותו אחד יכול להיות כל איבר ב-$\mathbb{Z}_N$ ולכן גם M יכול להיות כל איבר ב-$\mathbb{Z}_N$).

הערה 26.5. חייבים לעבוד מודולו N כדי שתהיה הסתברות אחידה על המספרים. בנוסף, שעובדים מודולו N אי אפשר לקבל אף מידע על הגודל של M.

דוגמה 26.6. ניקח $M=12$, $n=4$ ו-$N=22$.
אזי נוכל לבחור: $a_1=8,a_2=17,a_3=11$.

$$a_4=12-8-17-11\pmod{22}=20$$

אזי גם אם שלושה משתתפים כלשהם ישתפו פעולה - למשל: a_1,a_2,a_4 - הם ידעו שבשביל לגלות את הסוד הם צריכים גם את a_3 והסיכוי לגלות אותו הוא בדיוק כמו הסיכוי שלהם לגלות את M (במילים אחרות, קיימת התאמה חח"ע ועל בין הערכים האפשריים של a_3 לערכים האפשריים של M). לכן זה כאילו כל אחד מהם מנסה לגלות את M לבד...

26.3 סכמת סף (k,n) של שמיר

26.3.1 פולינום האינטרפולציה של לגראנז'

בשביל להבין את סכמת הסף של שמיר, צריך להבין קודם מהו פולינום האינטרפולציה של לגראנג'.

משפט 26.7. דרך k נקודות: $(x_1,y_1),(x_2,y_2),\ldots,(x_k,y_k)$ עם x-ים שונים עובר פולינום יחיד ממעלה $k-1$, כלומר, ישנו פולינום יחיד:

$$P(x)=a_0+a_1x+a_2x^2+\cdots+a_{k-1}x^{k-1}$$

כך ש:
$a_{k-1}\neq 0$ וכך ש-$P(x_i)=y_i$ לכל i.

ניתן לחשב את הפולינום הזה באמצעות נוסחת האינטרפולציה של לגראנז':
יהיו k נקודות: $(x_1,y_1),(x_2,y_2),\ldots,(x_k,y_k)$ כך ש-$x_i\neq x_j$ לכל $i<j$ אזי הפולינום:

$$P(x)=\sum_{i=1}^{k}y_i\left(\prod_{\substack{i\neq j\\1\leq j\leq k}}\frac{x-x_j}{x_i-x_j}\right)$$

מקיים $P(x_i)=y_i$ לכל $1\leq i\leq k$.

26.3.2 סכמת הסף

יהי M סוד.
יהי p ראשוני כך ש-$n, m < P$.
לכל $1 \leq i \leq k-1$ בוחרים a_i כך ש: $0 \leq a_i < p$ באופן אקראי. $a_{k-1} \neq 0$.
יהי:

$$P\left(x\right) = M + a_1 x + a_2 x^2 + \cdots a_{k-1} x^{k-1}$$

הנקודות $\left(i, P\left(i\right)\right)$ עבור $1 \leq i \leq n$ הן החלקים של הסוד **ואת הנקודות הללו אנחנו מחלקים למשתתפים**.

הערה 26.8. $M = P\left(0\right)$ - כלומר, הנקודה $\left(0, M\right)$ נמצאת על הפולינום.

כדי לחשב את הסוד עם הנקודות $\left(x_1, y_1\right), \left(x_2, y_2\right), \ldots, \left(x_k, y_k\right)$ מחשבים:

$$M = \sum_{i=1}^{k} y_i \left(\prod_{\substack{i \neq j \\ 1 \leq j \leq k}} \frac{-x_j}{x_i - x_j} \right) \bmod p \qquad (3)$$

הערה 26.9. אם מכירים רק $k-1$ נקודות אי אפשר לדעת שום דבר על הסוד, כי כל נקודה מהצורה $\left(0, y_0\right)$ מגדירה ביחד עם הנקודות האלה פולינום יחיד שונה ולכן כל ערך של M סביר באותה מידה.

הערה 26.10. חייבים לעבוד מודולו מספר סופי כדי שתהיה התפלגות אחידה על הערכים האפשריים.

הערה 26.11. חייבים לעבוד מודולו מספר ראשוני כי בנוסחת האינטרפולציה של לגראנז' צריך לחלק ולכן צריך לעבוד בשדה (תזכורת: אם p ראשוני, אזי $\mathbb{Z}_p$ הוא שדה).

26.4 סכמת סף מפוצלת

נניח כי גם הפעם אנחנו רוצים לחלק את הסוד בים מספר אנשים, אך לא עם אותו משקל. למשל:

<u>שאלה 1</u>

חלקו את הסוד $M = 10$ בין שלושה מרצים וחמישה סטודנטים כך שרק שיתוף פעולה של שני מרצים ושלושה סטודנטים יאפשר לשחזר את הסוד. הגדירו את כל הנתונים עם מספרים מפורשים והסבירו איך ניתן לשחזר את הסוד.

תשובה

את הפתרון נצטרך לחלק לשני שלבים: <u>פיצול הסוד</u> ו<u>שחזור הסוד</u>.

פתרון. <u>פיצול הסוד:</u>
<u>שלב ראשון - פיצול הסוד באופן כללי:</u>
בוחרים p ראשוני מספיק גדול.
מפצלים את M ל-2 בסכמה פשוטה $\left(2, 2\right)$ (מכיוון שיש לנו שני סוגי חלוקות שונות):

$$M = M_1 + M_2 \pmod{p}$$

(M_1 יבחר באופן אקראי, ו-$M_2 = M - M_1 \pmod{p}$).

M_1: סוד של מרצים.
M_2: סוד של סטודנטים.
שלב שני - פיצול הסוד באופן שווה לכל קבוצה:
כעת נחלק את M_1 לפי סכמת $(2,3)$ ונקבל:

$$P_1(x) = M_1 + a_1 x$$

הערה 26.12. שתי נקודות זה ישר, ולכן קיבלנו משהו ממעלה 1.

נותנים למרצה i את הנקודה $(i, P(i))$ עבור $1 \le i \le 3$. ככה שאם יש לו רק נקודה, אין לו מושג מה הישר. בשביל לדעת מה הישר הוא צריך נקודה אחת לפחות...
כעת נעבור לסטודנטים:
מחלקים את M_2 לפי סכמת $(3,5)$, מה שנקבל הוא:

$$P_2(x) = M_2 + a_1 x + a_2 x^2$$

רק שיתוף פעולה של שני מרצים יכול לגלות את M_1,
ושיתוף פעולה של שלושה סטודנטים יכול לגלות את M_2

שחזור הסוד:

1. שתי נקודות של המרצים $\leftarrow M_1$ (שני המרצים שמשתפים פעולה מוצאים את M_1 באמצעות לגראנז' (נוסחה 3).
2. שלוש הנקודות של הסטודנטים $\leftarrow M_2$ (כנ"ל: באמצעות לגראנז', נוסחה 3).
3. לבסוף: $M = M_1 + M_2 \pmod p$ ☺.

27. מבנה גישה לחלוקת סוד

תהי Ω אוסף המשתתפים בחלוקת סוד. תהי $\Gamma \subseteq P(\Omega)$ (כלומר, Γ היא קבוצה של תת-קבוצות של Ω, $P(\Omega)$ זוהי קבוצת החזקה של Ω).
תהי Γ אוסף תתי הקבוצות שמותר להן לשחזר את הסוד.

צורת רישום 27.1. Γ נקראת - מבנה גישה לחלוקת סוד (Secret Sharing Access Structure).

הערה 27.2. מבנה הגישה לסכמת-סף (k,n) הוא:

$$\Gamma = \left\{ A \subseteq \{1, \ldots, n\} \middle| |A| \ge k \right\}$$

הגדרה 27.3. נסמן ב-Γ_0 את אוסף האיברים המינימליים של Γ - וזה יקרא - הבסיס של Γ.

דוגמה 27.4. נניח כי $\Omega = \{a,b,c,d\}$, ו-$\Gamma_0 = \{\{a,b\}, \{a,c,d\}, \{c,d\}\}$.

כעת $\Gamma = \Gamma_0$ איחוד כל האיחודים של Γ_0 (של קבוצות ב־Γ_0):

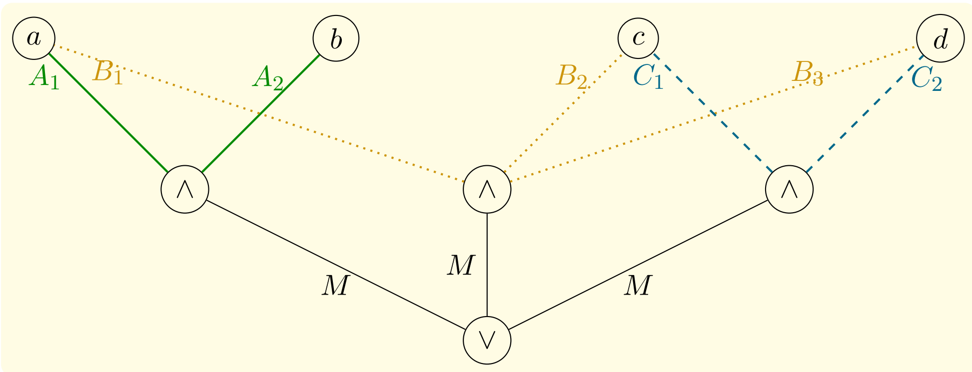
$$\Gamma = \Gamma_0 \cup \{\{a,b,c,d\}, \{a,c,d\}\}$$

27.1 צורת כתיבה של Γ_0 כפסוקית DNF

בין כל איבר בתת-קבוצה של Γ_0 נשים $\wedge$ ובין כל תת-קבוצה $\vee$:

$$(a \wedge b) \vee (a \wedge c \wedge d) \vee (c \wedge d)$$

וניתן גם לשרטט את זה כגרף:
בכל צומת $\vee$ נעביר את הסוד כפי שהוא, ובצומת $\wedge$ עם k משתתפים נחלק את הסוד לפי סכמה פשוטה (k,k):



נשים לב כי:

$$M \equiv A_1 + A_2 \pmod N$$
$$M \equiv B_1 + B_2 + B_3 \pmod N$$
$$M \equiv C_1 + C_2 \pmod N$$

וכמו-כן:
a מקבל את A_1, B_1,
b מקבל את A_2,
c מקבל את B_2, C_1,
d מקבל את B_3, C_2.
לכן למשל, b יכול לגלות את הסוד רק עם a,
ו-c יכול לגלות את הסוד רק עם a ו-b או רק עם d וכו'...

חלק X: הצפנה קוונטית

28. רקע ומושגים בסיסיים

הערה 28.1. המושגים שיוגדרו כאם הם נכונים באופן כללי, אבל לא הכי מדויקים.

28.1 רקע

במאה ה-20 החלו להופיע תופעות מעניינות שלפיהן באור הוא גם גל וגם חלקיק, כלומר, היו ניסויים שהראו כי האור הוא גל והיו ניסויים שהראו שהוא חלקיק.
אחד מהניסויים הללו היה ניסוי שבו מעבירים קרני אור דרך מסנן ובניסויי הזה אנחנו נדון.

28.2 מושגים בסיסיים

הגדרה 28.2. פוטון זוהי קרן אור שעוברת בזווית מסוימת (או שיכול להיות שאלו מספר קרניים שוברות בכמה זויות).

הגדרה 28.3. מקטב (פולורויד) זהו מסנן שדרכו האור יכול לעבור בכיוון של המקטב בלבד.

צורת רישום 28.4. כל החצים מהסוג הזה $\uparrow$ יסמלו וקטורי יחידה אלא אם צוין אחרת.

28.3 שינוי הזווית האור באמצעות המקטב

נניח כי $\rightarrow a$ הוא מקטב אופקי, ואילו $\uparrow b$ הוא מקטב אנכי, אזי מה ההסתברות לכך שהאור יעבור מקטב אנכי (b)? התשובה לכך היא b^2.
ההסבר לכך הוא שצריך לזכור ש:

$$a^2+b^2=1$$

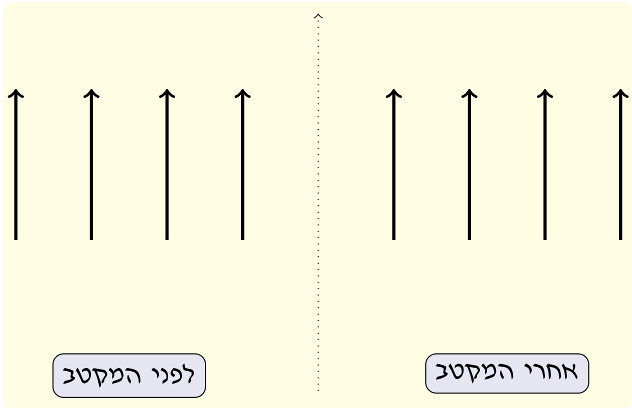
לכן, אם הפוטון הוא אנכי אזי $a=0$, $b=1$ ולכן ההסתברות שהוא יעבור את המקטב האנכי היא $b^2=1$.
אם לעומת זאת הפוטון הוא אופקי, אזי $a=1$, $b=0$ ולכן $b^2=0$ (כלומר, האור לא יעבור ויוחזר).
כעת, אם נניח הפוטון הוא בזווית של 45° (או 135°) אזי רק חצי יעבור היות ו-$b^2=\frac{1}{2} \Rightarrow b=\frac{1}{\sqrt{2}}$.
חשוב לזכור:

ברגע שאנחנו מודדים את כיוון הפוטון - אנחנו גם משפיעים עליו!

כי יכול להיות שהעברנו רק חלק ממנו, ואת החלק שעבר דרך המקטב אנחנו שינינו בהתאם לכיוון המקטב.

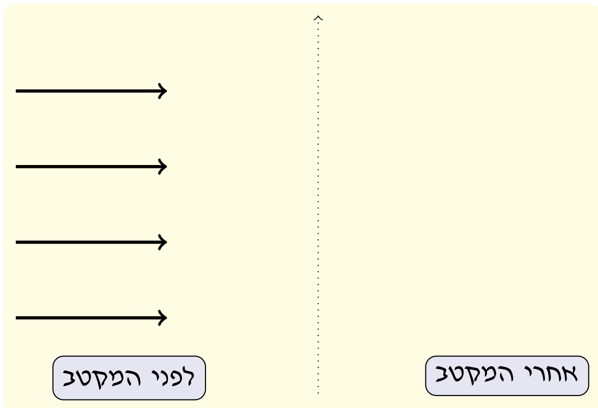
28.3.1 המקטב והפוטון באותו הכיוון

במקרה כזה - כל האור יעבור דרך המקטב:



28.3.2 המקטב והפוטון בכיוונים מנוגדים

במקרה כזה אף פוטון לא יעבור, כלומר, שום חלק מהאור לא יעבור:



28.3.3 כאשר המקטב לא אנכי או אופקי

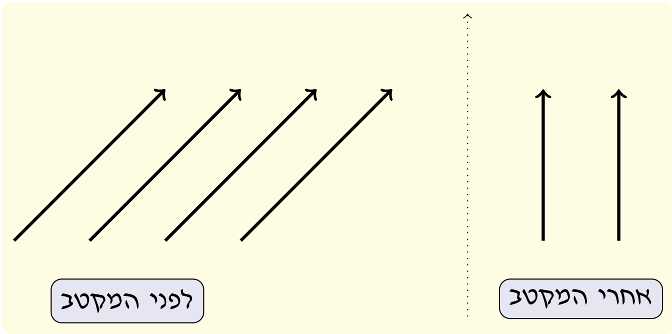
יכול להיות גם שהמקטב יהיה בזווית אחרת שהיא לא אופקית או אנכית לאור (יכול להיות שגם האור, הפוטונים, יהיו בזוויות שהן לא אנכיות או אופקיות).
נניח לשם הפשטות כי הפוטונים (כולם) הם בכיוון אופקי, והמקטב הוא בזווית של $45°$:

נשים לב לשני דברים מעניינים בחלק הזה:

1. רק חלק מהאור עבר (במקרה שלנו זה $\frac{1}{2}$ מכמות האור בגלל זווית המקטב).
2. הפוטונים שעברו **השתנו** (מבחינת הכיוון) ע"פ המקטב! כלומר, המקטב שינה את כיוון האור.

28.3.4 כאשר המקטב אופקי/אנכי אך הפוטונים לא

זה מאוד דומה למקרה הקודם אבל הפוך:
נניח כי הפוטונים הם בזווית של $45°$ ואילו המקטב הוא אנכי.



רק חצי מהאור עבר ושונה בהתאם למקטב.

29. ייצוג סיביות על ידי מקטב או קיטוב של פוטונים

29.1 התאמת מקטב לסיבית

צורת רישום 29.1. נתייחס כאן לשתי מקטבים:
$\oplus$ - זה מקטב המכיל שני מקטבים - אחד אופקי ואחד אנכי ונסמנו ב-0.
$\otimes$ - זה מקטב המכיל שני מקטבים אלכסוניים ונסמנו ב-1.

כעת, נשים לב להסתברויות שפוטונים יעברו דרך מקטבים אלה:

טבלה 1: ההסתברות למעבר של פוטונים דרך מקטבים

כיוון הפוטון הנכנס	המקטב	כיוון הפוטון שיצא
$\uparrow, \rightarrow$	$\oplus$	בדיוק כמו זה שנכנס
$\uparrow, \rightarrow$	$\otimes$	$\nwarrow$ בהסתברות $\frac{1}{2}$, $\nearrow$ בהסתברות $\frac{1}{2}$
$\nearrow, \nwarrow$	$\oplus$	$\rightarrow$ בהסתברות $\frac{1}{2}$, $\uparrow$ בהסתברות $\frac{1}{2}$
$\nearrow, \nwarrow$	$\otimes$	בדיוק כמו זה שנכנס

הערה 29.2. כל זוג חצים, למשל "$\uparrow, \rightarrow$" מסמל שזה אחד מהשניים שנכנס למקטב.

הערה 29.3. ניתן להסתכל על החצים כמו כדו כיוונים ולא רק בכיוון של ראש החץ.

הערה 29.4. היכן שכתוב שההסתברות היא $\frac{1}{2}$ אזי בטוח יצא אחד מהשניים, אבל כל אחד בהסתברות של $\frac{1}{2}$, היכן שכתוב שההסתברות היא 1 - הפוטון שנכנס הוא גם הפוטון שיצא.

29.2 התאמת מקטב לסיבית קיטוב

ניתן להתאים כל אחד מהמקטבים $\oplus, \otimes$ לשתי סיביות באופן הבא:

טבלה 2: התאמה בין מקטב לסיבית קיטוב

המקטב	כיוון הפוטון	הסיבית
$\oplus$	$\uparrow$	1
$\oplus$	$\rightarrow$	0
$\otimes$	$\nwarrow$	1
$\otimes$	$\nearrow$	0

30. הצפנה באמצעות פוטונים ומקטבים

30.1 התחייבות לסיבית

אפרת רוצה להתחייב לבנימין על סיבית (מבלי לגלות לו אותה כמובן), מה שהיא עושה זה שהיא בוחרת סיבית לפי צורת רישום 29.1:

$$\boxed{*} = \begin{cases} \oplus & 0 \\ \otimes & 1 \end{cases} \tag{4}$$

ואת הסיבית הזאת נסמן ב-B, כעת, היא מגרילה k סיביות $b_1, \ldots, b_k$ ושולחת לבנימין בהתאם לקטב שהיא בחרה (בעזרת טבלה 2):

דוגמה 30.1. אם הסיבית שהיא בחרה היא 0 ($\oplus$ זה המקטב) והסיבית שהיא הגרילה היא 0, אזי היא תשלח את $\rightarrow$, ואם הסיבית הייתה 1 אזי היא הייתה שולחת $\uparrow$.

בנימין מגריל גם הוא סדרה של k סיביות $c_1, \ldots, c_k$ ובודק את הפוטון ה-i עם המקטב המתאים לסיבית ה-c_i (לפי 4 - $\boxed{*}$).
כמה דוגמאות:

דוגמה 30.2. נניח שהסיבית שאפרת בחרה היא 0 ולכן המקטב הוא $\oplus$. היא הגרילה את הסיבית 1 ולכן היא תשלח את הפוטון $\uparrow$. בנימין לעומת זאת הגריל את הסיבית 0 ולכן הוא יעביר את הפוטון שאפרת שלחה לו דרך המקטב $\oplus$, ולכן מה שהוא יקבל את זה הפוטון $\uparrow$ שזה 1 (זהה למה שאפרת הגרילה).

דוגמה 30.3. אם לעומת זאת הוא היה מגריל את הסיבית 1 הוא היה מקבל את הפוטון $\uparrow$ בהסתברות של $\frac{1}{2}$ (בהתאם לטבלה 1).

מסקנה 30.4. אם $B = c_i$ (אם הסיבית שבנימין הגריל זהה לסיבית שאפרת בחרה) הוא יקבל סיבית זהה לסיבית לזאת שאפרת <u>הגרילה</u> (b_i).
אם $B \neq c_i$ אזי הסיכוי שבנימין יקבל סיבית שונה ממנה שאפרת הרגילה היא $\frac{1}{2}$.

דוגמה 30.5. כעת נניח כי אפרת בחרה את הסיבית 0 ($\oplus$) והגרילה את סדרת הסיביות 10011, אז מה שאפרת תשלח לבנימין הוא:

הסיבית שאפרת הגרילה	1	1	0	0	1
הפוטון שהיא תשלח לבנימין	$\uparrow$	$\uparrow$	$\rightarrow$	$\rightarrow$	$\uparrow$

בנימין הגריל את סדרת הביטים: 11001.
כעת הוא מתאים לכל סיבית מקטב לפי $\boxtimes$:

הסיבית שבנימין הגריל	1	0	0	1	1
המקטב שדרכו הוא יעביר את הפוטון שקיבל מאפרת	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$
הפוטון שבנימין קיבל מאפרת	$\uparrow$	$\uparrow$	$\rightarrow$	$\rightarrow$	$\uparrow$
התוצאה	$\nearrow$	$\uparrow$	$\rightarrow$	$\nearrow$	$\nwarrow$
הסיבית לפי טבלה 2	0	1	0	0	1
הסיבית שאפרת הגרילה	1	1	0	0	1

שלב הבדיקה:

כעת אפרת שולחת לבנימין את B ואת סדרת הסיביות שהיא הגרילה.
בנימין בודק בהתאם ל-B: **עבור $\oplus$ הוא בודק את העמודות האדומות, ועבור $\otimes$ את העמודות הירוקות.**
היות ואפרת בחרה ב-0 ($\oplus$) - הוא בודק שבעמודות האדומות כל הביטים שהוא קיבל אחרי הקיטוב שהוא עשה זהות לסיביות שאפרת הגרילה, וככה הוא יודע שהיא לא רימתה ואכן בחרה בסיבית B.
<u>הסבר:</u>
לפי מסקנה 30.4 אם הסיבית שבנימין הגריל זהה ל-B (כלומר, כל הסיביות שהוא הגריל שהן 0), אזי הוא אמור לקבל בדיוק את מה שאפרת הגרילה אחרי הקיטוב. (כל הסיביות שהוא הגריל שהן 0 הן בעמודות האדומות).
אם הוא היה בודק את העמודות הירוקות, אזי בהסתברות $\frac{1}{2}$ הוא היה מקבל את מה שיש לאפרת, ולכן הוא צריך לבדוק את העמודות האדומות.

30.1.1 האם ניתן לרמות בהתחייבות לסיבית?

נניח כי אפרת לא רוצה להתחייב על סיבית ורק בסוף להחליט עליה או שהיא משנה את דעתה בסוף התהליך. האם היא תוכל לרמות?
אזי היא הסיכוי שבנימין יעלה על זה שהיא רימתה אותו הוא: $75\% = 0.75 = \frac{3}{4}$, כי היא תצליח לשכנע אותו שהיא לא רימתה רק עם המקטב הוא אותו מקטב (סיכוי של $\frac{1}{2}$) וגם הפוטון שיעבור דרך אותו מקטב יהיה באותו כיוון (ולזה גם יש סיכוי של $\frac{1}{2}$) . .
והיות וזה גם וגם, אזי הסיכוי ששניהם יענו על התנאים הוא: $25\% = \frac{1}{4} = \frac{1}{2} \cdot \frac{1}{2}$, ולכן הסיכוי שהוא יעלה על הרמאות היא: $1 - \frac{1}{4} = \frac{3}{4} = 75\%$.

30.2 הטלת מטבע

הרעיון בהטלת מטבע הוא בדיוק אותו הרעיון כמו בהתחייבות לסיבית, רק שכאן זה מתנהל באופן הבא:

1. אפרת מגרילה את הסיבית B ואת סדרת הסיביות b_i.
2. בנימין מגריל את c_i ומקבל מאפרת את הפוטונים ומעביר אותם דרך המקטבים שלו.

3. בניגוד למקודם אפרת לא מגלה לו מהי B.

4. בנימין מנחש מה הסיבית B שאפרת בחרה ובודק לפי הסיביות אם הוא צדק או לא.

5. אפרת מגלה לו אם הוא צדק או לא והוא יכול לבדוק זאת על ידי כך: הוא הולך לעמודות לפי הסיבית שאפרת אמרה לו, ואם היא לא שיקרה באותו עמודות הסיביות שהוא קיבל חייבות להיות זהות למה שהיא שלחה (מסקנה 30.4).

למשל, ניקח את דוגמה 30.5 (שבעמוד 58) - במקרה שתואר בדוגמה, אפרת קודם גילתה לבנימין מהי B ורק אחרי זה הוא השווה (כדי לדעת אם היא לא רימתה), כאן הוא קודם בוחר סיבית ורק אז אפרת אומרת לו מה היא בחרה.
אם למשל הוא בוחר את הסיבית 0 ($\oplus$) אזי הוא רואה שבכל העמודות האדומות מה שיצא לו זהה לסיבית שיצא לאפרת (את ה-b-ים היא שולחת לו כאמור) ואז הוא אומר לה שהיא בחרה 0. הוא יכול לבדוק את זה כי אז באמת חייב להיות שכל הסיביות שהוא קיבל יהיו זהות לשלה, כלומר, לכל i: $b_i = c_i$.
אם הוא היה בוחר ב-1 ($\otimes$) אזי בנימין היה מסתכל על העמודות הירוקות ובהסתברות $\frac{1}{2}$ עבור כל סיבית הוא יקבל את אותה סיבית כמו של אפרת, כלומר: בהסתברות של $\frac{1}{2^n}$ (כאשר n הוא מספר הסיביות) הוא יקבל בדיוק את מה שאפרת קיבלה - במקרה כזה הוא יטעה (ויאמר לה שהיא בחרה ב-1 וכך הוא לא יכול לדעת באמת מה תוצאות ההטלה שלה), אבל מספיק שסיבית אחת תצא לא אותו הדבר - והוא יאמר לאפרת שהיא בחרה ב-0 (כי אחרת הוא היה חייב לקבל את אותן תוצאות בדיוק! (מסקנה 30.4).

30.3 העברת מפתח

הערה 30.6. העברת המפתח מורכבת ממספר של מספר שלבים, בגלל ששני השלבים האחרונים מאוד מורכבים הם יתומצתו בקצרה ורק השלב הראשון - העברת המפתח - יפורט.

30.3.1 העברת המפתח

המטרה: להעביר רצף של סיביות ולהיות בטוחים ש:

- הוא אכן עבר בשלמותו.
- קיבלנו את אותו רצף.
- אף אחד לא האזין.

בשניים האחרונים פחות נדון כאן אלא רק נציין אותם ונסביר בקצרה.

1. אפרת בוחרת סדרה אקראית של מקטבים ושל פוטונים.

2. בנימין בוחר סדרה אקראית של מקטבים (כרגע אף אחד מהם לא יודע מה השני בחר).

3. אפרת שולחת לבנימין את הפוטונים דרך המקטבים שהיא בחרה, ובנימין מפענח את הפוטונים לפי המקטבים שלו.

4. הם שולחים אחד לשנייה את סדרת המקטבים שלהם וכל סיבית מתאימה (כלומר, כל פוטון שבנימין קיבל את אותו אחד שאפרת שלחה לו) הם משאירים וסיבית שלא מתאימה (בחרו מקטבים שונים) הם זורקים. סה"כ אמורים להיות 25% סיביות ללא התאמה.

הסבר

נניח כי אפרת ובנימין בוחרים את אותו המקטב, אזי בהכרח בנימין יקבל את אותו הפוטון שאפרת שלחה לו. אם הם בחרו במקטבים שונים, אזי בנימין יקבל בהסתברות $\frac{1}{2}$ פוטון שונה ממה שאפרת שלחה לו, ולכן ההסתברות שהוא יקבל פוטון שונה היא 25% היות וצריך גם שני מקטבים שונים (ויש לכך הסתברות של $\frac{1}{2}$) וגם שהפוטון יצא שונה (הסתברות של $\frac{1}{2}$), סה"כ: $\frac{1}{2}\cdot\frac{1}{2}=\frac{1}{4}=25\%$.

לכן, את כל הסיביות שאינן זהות אצל אפרת ובנימין - הם זורקים ועובדים רק על מה שזהה.

30.3.2 בדיקת המפתח

יכול להיות ששניהם השתמשו באותו מקטב אבל למרות זאת קיבלו סיבית שונה (פוטון שונה) - או בגלל בעיה טכנית או כי מישהו האזין להם ושינה את הכיתוב (לכן הם לא מפרסמים אלו מקטבים יש להם עד שבנימין מקבל את הפוטונים, כי ככה מישהו יכול לדעת ולהאזין מבלי לשנות [לשים את אותו מקטב בדיוק וכך הם לא יכולו לדעת שמישהו האזין להם], ברגע שיש האזנה אזי אם לאפרת יש את המקטב $\oplus$ והיא שולחת את $\uparrow$ ואיב מקשיבה עם מקטב $\otimes$, אזי גם אם לבנימין יש את המקטב $\oplus$ - סיכוי של 50% שהוא יקבל $\uparrow$ ולא את $\rightarrow$ הוא יקבל את הפוטון: $\nearrow$ או $\nwarrow$).
לכן הם בוחרים מספר מקומות מסוים ושולחים בתקשורת רגילה את הסיביות הללו (שכמובן **לא** ישמשו אותם למפתח) - אם הסיבית שונה - סיכוי גבוה שהיה פגם או שמישהו האזין ושינה את הפוטון. לכן אם יש הרבה כאלה - לא כדאי להשתמש במפתח כי ככל הנראה מישהו האזין או שהיה פגם בתקשורת.

30.3.3 תיקון שגיאות והגברת פרטיות

לא נכנס לזה כאן, אבל במקרה שמדובר במספר קטן מאוד של סיביות ישנן דרכים לתקן אותן וגם להגביר את הפרטיות (באמצעות פונקצית גיבוב על המפתח).

תוכן העניינים

רשימת אלגוריתמים

מפתח