פתרון תרגיל מספר 3 ־ מבוא לקריפטוגרפיה ואבטחת תוכנה

שם: מיכאל גרינבאום, **ת.ז:** 211747639

18 במאי 2022

1. **פתרון:**

(א) **צ"ל:** סכימה Π היא לא Mac Secure עם $t=F_k(m_1)\oplus\cdots\oplus F_k(m_d)$

הוכחה:

נגדיר יריב $\mathcal{A}$ לסכימה Π באופן הבא:

i. נקבל פרמטר בטיחות 1^n

ii. נגדיר $m_0=\underbrace{0^n||\ldots||0^n}_{d-1\text{ times}}||1^n$, $m=1^n||\underbrace{0^n||\ldots||0^n}_{d-1\text{ times}}$

iii. נחשב את $t=\mathrm{Mac}_k(m_0)$

iv. נחזיר (m,t)

נשים לב ש־ $\mathcal{A}$ הוא PPT כי רוב הריצה היא Mac_k שהוא PPT וגם נשים לב כי

$$\mathrm{Mac}_k(m)=F_k(1^n)\oplus\underbrace{F_k(0^n)\oplus\cdots\oplus F_k(0^n)}_{d-1\text{ times}}=\underbrace{F_k(0^n)\oplus\cdots\oplus F_k(0^n)}_{d-1\text{ times}}\oplus F_k(1^n)=\mathrm{Mac}_k(m_0)=t$$

ולכן $\boxed{1=\mathrm{Vrfy}_k(m,\mathrm{Mac}_k(m))=\mathrm{Vrfy}_k(m,t)}$,

וגם מתקיים כי $m\notin\{m_0\}=Q$, ולכן $\mathcal{A}$ תמיד מנצח בניסוי $\mathrm{MacForge}_{\Pi,\mathcal{A}}$, כלומר

$$\mathbb{P}\left(\mathrm{MacForge}_{\Pi,\mathcal{A}}(n)=1\right)=1$$

לכל $n\in\mathbb{N}$,

כלומר הראנו שקיים יריב $\mathcal{A}$ ופולינום $p(n)=1$ כך ש

$$\mathbb{P}\left(\mathrm{MacForge}_{\Pi,\mathcal{A}}(n)=1\right)\geq\frac{1}{p(n)}$$

לכל $n\in\mathbb{N}$,

כלומר Π הוא לא Mac Secure מההגדרה, כנדרש

מ.ש.ל.א.☺

(ב) **צ"ל:** סכימה Π היא לא Mac Secure עם $t=F_k(\langle 1\rangle||m_1)\oplus\cdots\oplus F_k(\langle d\rangle||m_d)$

הוכחה:

נגדיר יריב $\mathcal{A}$ לסכימה Π באופן הבא:

i. נקבל פרמטר בטיחות 1^n

ii. נגדיר $m_0=0^{\frac{n}{2}}||0^{\frac{n}{2}},m_1=0^{\frac{n}{2}}||1^{\frac{n}{2}},m_2=1^{\frac{n}{2}}||1^{\frac{n}{2}}$, $m^*=1^{\frac{n}{2}}||0^{\frac{n}{2}}$

iii. נחשב את $t_0=\mathrm{Mac}_k(m_0),t_1=\mathrm{Mac}_k(m_1),t_2=\mathrm{Mac}_k(m_2)$

iv. נחזיר $(m^*,t_0\oplus t_1\oplus t_2)$

נשים לב ש־ $\mathcal{A}$ הוא PPT כי רוב הריצה היא Mac_k שהוא PPT מספר פולינומי של פעמים וגם נשים לב כי

$$\begin{aligned}
&t_0 \oplus t_1 \oplus t_2 = \mathrm{Mac}_k\left(m_0\right) \oplus \mathrm{Mac}_k\left(m_1\right) \oplus \mathrm{Mac}_k\left(m_2\right)\\
&= \left[F_k\left(\langle 1\rangle \|0^{\frac{n}{2}}\right) \oplus F_k\left(\langle 2\rangle \|0^{\frac{n}{2}}\right)\right] \oplus \left[F_k\left(\langle 1\rangle \|0^{\frac{n}{2}}\right) \oplus F_k\left(\langle 2\rangle \|1^{\frac{n}{2}}\right)\right] \oplus \left[F_k\left(\langle 1\rangle \|1^{\frac{n}{2}}\right) \oplus F_k\left(\langle 2\rangle \|1^{\frac{n}{2}}\right)\right]\\
&= \left[F_k\left(\langle 1\rangle \|0^{\frac{n}{2}}\right) \oplus F_k\left(\langle 1\rangle \|0^{\frac{n}{2}}\right)\right] \oplus \left[F_k\left(\langle 2\rangle \|0^{\frac{n}{2}}\right) \oplus F_k\left(\langle 1\rangle \|1^{\frac{n}{2}}\right)\right] \oplus \left[F_k\left(\langle 2\rangle \|1^{\frac{n}{2}}\right) \oplus F_k\left(\langle 2\rangle \|1^{\frac{n}{2}}\right)\right]\\
&= 0^n \oplus \left[F_k\left(\langle 1\rangle \|1^{\frac{n}{2}}\right) \oplus F_k\left(\langle 2\rangle \|0^{\frac{n}{2}}\right)\right] \oplus 0^n = \mathrm{Mac}_k\left(m^*\right)
\end{aligned}$$

ולכן $\boxed{1 = \mathrm{Vrfy}_k\left(m, \mathrm{Mac}_k\left(m\right)\right) = \mathrm{Vrfy}_k\left(m, t_0 \oplus t_1 \oplus t_2\right)}$,
וגם מתקיים כי $m \notin \{m_0, m_1, m_2\} = Q$, ולכן $\mathcal{A}$ תמיד מנצח בניסוי $\mathrm{MacForge}_{\Pi,\mathcal{A}}$, כלומר

$$\mathbb{P}\left(\mathrm{MacForge}_{\Pi,\mathcal{A}}\left(n\right) = 1\right) = 1$$

לכל $n \in \mathbb{N}$,
כלומר הראנו שקיים יריב $\mathcal{A}$ ופולינום $p\left(n\right) = 1$ כך ש

$$\mathbb{P}\left(\mathrm{MacForge}_{\Pi,\mathcal{A}}\left(n\right) = 1\right) \geq \frac{1}{p\left(n\right)}$$

לכל $n \in \mathbb{N}$,
כלומר Π הוא לא Mac Secure מההגדרה, כנדרש

מ.ש.ל.ב.☺

(ג) **צ"ל:** סכימה Π היא לא Mac Secure עם $t = F_k\left(r\right) \oplus F_k\left(m\right)$
הוכחה:
נגדיר יריב $\mathcal{A}$ לסכימה Π באופן הבא:

i. נקבל פרמטר בטיחות 1^n
ii. נחזיר $\left(0^n, \left(0^n, 0^n\right)\right)$

נשים לב ש־ $\mathcal{A}$ הוא PPT כי רוב הריצה היא Mac_k שהוא PPT וגם נשים לב כי

$$\boxed{\mathrm{Vrfy}_k\left(m = 0^n, \left(r = 0^n, t = 0^n\right)\right) = \begin{cases}1 & 0^n = F_k\left(0^n\right) \oplus F_k\left(0^n\right)\\ 0 & else\end{cases} = \begin{cases}1 & 0^n = 0^n\\ 0 & else\end{cases} = 1}$$

וגם מתקיים כי $m \notin \emptyset = Q$, ולכן $\mathcal{A}$ תמיד מנצח בניסוי $\mathrm{MacForge}_{\Pi,\mathcal{A}}$, כלומר

$$\mathbb{P}\left(\mathrm{MacForge}_{\Pi,\mathcal{A}}\left(n\right) = 1\right) = 1$$

לכל $n \in \mathbb{N}$,
כלומר הראנו שקיים יריב $\mathcal{A}$ ופולינום $p\left(n\right) = 1$ כך ש

$$\mathbb{P}\left(\mathrm{MacForge}_{\Pi,\mathcal{A}}\left(n\right) = 1\right) \geq \frac{1}{p\left(n\right)}$$

לכל $n \in \mathbb{N}$,
כלומר Π הוא לא Mac Secure מההגדרה, כנדרש

מ.ש.ל.ג.☺

2. **צ"ל:** ניתן ליצר Π Mac Secure מ־ 2 סכימות שאחת מהן היא Mac Secure
הוכחה:
נגדיר סכמה Π באופן הבא:

(א) $\mathrm{Gen}\left(1^n\right)$: נחשב $k_1 \leftarrow \mathrm{Gen}_1\left(1^n\right)$ ו־ $k_2 \leftarrow \mathrm{Gen}_2\left(1^n\right)$ באופן בלתי תלוי ונחזיר $k_1 \| k_2$

(ב) $\mathrm{Mac}_{k_1||k_2}(m)$: נחזיר $\left(\mathrm{Mac}_{1,k_1}(m), \mathrm{Mac}_{2,k_2}(m)\right)$

(ג) $\mathrm{Vrfy}_{k_1||k_2}(m,(t_1,t_2))$: נחזיר 1 אם"ם $\left(\mathrm{Vrfy}_{2,k_2}(m,t_2)=1\right) \wedge \left(\mathrm{Vrfy}_{1,k_1}(m,t_1)=1\right)$

נשים לב שהכל PPT ונכונה כי היא צירוף של 2 אימותים נכונים, ועתה נוכיח כי Π היא Mac Secure,
נניח בשלילה ש־ Π היא לא Mac Secure כלומר קיים יריב $\mathcal{A}$ שהוא PPT ופולינום $p(\cdot)$ כך ש־

$$\mathbb{P}\left(\mathrm{MacForge}_{\Pi,\mathcal{A}}(n)=1\right) \geq \frac{1}{p(n)}$$

לאינסוף ערכים של $n \in \mathbb{N}$,
נניח בלי הגבלת הכלליות כי Π_1 היא Mac Secure (כל ההוכחה סימטרית וזהה ל־ Π_2)
נגדיר יריב D ל־ Π_1 עם פונקצית אימות $\mathrm{Mac}_{1,k}$ באופן הבא:

(א) נקבל פרמטר בטיחות 1^n

(ב) נגריל $k_2 \leftarrow \mathrm{Gen}_2(1^n)$

(ג) נריץ את $\mathcal{A}(1^n)$ ולכל בקשה שלו m לאימות, נחזיר את $\left(\mathrm{Mac}_{1,k}(m), \mathrm{Mac}_{2,k_2}(m)\right)$

(ד) נשמור את התשובה של $\mathcal{A}$ ב־ $(m^*,(t_1,t_2))$

(ה) נחזיר (m^*,t_1)

נשים לב ש־ D הוא PPT כי רוב ריצתו היא הרצת $\mathcal{A}$ ו־ Mac_{k_2} מספר פולינומי של פעמים והם PPT.
נסמן את התשובה של $\mathcal{A}$ לריצה מסוימת ב־ $(m^*,(t_1,t_2))$, לכן הריצה של D תחזיר (m^*,t_1),
נשים לב שכאשר $\mathcal{A}$ מנצח בניסוי Mac Forge מול Π מתקיים כי $\left(\mathrm{Vrfy}_{2,k_2}(m^*,t_2)=1\right) \wedge \left(\mathrm{Vrfy}_{1,k_1}(m^*,t_1)=1\right)$ וגם $m \notin Q$, ולכן מתקיים כי $\mathrm{Vrfy}_{1,k_1}(m^*,t_1)=1$ וגם $m \notin Q$, כלומר D ניצח בניסוי Mac Forge מול Π_1, כלומר

$$\mathbb{P}\left(\mathrm{MacForge}_{\Pi_1,D}(n)=1\right) \geq \mathbb{P}\left(\mathrm{MacForge}_{\Pi,\mathcal{A}}(n)=1\right) \geq \frac{1}{p(n)}$$

לאינסוף ערכים של $n \in \mathbb{N}$,
כלומר הראנו שקיים יריב D שהוא PPT ופולינום $p(\cdot)$ כך ש־

$$\mathbb{P}\left(\mathrm{MacForge}_{\Pi_1,D}(n)=1\right) \geq \frac{1}{p(n)}$$

לאינסוף ערכים של $n \in \mathbb{N}$, בסתירה לכך ש־ Π_1 היא Mac Secure,
כלומר נקבל כי Π היא Mac Secure, כנדרש

מ.ש.ל.☺

3. **פתרון:**

(א) **צ"ל:** $\hat{\mathcal{H}}$ היא colision resistant hash family
הוכחה:
נניח בשלילה ש־ $\hat{\mathcal{H}}$ היא לא colision resistant hash family,
כלומר קיים $\mathcal{A}$ שהוא PPT ופולינום $p(\cdot)$ כך ש־

$$\mathbb{P}\left(\mathrm{HashColl}_{\hat{\mathcal{H}},\mathcal{A}}(n)=1\right) \geq \frac{1}{p(n)}$$

לאינסוף ערכים של $n \in \mathbb{N}$,
נגדיר יריב D ל־ $\mathcal{H}$ באופן הבא:

i. נקבל פרמטר בטיחות 1^n ומפתח s

ii. נריץ את $\mathcal{A}(1^n,s)$ ונשמור את התוצאה ב־ $(x||b, x'||b')$

iii. נחזיר (x,x')

נשים לב ש־ D הוא PPT כי $\mathcal{A}$ הוא PPT.
נסמן את התשובה של $\mathcal{A}$ ב־ $(x||b, x'||b')$, לכן התשובה של D היא (x, x'),
נניח ש־ $\mathcal{A}$ ניצח בניסוי Hash Coll מול $\hat{\mathcal{H}}$, כלומר $(x||b \neq x'||b') \wedge \hat{H}_s(x||b) = \hat{H}_s(x'||b')$, נשים לב כי

$$H_s(x)||b = \hat{H}_s(x||b) = \hat{H}_s(x'||b') = H_s(x')||b'$$
$$\Rightarrow \boxed{b = b', H_s(x') = H_s(x)}$$

נשים לב כי $x||b \neq x'||b'$ ולכן מהיות $b = b'$, נקבל כי $x \neq x'$ וגם $H_s(x') = H_s(x)$, כלומר (x, x') זה ניצחון בניסוי Hash Coll מול $\mathcal{H}$, כלומר D ניצח בניסוי Hash Coll מול $\mathcal{H}$.
כלומר נקבל כי

$$\mathbb{P}\left(\text{HashColl}_{\mathcal{H},D}(n) = 1\right) \geq \mathbb{P}\left(\text{HashColl}_{\hat{\mathcal{H}},\mathcal{A}}(n) = 1\right) \geq \frac{1}{p(n)}$$

לאינסוף ערכים של $n \in \mathbb{N}$,
כלומר הראנו שקיים יריב D שהוא PPT ופולינום $p(\cdot)$ כך ש־

$$\mathbb{P}\left(\text{HashColl}_{\mathcal{H},D}(n) = 1\right) \geq \frac{1}{p(n)}$$

לאינסוף ערכים של $n \in \mathbb{N}$, בסתירה לכך ש־ $\mathcal{H}$ היא colision resilant hash family,
ולכן נקבל כי $\hat{\mathcal{H}}$ colision resistant hash family, כנדרש

מ.ש.ל.א.☺

(ב) **צ"ל:** $\mathcal{W}$ היא לא colision resistant hash family
הוכחה:
תהי $\mathcal{H}$ colision resistant hash family,
נעשה את הבניית עזר שנעשתה בסעיף הקודם ונגדיר $\hat{\mathcal{H}}$ כמו שהוגדר בסעיף הקודם,
כלומר לכל $x \in \{0,1\}^*, b \in \{0,1\}, s \in \{0,1\}^n$ מתקיים $H_s(x)||b = \hat{H}_s(x||b)$,
עתה נסתכל על $\mathcal{W}$ מעל למשפחת הפונקציות $\hat{\mathcal{H}}$,
לכן נשים לב כי לכל $x \in \{0,1\}^*, b \in \{0,1\}, s \in \{0,1\}^n$ מתקיים

$$W_s(x||b) = \underbrace{H_s(x)||b}_{\text{n-1 left most bits}} = \underbrace{H_s(x)}_{\text{n-1 left most bits}}$$

ולכן נשים לב כי $W_s(x||1) = \underbrace{H_s(x)}_{\text{n-1 left most bits}} = W_s(x||0)$ לכל $x \in \{0,1\}^*, s \in \{0,1\}^n$,
בעקבות העובדה הזאת נגדיר את היריב $\mathcal{A}$ הבא:

i. נקבל פרמטר בטיחות 1^n ומפתח s
ii. החזר $(0^n||0, 0^n||1)$

נשים לב ש $\mathcal{A}$ הוא PPT (לינארי אפילו) וגם $0^n||0 \neq 0^n||1$ וגם $W_s(0^n||0) = W_s(0^n||1)$, כלומר ניצחנו בניסוי Hash Coll מול $\mathcal{W}$, כלומר $\mathbb{P}\left(\text{HashColl}_{\mathcal{W},\mathcal{A}}(n) = 1\right) = 1$ לכל $n \in \mathbb{N}$,
כלומר הראנו שקיים יריב $\mathcal{A}$ ופולינום $p(n) = 1$ כך ש

$$\mathbb{P}\left(\text{HashColl}_{\mathcal{W},\mathcal{A}}(n) = 1\right) \geq \frac{1}{p(n)}$$

לכל $n \in \mathbb{N}$,
כלומר $\mathcal{W}$ הוא לא colision resistant hash family מההגדרה, כנדרש

מ.ש.ל.ב.☺

4. **צ"ל:** Π היא Mac Secure
הוכחה:
נניח בשלילה ש־ Π היא לא Mac Secure כלומר קיים יריב $\mathcal{A}$ שהוא PPT ופולינום $p(\cdot)$ כך ש־

$$\mathbb{P}\left(\text{MacForge}_{\Pi,\mathcal{A}}(n)=1\right)\geq\frac{1}{p(n)}$$

לאינסוף ערכים של $n\in\mathbb{N}$,
נגדיר יריב ל־ F שנסמנו ב־ D עם גישה לאורקל $\mathcal{O}$ באופן הבא:

(א) נקבל פרמטר בטיחות 1^n
(ב) נגריל $k_2\leftarrow\{0,1\}^n$
(ג) נריץ את $\mathcal{A}(1^n)$ ולכל בקשה שלו m, נחזיר את $\mathcal{O}(m)\oplus F_{k_2}(\mathcal{O}(m))$, ונשמור את הבקשות ב־ Q
(ד) נשמור את התוצאה של $\mathcal{A}$ ב־ (m^*,t^*)
(ה) ונחזיר 1 אם"ם $m^*\notin Q$ וגם $t^*=\mathcal{O}(m^*)\oplus F_{k_2}(\mathcal{O}(m^*))$, אחרת 0

נשים לב ש־ D הוא PPT כי הוא רק מריץ את $\mathcal{A}$, ניגש לאורקל מספר פולינומי של פעמים ובודק שייכות של איבר ל־ Q שמכילה מספר פולינומי של איברים.
נשים לב שאם $\mathcal{O}=F_k$ אז D מסמלץ ל־ $\mathcal{A}$ את הניסוי Mac Forge ולכן

$$\mathbb{P}_{k_1\leftarrow\{0,1\}^n}\left(D^{F_{k_1}(\cdot)}(1^n)=1\right)=\mathbb{P}\left(\text{MacForge}_{\Pi,\mathcal{A}}(n)=1\right)$$

נשים לב שאם $\mathcal{O}=f\leftarrow Func_{n\to n}$, תחילה מתקיים כי $f(m^*)$ הוא מתפלג באופן אחיד ובלתי תלוי בשאר הערכים, וגם בשביל ש־ D ינצח בניסוי צריך שיתקיים ש־ $m^*\notin Q$, כלומר $\mathcal{A}$ הוא בלתי תלוי בערך $f(m^*)$ ולכן הסיכוי של $\mathcal{A}$ לנצח במקרה זה הוא בדיוק הסיכוי לנחש את $f(m^*)$ נכון ולכן

$$\mathbb{P}_{f\leftarrow Func_{n\to n}}\left(D^{f(\cdot)}(1^n)=1\right)=\frac{1}{2^n}$$

נשים לב שקיים פולינום $q(n)$ המקיים $\frac{1}{p(n)}-\frac{1}{2^n}\geq\frac{1}{q(n)}$ לכל $n\in\mathbb{N}$,
ולכן נקבל כי

$$\left|\mathbb{P}_{k_1\leftarrow\{0,1\}^n}\left(D^{F_{k_1}(\cdot)}(1^n)=1\right)-\mathbb{P}_{f\leftarrow Func_{n\to n}}\left(D^{f(\cdot)}(1^n)=1\right)\right|\geq\frac{1}{p(n)}-\frac{1}{2^n}\geq\frac{1}{q(n)}$$

לאינסוף ערכים של $n\in\mathbb{N}$,
כלומר הראנו שקיים יריב D ופולינום $q(n)=1$ כך ש

$$\left|\mathbb{P}_{k_1\leftarrow\{0,1\}^n}\left(D^{F_{k_1}(\cdot)}(1^n)=1\right)-\mathbb{P}_{f\leftarrow Func_{n\to n}}\left(D^{f(\cdot)}(1^n)=1\right)\right|\geq\frac{1}{q(n)}$$

לאינסוף ערכים של $n\in\mathbb{N}$, בסתירה לכך ש־ F היא PRF
כלומר Π היא Mac Secure, כנדרש

מ.ש.ל.☺

5. **פתרון:**
(א) **צ"ל:** Π היא left-most bit leakage resilent Mac secure.
הוכחה:
נניח בשלילה ש־ Π היא לא left-most bit leakage resilent Mac secure,
כלומר קיים יריב $\mathcal{A}$ שהוא PPT ופולינום $p(\cdot)$ כך ש־

$$\mathbb{P}\left(\text{MacForgeBitLeakage}_{\Pi,\mathcal{A}}(n)=1\right)\geq\frac{1}{p(n)}$$

לאינסוף ערכים של $n\in\mathbb{N}$,
נגדיר יריב D לסכמה Π עם אלגוריתם יצירת אימותים Mac_k באופן הבא:

.i נקבל פרמטר בטיחות 1^n
.ii נגריל $b \leftarrow \{0,1\}$
.iii נריץ את $\mathcal{A}(1^n, b)$ ולכל בקשה שלו m נחזיר את $\mathrm{Mac}_k(m)$ ונשמור את התשובה ב־ (m^*, t^*)
.iv נחזיר את (m^*, t^*)

נשים לב ש־ D הוא PPT כי הוא רק מריץ את $\mathcal{A}$ שהוא בעצמו PPT,
נשים לב שבמקרה והגרלנו b שהוא באמת הביט השמאלי ביותר של המפתח, אנחנו בניסוי מסמלצים ל־ $\mathcal{A}$ את הניסוי Mac Forge Bit Leakage ולכן נשים לב כי

$$\begin{aligned}
&\mathbb{P}\left(\mathrm{MacForge}_{\Pi,D}(n)=1\right)\\
&\geq \mathbb{P}(\text{guessed correctly last bit}) \cdot \mathbb{P}\left(\mathrm{MacForgeBitLeakage}_{\Pi,\mathcal{A}}(n)=1\right)\\
&= \frac{1}{2} \cdot \mathbb{P}\left(\mathrm{MacForgeBitLeakage}_{\Pi,\mathcal{A}}(n)=1\right) \geq \frac{1}{2 \cdot p(n)}
\end{aligned}$$

לאינסוף ערכים של $n \in \mathbb{N}$,
כלומר הראנו שקיים יריב D שהוא PPT ופולינום $q(\cdot)$ כל ש־

$$\mathbb{P}\left(\mathrm{MacForge}_{\Pi,D}(n)=1\right) \geq \frac{1}{q(n)}$$

לאינסוף ערכים של $n \in \mathbb{N}$, בסתירה לכך ש־ Π היא Mac Secure,
ולכן נקבל כי Π היא left-most bit leakage resilent Mac secure, כנדרש

מ.ש.ל.א.☺

(ב) **צ"ל:** להגדיר left-half bit leakage resilient Mac secure.
הוכחה:
נגדיר ניסוי עזר Mac Forge Left half leakage ביחס ליריב $\mathcal{A}$ וסכמה Π באופן הבא:

.i נקבל פרמטר בטיחות 1^n
.ii נגריל מפתח $k \leftarrow \mathrm{Gen}(1^n)$ ונסמן $k = k_L || k_R$ כאשר $|k_L| = |k_R|$
.iii נריץ $\mathcal{A}(1^n, k_L)$ ולכל בקשה שלו m, נחזיר לו את $\mathrm{Mac}_k(m)$. נשמור את כל הבקשות שלו ברשימה Q
.iv נשמור את התוצאה של $\mathcal{A}$ ב־ (m^*, t^*)
.v נחזיר 1 אם"ם $m^* \notin Q$ וגם $\mathrm{Vrfy}_k(m^*, t^*) = 1$

נאמר ש־ Π היא left-half bit leakage resilient Mac secure אם לכל יריב $\mathcal{A}$ שהיא PPT קיימת פונקציה זניחה $\nu(\cdot)$ כך ש־

$$\mathbb{P}\left(\mathrm{MacForgeLeftHalfLeakage}_{\Pi,\mathcal{A}}(n)=1\right) < \nu(n)$$

לכל $n \in \mathbb{N}$.
באופן דומה נגדיר ניסוי Mac Forge Right half leakage כאשר ההבדל בניסוי הוא שבשלב 3 נריץ את $\mathcal{A}(1^n, k_R)$.
נאמר ש־ Π היא right-half bit leakage resilient Mac secure אם לכל יריב $\mathcal{A}$ שהיא PPT קיימת פונקציה זניחה $\nu(\cdot)$ כך ש־

$$\mathbb{P}\left(\mathrm{MacForgeRightHalfLeakage}_{\Pi,\mathcal{A}}(n)=1\right) < \nu(n)$$

לכל $n \in \mathbb{N}$.

מ.ש.ל.ב.☺

(ג) **צ"ל:** קיימת Π' שהיא לא left-half bit leakage resilient Mac secure.
הוכחה:
תהי $\Pi = \langle \mathrm{Gen}, \mathrm{Mac}, \mathrm{Vrfy} \rangle$ סכמה שהיא Mac Secure,
נגדיר Π' באופן הבא:

.i $\mathrm{Gen}'(1^n)$: נחשב $k \leftarrow \mathrm{Gen}(1^n)$ ונחזיר $k||k$

ii. $\mathrm{Mac}'_{k||k}(m)$: נחזיר $\mathrm{Mac}_k(m)$

iii. $\mathrm{Vrfy}'_{k||k}(m,t)$: נחזיר $\mathrm{Vrfy}_k(m,t)$

נשים לב ש־ $\mathrm{Mac}'_{k||k}(m) = \mathrm{Mac}_k(m)$ וגם $\mathrm{Vrfy}'_{k||k}(m,t) = \mathrm{Vrfy}_k(m,t)$ ולכן $\mathrm{Vrfy}'_{k||k}\left(m, \mathrm{Mac}'_{k||k}(m)\right) =$ $\mathrm{Vrfy}_k(m, \mathrm{Mac}_k(m)) = 1$, כלומר הסכמה נכונה,
עתה יהי $\mathcal{A}$ יריב שהוא PPT, לכן קיימת פונקציה זניחה $\nu(\cdot)$ כך ש־

$$\mathbb{P}\left(\mathrm{MacForge}_{\Pi,\mathcal{A}}(n) = 1\right) < \nu(n)$$

לכל $n \in \mathbb{N}$.
נשים לב שמבחינת $\mathcal{A}$ פונקציות יצירת האימותים של Π, Π' זהות ולכן

$$\mathbb{P}\left(\mathrm{MacForge}_{\Pi',\mathcal{A}}(n) = 1\right) = \mathbb{P}\left(\mathrm{MacForge}_{\Pi,\mathcal{A}}(n) = 1\right) < \nu(n)$$

לכל $n \in \mathbb{N}$,
כלומר לכל יריב $\mathcal{A}$ שהוא PPT קיימת פונקציה זניחה $\nu(\cdot)$ כך ש־

$$\mathbb{P}\left(\mathrm{MacForge}_{\Pi',\mathcal{A}}(n) = 1\right) < \nu(n)$$

לכל $n \in \mathbb{N}$.
כלומר Π' היא Mac Secure.
עתה נוכיח ש־ Π' היא לא left-half bit leakage resilient Mac secure,
נגדיר יריב D באופן הבא:

i. נקבל פרמטר בטיחות 1^n וחלק שמאלי של מפתח k_L

ii. נחזיר $(0^n, \mathrm{Mac}_{k_L}(0^n))$

נשים לב ש־ D הוא PPT כי Mac_{k_L} הוא PPT וגם נשים לב כי $Q = \emptyset \notin 0^n$ וגם $\mathrm{Vrfy}_{k_L||k_L}(0^n, \mathrm{Mac}_{k_L}(0^n)) =$ $\mathrm{Vrfy}_{k_L}(0^n, \mathrm{Mac}_{k_L}(0^n)) = 1$,
כלומר D תמיד מנצח בניסוי Mac Forge, כלומר

$$\mathbb{P}\left(\mathrm{MacForgeLeftHalfLeakage}_{\Pi',D}(n) = 1\right) = 1$$

לכל $n \in \mathbb{N}$.
כלומר הראנו שקיים יריב $\mathcal{A}$ ופולינום $p(n) = 1$ כך ש

$$\mathbb{P}\left(\mathrm{MacForgeLeftHalfLeakage}_{\Pi',D}(n) = 1\right) \geq \frac{1}{p(n)}$$

לכל $n \in \mathbb{N}$,
כלומר Π' הוא לא left-half bit leakage resilient Mac secure מההגדרה, כנדרש

מ.ש.ל.ג.☺

6. **פתרון:**

(א) **צ"ל:** Π' היא right-half bit leakage resilient Mac secure.
הוכחה:
נניח בשלילה ש־ Π' היא לא right-half bit leakage resilient Mac secure,
כלומר קיים יריב $\mathcal{A}$ שהוא PPT ופולינום $p(\cdot)$ כך ש־

$$\mathbb{P}\left(\mathrm{MacForgeRightHalfLeakage}_{\Pi',\mathcal{A}}(n) = 1\right) \geq \frac{1}{p(n)}$$

לאינסוף ערכים של $n \in \mathbb{N}$,
נגדיר יריב D לסכמה Π עם אלגוריתם אימות Mac_k באופן הבא:

i. נקבל פרמטר בטיחות 1^n

ii. נגריל $k_R \leftarrow \{0,1\}^n$
iii. נריץ את $\mathcal{A}(1^n, k_R)$ ולכל בקשה שלו m, נחזיר את $\mathrm{Mac}_k(m \oplus k_R)$, נשמור את כל הבקשות $m \oplus k_R$ ב־ Q
iv. נשמור את התשובה של $\mathcal{A}$ ב־ (m^*, t^*)
v. נחזיר את $(m^* \oplus k_R, t^*)$

נשים לב ש־ D הוא PPT כי הוא מריץ את $\mathcal{A}$ ואת Mac_k מספר פולינומי של פעמים.
עתה נשים לב ש־ D מסמלץ ל־ $\mathcal{A}$ את הניסוי Mac Forge,
נסמן הרצה של $\mathcal{A}$ ב־(m^*, t^*) ושל D ב־ $(m^* \oplus k_R, t^*)$
וגם נשים לב ש־ $\mathcal{A}$ מנצח בניסוי Mac Forge Right Half Leakage מול Π' אם"ם $\mathrm{Vrfy}_{k_L}(m^* \oplus k_R, t^*) = 1$ וגם $m^* \notin Q = \{m_0, m_1, \ldots, m_l\}$ אם"ם $\mathrm{Vrfy}_{k_L}(m^* \oplus k_R, t^*) = 1$ וגם $m^* \oplus k_R \notin Q = \{m_0 \oplus k_R, m_1 \oplus k_R, \ldots, m_l \oplus k_R\}$
אם"ם D מנצח בניסוי Mac Forge מול Π,
כלומר

$$\mathbb{P}\left(\mathrm{MacForge}_{\Pi,D}(n) = 1\right) = \mathbb{P}\left(\mathrm{MacForgeRightHalfLeakage}_{\Pi',\mathcal{A}}(n) = 1\right) \geq \frac{1}{p(n)}$$

לאינסוף ערכים של $n \in \mathbb{N}$,
כלומר קיים יריב D שהוא PPT ופולינום $p(\cdot)$ כך ש־

$$\mathbb{P}\left(\mathrm{MacForge}_{\Pi,D}(n) = 1\right) \geq \frac{1}{p(n)}$$

לאינסוף ערכים של $n \in \mathbb{N}$, בסתירה לכך ש־ Π היא Mac Secure,
ולכן Π' היא right-half bit leakage resilient Mac secure, כנדרש

מ.ש.ל.א.☺

(ב) **צ"ל:** Π' היא לא בהכרח left-half bit leakage resilient Mac secure.
הוכחה:
תהי $\Pi = \langle \mathrm{Gen}, \mathrm{Mac}, \mathrm{Vrfy} \rangle$ סכמה שהיא Mac Secure,
נגדיר Π_1 באופן הבא:

i. $\mathrm{Gen}_1(1^n)$: נחשב $k \leftarrow \mathrm{Gen}(1^n)$ ונחזיר k
ii. $\mathrm{Mac}_{1,k}(m)$: נחזיר $(\mathrm{Mac}_k(m), m)$
iii. $\mathrm{Vrfy}_{1,k}(m, (t_1, t_2))$: נחזיר $\mathrm{Vrfy}_k(m, t_1)$

תחילה נוכיח ש־ Π_1 היא Mac Secure,
נניח בשלילה ש־ Π_1 היא לא Mac Secure,
כלומר קיים יריב $\mathcal{A}$ שהוא PPT ופולינום $p(\cdot)$ כך ש־

$$\mathbb{P}\left(\mathrm{MacForge}_{\Pi_1,\mathcal{A}}(n) = 1\right) \geq \frac{1}{p(n)}$$

לאינסוף ערכים של $n \in \mathbb{N}$,
נגדיר יריב D ל־ Π עם אלגוריתם יציתר אימותים Mac_k באופן הבא:

i. נקבל פרמטר בטיחות 1^n
ii. נריץ את $\mathcal{A}(1^n)$ ולכל בקשה שלו m, נחזיר $(\mathrm{Mac}_k(m), m)$
iii. נשמור את התוצאה של $\mathcal{A}$ ב־ $(m^*, (t_1^*, t_2^*))$
iv. נחזיר (m^*, t_1^*)

נשים לב ש־ D הוא PPT כי הוא רוב ריצתו היא הרצה של $\mathcal{A}$ ושל Mac_k מספר פולינומי של פעמים.
נסמן את התוצאה של $\mathcal{A}$ ב־ $(m^*, (t_1^*, t_2^*))$,
נשים לב ש־ $\mathcal{A}$ ניצח בניסוי Mac Forge מול Π_1 אם"ם $\mathrm{Vrfy}_{1,k}(m^*, (t_1^*, t_2^*)) = 1$ וגם $m^* \notin Q$ אם"ם $1 = \mathrm{Vrfy}_k(m^*, t_1^*)$ וגם $m^* \notin Q$ אם"ם D ניצח בניסוי Mac Forge מול Π, כלומר

$$\mathbb{P}\left(\mathrm{MacForge}_{\Pi,D}(n) = 1\right) = \mathbb{P}\left(\mathrm{MacForge}_{\Pi_1,\mathcal{A}}(n) = 1\right) \geq \frac{1}{p(n)}$$

לאינסוף ערכים של $n \in \mathbb{N}$,
כלומר קיים יריב D שהוא PPT ופולינום $p(\cdot)$ כך ש־

$$\mathbb{P}\left(\mathrm{MacForge}_{\Pi,D}(n)=1\right) \geq \frac{1}{p(n)}$$

לאינסוף ערכים של $n \in \mathbb{N}$, בסתירה לכך ש־ Π היא Mac Secure,
לכן קיבלנו כי Π_1 היא Mac Secure.
עתה נסתכל על הבניית עזר שהוגדרה בתרגיל לבניית Π' ביחס לסכמה Π_1.
נוכיח ש־ Π' היא לא left-half bit leakage resilient Mac secure.
נגדיר יריב $\mathcal{A}'$ לסכמה Π' באופן הבא:

i. נקבל פרמטר בטיחות 1^n וחלק שמאלי של מפתח שנסמנו ב־ k_L
ii. נבקש ערך אימות עבור $m=0^n$, אזי נקבל חזרה את

$$\mathrm{Mac}'_{k_L}(0^n) \stackrel{\mathrm{def}}{=} \mathrm{Mac}_{1,k_L}(0^n \oplus k_R) = \left(\mathrm{Mac}_{k_L}(0^n \oplus k_R), 0^n \oplus k_R\right) = \left(\mathrm{Mac}_{k_L}(0^n \oplus k_R), k_R\right)$$

נשמור את התוצאה ב־ (t_1, k_R)
iii. נחזיר $\left(1^n, \mathrm{Mac}'_{k_L}(1^n \oplus k_R)\right)$

נשים לב ש־ $\mathcal{A}'$ הוא PPT כי הוא רק ניגש ל־ Mac'_{k_L} פעמיים, והאלגוריתם ההוא בעצמו פולינומי.
נסמן את התוצאה של $\mathcal{A}'$ ב־ ר $\left(1^n, \mathrm{Mac}'_{k_L}(1^n \oplus k_R)\right)$,
עתה נשים לב ש־ $1^n \notin \{0^n\} = Q$ וגם

$$\mathrm{Vrfy}'_{k_L}\left(1^n, \mathrm{Mac}'_{k_L}(1^n \oplus k_R)\right) = \mathrm{Vrfy}_{1,k_L}\left(1^n, \mathrm{Mac}'_{k_L}(1^n \oplus k_R)\right) = \mathrm{Vrfy}_{1,k_L}\left(1^n, \mathrm{Mac}_{1,k_L}(1^n \oplus k_R)\right) = 1$$

כלומר $\mathcal{A}'$ תמיד מנצח בניסוי Mac Forge Left Half Leakage ולכן

$$\mathbb{P}\left(\mathrm{MacForgeLeftHalfLeakage}_{\Pi',\mathcal{A}'}(n)=1\right) = 1$$

לכל $n \in \mathbb{N}$.
כלומר הראנו שקיים יריב $\mathcal{A}$ ופולינום $p(n)=1$ כך ש

$$\mathbb{P}\left(\mathrm{MacForgeLeftHalfLeakage}_{\Pi',\mathcal{A}'}(n)=1\right) \geq \frac{1}{p(n)}$$

לכל $n \in \mathbb{N}$,
כלומר Π היא לא left-half bit leakage resilient Mac secure מההגדרה, כנדרש

מ.ש.ל.ב.☺