קריפטו - תרגיל 1

חגי בן יהודה 305237000
יונתן בלאן 204761233

1) הפסקתאות לקחתי מתוך "I am Prepared To Die" של לסון מוזר.

להלן הסבר לגבי סיבוב הבינום:

תחילה בנתתי תרגום פיתון אשר מפרה את מספר המופעים של כל אות בטקסט ומיינה את האותיות לפי ~~המספר~~ מספר המופעים. לאחר מכן יצרתי מילון תרגום, תחילה המילון תרגם כל אות לאות אחרת לפי השכיחויות בשפה האנגלית.

לאחר שם צר קבלתי טקסט בו הופיעו פעמים רבות הצירוף lhos ובכן הופיע hos לפני מילה המתחילה באות l,

לכן הבנתי כי התרגום שלי שגוי (אמור a עובר ל-b כ"ל $a \to b$)

משום שעלפיו:

$o \to o$
$m \to a$
$z \to l$
$h \to s$

לכן בינגתי שינוי לפיו:

$z \to d$
$h \to s$
$o \to a$
$m \to o$

(בעומר lhos אמור להיות lana ו- hos אמור להיות oan)

כעת לאחר שינוי זה הופיע המשפט: i rave dedicated wy iiue

אשר אמור להיות כך הבאה:

i have dedicated my life

כאשר עם התרגום הנוכחי:

$u \to r$
$a \to h$
$h \to u$
$x \to f$
$r \to w$
$e \to m$

לכן בינגתי שינוי נוסף:

$u \to h$
$a \to r$
$h \to f$
$x \to u$
$r \to m$
$e \to w$

כעת הופיע המשפט: all hersons pill live together in harmony and pith ...

אשר אמור כך הבאה להיות:

all persons will live together in harmony and with...

כאשר עם התרגום הנוכחי:

$x \to u$
$p \to p$
$x \to p$
$e \to w$
$x \to w$
$d \to g$

(לאחרי השינוי שעשה לx- מהתרגום הנוכחי המשוער)

(שם אחרי השינוי)

לפי הניסוי: את השינוי

[redacted]

p → u

[redacted]

e → p

x → g

d → w

בסוף הניסוי: goverty and the wreakdown

אשר אמור להיות: Poverty and the breakdown

באשר במילון הנוכחי:

x → g

e → p

d → w

c → b

p → u

c → w (אחרי ההלבה)

לפי הניסוי: את השינוי:

x → p

e → g

d → b

[redacted]

p → w

c → u

בסוף הניסוי היה קרוב ותיפוש בגלל הביטוי לשם הקאות.

הקבוצות נעשה בשלבים הבאים:

a → r	i → x	n → f	w → j
c → u	h → l	q → c	v → k
b → s	k → i	p → w	y → t
e → g	j → v	s → q	x → p
d → b	m → o	r → m	z → d
g → h	l → y	u → h	
f → z	o → a	t → q	

ב) נתון לנו

$\mathcal{E}$ is Perfectly secret

$\longrightarrow$ $\mathcal{E}$ is Perfectly indistinguishable

ניתן כי $\mathcal{E}$ סוד מושלם

אזי לכל $m_0, m_1 \in \mathcal{M}$ מתקיים:

$\forall i \in \{0,1\}$:

$$Pr(M = m_i \mid Enc_k(M) = c) = Pr(M = m_i)$$

$$\longrightarrow \frac{Pr(M = m_i, Enc_k(M) = c)}{Pr(Enc_k(M) = c)} = Pr(M = m_i)$$

$$\longrightarrow \frac{Pr(M = m_i, Enc_k(m_i) = c)}{Pr(Enc_k(M) = c)} = Pr(M = m_i)$$

$$\longrightarrow \frac{Pr(M = m_i)\, Pr(Enc_k(m_i) = c)}{Pr(Enc_k(M) = c)} = P(M = m_i)$$

$$\longrightarrow Pr(Enc_k(m_i) = c) = \underbrace{Pr(Enc_k(M) = c)}_{\text{לא תלוי ב-}i}$$

$$\longrightarrow Pr(Enc_k(m_0) = c) = Pr(Enc_k(m_1) = c)$$

סבבנו.

המשך בעמוד הבא...

נראה כמו

$\mathcal{E}$ is perfectly indistinguishable

$\longrightarrow$ $\mathcal{E}$ is perfectly secrete

$$Pr(M=m_0 \mid Enc_k(M)=c) = \frac{Pr(M=m_0, Enc_k(M)=c)}{Pr(Enc_k(M)=c)} =$$

$$= \frac{Pr(M=m_0, Enc_k(m_0)=c)}{Pr(Enc_k(M)=c)} \underset{\substack{k \text{ ו- } M \\ \text{בלתי תלויים}}}{=} \frac{Pr(M=m_0)\, Pr(Enc_k(m_0)=c)}{Pr(Enc_k(M)=c)} \ominus$$

כמו רש"מ לפם כי:

$$Pr(Enc_k(M)=c) = \sum_{m\in\mathcal{M}} Pr(Enc_k(M)=c \mid M=m)\cdot Pr(M=m) =$$

$$= \sum_{m\in\mathcal{M}} Pr(Enc_k(m)=c)\, Pr(M=m) =$$

$$\underset{\substack{\text{מניחים בלתי} \\ \text{ניתן להתחלה}}}{=} Pr(Enc_k(m_0)=c)\cdot \underbrace{\sum_{m\in\mathcal{M}} Pr(M=m)}_{1} =$$

$$= Pr(Enc_k(m_0)=c)$$

$$\ominus \quad \frac{Pr(M=m_0)\, Pr(Enc_k(m_0)=c)}{Pr(Enc_k(m_0)=c)} = Pr(M=m_0)$$ לפי:

כנדרש.

כדר נראה

$\mathcal{E}$ is adversarial indistinguishable

$\longleftrightarrow$ $\mathcal{E}$ is perfectly indistinguishable

ניתן כי $\mathcal{E}$ מקיים בלתי ניתן להבחנה.

אזי יהיה

$$Pr(Enc_k(m_0)=c) = Pr(Enc_k(m_1)=c)$$

לכל $m_1, m_0 \in \mathcal{M}$ ו- $c \in C$

ניתן כי $f: C \to \{0,1\}$ הינו ההחלטה של A עבור c

כשהוא (צריך לחשוב בהכרח פונקציה, יכול להיות גם משהו מקרי, על המרחב C) ניתן כי M הינו הודעה המוצפנת ע"י ההיצרה האמיתית שבהתחה.

אזי

$$Pr(A \text{ is Right}) = Pr(M=m_0 \cap f(Enc_k(M_0))=0) + Pr(M=m_1 \cap f(Enc_k(M))=1) =$$

$$= Pr(M=m_0 \cap f(Enc_k(m_0))=0) + Pr(M=m_1 \cap f(Enc_k(m_1))=1) =$$

$$= Pr(M=m_0)\cdot Pr(f(Enc_k(m_0))=0) + Pr(M=m_1)\, Pr(f(Enc_k(m_1))=1) =$$

$$= \frac{1}{2}\left(Pr(f(Enc_k(m_0))=0) + Pr(f(Enc_k(m_1))=1)\right) =$$

$$= \frac{1}{2}\left(\sum_{c\in C}\left[Pr(f(c)=0)\cdot Pr(Enc_k(m_0)=c) + Pr(f(c)=1)\cdot Pr(Enc_k(m_1)=c)\right]\right) =$$

הנחנו ש- $\mathcal{E}$ בלתי ניתן להבחנה, לכן $Pr(Enc_k(m_1)=c) = Pr(Enc_k(m_0)=c)$

$$= \frac{1}{2}\left(\sum_{c\in C}\left(\underbrace{Pr(f(c)=0) + Pr(f(c)=1)}_{1}\right)\cdot Pr(Enc_k(m_0)=c)\right) =$$

$$= \frac{1}{2}\cdot\underbrace{\sum_{c\in C} Pr(Enc_k(m_0)=c)}_{1} = \frac{1}{2}$$

לכן הוכחנו 33 צב של הדרישה.

נסמן ל"ט את הצד השני

מספיק להראות

$\neg$($\mathcal{E}$ is perfectly indistinguishable)

$\rightarrow \neg$($\mathcal{E}$ is adrserial indistinguishable)

אכן, אם $\mathcal{E}$ אינה בלתי ניתנת להבחנה, אזי קיימות $m_0, m_1 \in M$ ו- $c_0 \in C$ כך ש:

$$Pr(Enc_k(m_0) = c) > Pr(Enc_k(m_1) = C)$$

אזי נגדיר f באופן הבא: אם $Enc_k(M) = c$ בחר 0, אחרת הגרל.

אזי

$$Pr(A \text{ is Right}) = Pr(M = m_0 \cap f(Enc_k(M)) = 0) + Pr(M = m_1 \cap f(Enc_k(M)) = 1) =$$

$$= Pr(M = m_0 \cap f(Enc_k(m_0)) = 0) + Pr(M = m_1 \cap f(Enc_k(m_1)) = 0) =$$

$$= \sum_{c' \in C} \left[Pr(M = m_0 \cap f(c') = 0) \cdot Pr(Enc_k(m_0) = c') + Pr(M = m_1 \cap f(c') = 1) \cdot Pr(Enc_k(m_0) = c') \right] =$$

$$= \sum_{c' \in C \setminus \{c\}} \left[Pr(M = m_0 \cap f(c') = 0) \cdot Pr(Enc_k(m_0) = c') + Pr(M = m_1 \cap f(c') = 1) \cdot Pr(Enc_k(m_1) = c') \right] +$$

$$+ \underbrace{Pr(M = m_0 \cap f(c) = 0)}_{\text{f מתחזירה 0}} \cdot Pr(Enc_k(m_0) = c) +$$

$$+ \underbrace{Pr(M = m_1 \cap f(c) = 1)}_{\text{f מחזירה 0}} \cdot Pr(Enc_k(m_0) = c) =$$

$$= \frac{1}{4}\left(1 - Pr(Enc_k(m_0) = c)\right) + \frac{1}{4}\left(1 - Pr(Enc_k(m_1) = c)\right) + \frac{1}{2} Pr(Enc_k(m_0) = c) =$$

$$= \frac{1}{4}\left(1 - Pr(Enc_k(m_0) = c)\right) + \frac{1}{4}\left(1 - Pr(Enc_k(m_1) = c)\right) +$$

$$+ \frac{1}{4} \cdot 2\, Pr(Enc_k(m_0) = c) \quad (5)$$

אולם

$$Pr(Enc_k(m_0) = c) > Pr(Enc_k(m_1) = c)$$

לכן

$$\underset{\text{צדק מאמץ}}{>} \frac{1}{4}\left(1 - Pr(Enc_k(m_0) = c)\right) + \frac{1}{4}\left(1 - Pr(Enc_k(m_0) = c)\right) +$$

$$+ \frac{1}{4} Pr(Enc_k(m_0) = c) + Pr(Enc_k(m_1) = c) =$$

$$= \frac{1}{2}$$

לכן קיבלנו

$$Pr(A \text{ is Right}) > \frac{1}{2}$$

בדרוש. לכן הוכחנו את שקולות שלושת ההגדרות.

(3)

א) אכן, יהיו $b \in \mathbb{Z}_p$ ו- $u \sim uni(\mathbb{Z}_p)$

אזי לכל $c \in \mathbb{Z}_p$

$$Pr(u + b = c) = Pr(u = c - b) = \frac{1}{p}$$

(הפעולות בן מ- p מספרים)

לכן $u + b \sim uni(\mathbb{Z}_p)$

כאשר יהי $a \in \mathbb{Z}_p^*$ אזי

$$Pr(au = c) = Pr(u = a^{p-2} c) = \frac{1}{p}$$

כי $a^{p-1} = 1$ ממשפט פרמה הקטן.

ב) אכן, יהי $m \in \mathbb{Z}_p$, אזי

$$Pr(Enc_k(m) = c) = Pr(am + b = c) \quad (=)$$

כאשר אם $m = 0$ אזי b אכן מתפלג אחיד

ולכן $\frac{1}{p}$ $(=)$.

אם $m \neq 0$ אזי מהסעיף הקודם $am + b \sim uni(\mathbb{Z}_p)$

ולכן שוב $\frac{1}{p}$ $(=)$.

לכן בכל מקרה ההסתברות צריכה להיות $\frac{1}{p}$ ולכן:

מאחר ולא הוגדר דבר על m ו- c

$$\forall m_1, m_2, c \quad Pr(Enc_k(m_0) = c) = Pr(Enc_k(m_1) = c)$$

א) הטענה לא נכונה. לדוגמא עבור $m_1 = m_2 = 0$

ו- $m_1' = 1$, $m_2' = 2$

אזי $\sum_{c \in C} Pr((Enc_k(m_1), Enc_k(c_2)) = (c, c)) = 1$

ואילו $\sum_{c \in C} Pr((Enc_k(m_1'), Enc(m_2')) = (c, c)) < 1$

כי $Enc_{(1,0)}(m_1') = 1 \neq 2 = Enc_{(1,0)}(m_2')$

(p הראשוני נלקח לפחות 2 ו- $1 \neq 2 \bmod p$ עבור $p \geq 2$).

ב) במקרה זה ההצפנה אכן בטוחה.

יהיו $(m_1, m_2), (m_1', m_2') \in M^2$ ו- $c_1, c_2 \in C$ כך ש- $m_1 \neq m_2$ ו- $m_1' \neq m_2'$

אזי $Pr((Enc_k(m_1), Enc_k(m_2)) = (c_1, c_2)) =$

$$= Pr(am_1 + b = c_1, am_2 + b = c_2) =$$

יש לנו מערכת משוואות לינארית

$am_1 + b = c_1 \longrightarrow b = c_1 - am_1$

$am_2 + b = c_2$

$\longrightarrow am_2 + c_1 - am_1 = c_2$

$a(m_2 - m_1) = c_1 - c_2$

$a = (c_1 - c_2)(m_2 - m_1)^{p-2}$

$\longrightarrow b = c_1 - (c_1 - c_2)(m_2 - m_1)^{p-2}$

(לכן אם $c_1 = c_2$ ו- $m_1 \neq m_2$ אזי $a = 0$ בסתירה לכך ש- $a \in \mathbb{Z}_p^*$ לכן המקרה הזה אם $c_1 = c_2$ ההסתברות היא 0)

לכן:

$$= \begin{cases} 0 & c_1 = c_2 \\ \frac{1}{p(p-1)} & c_1 \neq c_2 \end{cases}$$

(כי יש עוד תנאים שמגבילים a ו- b וצריך בסיבוי להגרלו)

מאחר ולכל ההנחות שעשינו קודם לגבי m_1', m_2'

גם הם בהתפלגות

$$Pr((Enc_k(m_1'), Enc_k(m_2')) = (c_1, c_2') =$$

$$= \begin{cases} 0 & c_1 = c_2 \\ \frac{1}{p(p-1)} & c_1 \neq c_2 \end{cases}$$

ג) בדיוק נפרוץ, בסעיף הקודם.

ד) אכן, Enc_k מוגדר $M \to C$ כאשר הוא

חח"ע לכל בגמר $c \in C$ יש מוצא יחיד $m \in M$

כך ש- $Enc_k(m) = c$, אחרת לא ניתן לפענח המוצא

המוצפן בצורה חד-חד-ערכית לכן משקולי עובדות

$|M| \leq |C|$ כדרוש.

ה)

אכן, נראה כי המקרה הזה לא

perfectly indistinguishable

ניח $|K| < |M| \underset{\text{שאלה ד}}{\leq} |C|$

נקח $m_0 \in M$, אז נסמן

$$E_{m_0} = \{c \in C \mid \exists k \in K \text{ s.t } Enc_k(m_0) = c\}$$

אז $|E_{m_0}| \leq |K| < |C|$

לכן קיים $c \in C$ כך ש: $c \notin E_{m_0}$

ומאחר ו- $c \in C$ קיים מפתח $k \in K$ והודעה $m_1 \in M$

כך ש: $Enc_k(m_1) = c$, לכן

$$\underbrace{Pr(Enc_k(m_0) = c)}_{0} < \underbrace{Pr(Enc_k(m_1) = c)}_{\text{גדול מ- } 0}$$

לכן משקולות ההגרלות שהוכחנו בשאלה ב,

לא אינו בגמר סודי לחלוטין.

אחרת השינוי הזה המערכת איננה סודית לחלוטין יותר.

דרך אחרת להראות זאת היא שיי רנדומיה לשאלה 5, במקרה בו מגרילים את לס יש יותר הודעות אפשריות מאשר מפתחות.

דרך נשירה היא להראות שרבינו אינו בלתי ניתן להבחנה לירים.

נניח כי f היא הבחירה של הירים ו- A הינו הירים (כמו שהגדרנו בסעיף 2) אזי נגדיר:

$$f(c) = \begin{cases} m_0 & c = m_0 \\ m_1 & c = m_1 \\ 0 \text{ or } 1 \text{ with prob } \frac{1}{2} & \text{else} \end{cases}$$

אזי

$$P(A \text{ wins}) = Pr(M = m_0, f(Enc_K(M)) = 0) + Pr(M = m_1, f(Enc_K(M)) = 1) =$$

$$= Pr(M = m_0, f(Enc_K(m_0)) = 0) + Pr(M = m_1, f(Enc_K(m_1)) = 1) =$$

$$= Pr(M = m_0) \cdot Pr(f(Enc_K(m_0)) = 0) + Pr(M = m_0) \cdot Pr(f(Enc_K(m_1) = 1) =$$

$$= \frac{1}{2}\Big(\sum_{k \in K \setminus \{m_1 \oplus m_0\}} \Big(\big[Pr(Enc_K(m_0) = 0) + Pr(f(Enc_K(m_1)) = 1) \big] \cdot Pr(K = k) \Big) + Pr(k = m_1 \oplus m_0) \cdot \big[Pr(f(Enc_{(m_1 \oplus m_0)}(m_0)) = 0) + Pr(f(Enc_{(m_1 \oplus m_0)}(m_1)) = 1 \big] \Big) =$$

$$= \frac{1}{2}\Big(1 - Pr(K = m_1 \oplus m_0) + \big[\underbrace{Pr(f(m_0) = 1)}_{1} + \underbrace{Pr(f(m_1) = 0)}_{1} \big] \cdot Pr(K = m_1 \oplus m_0) \Big) =$$

$$= \frac{1}{2}\big(1 + Pr(K = m_1 \oplus m_2) \big) > \frac{1}{2}$$

אם המרחק $m_1 \neq m_2$

לכן המערכת לא Perfectly secrete יותר.

$(e^{(3}$

```
def Enc(P, key, m):
    return ((m*key[0] + key[1]) % P)
def Dec(P, key, c)
    d, u, v = xgcd(P, key[0])
    return ((c-key[1])v) % P)

P = random_Prime(10,000, Proof = True)
msg = randint(1,P)
a = randint(1, P-1)
b = randint(0, P-1)
key = (a, b)
enc = Enc(P, key, msg)
dec = Dec(P, key, enc)
```

---

execution example:

P was drawn to be: 7499
a was drawn to be: 2863
b ——— " ——— : 3063
msg ——— " ——— : 43
encryption is: 6188
decryption is: 43