קריפטו – מטלה 1.

עוד מעתוק 305181158

שאלה 1

לפי הגדרה 2:

$\bar{E}$ בטוחה בצורה מושלמת אם לכל התפלגות ~M על M והתפלגות ~C על C שמתקבלת מM מתקיים

לכל זוג הודעות $m \in \widetilde{\mathcal{M}}$, $c \in \widetilde{\mathcal{C}}$ (שהסתברותן > 0)

$$\Pr[M=m]=\Pr[M=m \mid C=c]$$

נניח בשלילה את הגדרה 3, ונראה כי גם הגדרה 2 נשללת.

נניח בשלילה כי קיים תוקף E אשר מנצח במשחק הבא:

Eve: בוחר זוג הודעות $m_0, m_1 \in \mathcal{M}$ ושולח אותן לChellanger.

Chellanger: (מתחיל את המשחק)

$k \leftarrow_R Gen$ (בוחר מפתח)

$b \leftarrow_R \{0,1\}$ (מטיל מטבע)

$c \leftarrow_R Enc(k, m_b)$ (מחשב הצפנה)

שולח את c ל-Eve.

Eve: מנחש ביט 'B.

נאמר שEve מנצח במשחק אמ"מ Eve פולט b'=b בהסתברות > 0.5 ($\Pr(B'=b) > \frac{1}{2}$)

נציג מקרה בו לתוקף E קיימת הסתברות הגדולה מ 0.5 לנצח במשחק.

עבור מערכת מסויימת קיימות שתי הודעות במערכת m0, m1 כך ש:

|K1| = קב' המפתחות אשר ניתן איתם להצפין את m1.

|K0| = קב' המפתחות אשר ניתן איתם להצפין את m0.

K = K1 U K2.

נניח ללא הגבלת הכלליות כי |K0| > |K1|,

(אם הקב' שוות ההסתברויות פשוט שוות לחצי וזהו מקרה לא מעניין של הטלת מטבע)

נניח כי שתי ההודעות ש E מנחש הן m0, m1. E מנחש את הביט לפי החוקיות הבאה: אם ההסתברות ש Gen יפיק מפתח להצפנת m0 גדולה מההסתברות ש Gen יפיק מפתח להצפנת m1 אזי יבחר 0, אחרת יבחר 1. מכך E מנצח במשחק בהסתברות הגדולה מחצי.

Pr[M=m0] עבור המערכת המתוארת שווה לחצי מפני ששווה להסתברות להטלת מטבע.

Pr[M=m0 | C=c] איינו יכול להיות שווה לחצי מפני שהקב' K1, K2 אינן שוות.

ומכך מתקיימת שלילת הגדרה 2. מ.ש.ל.

שאלה 2

למהו1: תהי $\overline{E}$ מע' הצפנה עם נכונות מושלמת, אז $\overline{E}$ היא בעלת בטיחות מושלמת אממ: לכל התפלגות $\widetilde{\mathcal{M}}$ מעל $\mathcal{M}$, ולכל זוג הודעות $m \in \mathcal{M}$, $c \in \mathcal{C}$ שהסתברותן > 0 מתקיים

$$\Pr_{\substack{M \leftarrow \widetilde{\mathcal{M}} \\ K \leftarrow \mathcal{K}}}[C = c] = \Pr_{\substack{M \leftarrow \widetilde{\mathcal{M}} \\ K \leftarrow \mathcal{K}}}[C = c \mid M = m]$$

נחשב Pr[C=c] עבור הצופן המוצג בשאלה,
מפני שקיימות 26^{l} אופציות לבחירת k מתוך K, וקיימות 26^{t} אופציות לבחירת m מתוך M אזי ללא ידיעת שום מידע מעבר לכך ש m נלקח מ M ו k נלקח מ K.
לכל c מתוך C, 26^{-t-l} = Pr[M=m & K=k] = Pr[c=Enc$_{k}$(m)]
ומפני שקיימות 26^{t} אופציות לבחירת c אזי 26^{-t} = 26^{l} * 26^{-t-l} = Pr[C=c].

נחשב Pr[C=c | M=m], ומפני ש m נתון, אזי לכל c מתוך C
Pr[c=Enc$_{k}$(m) | M=m] = Pr[M=m & K=k | M=m] = Pr[K=k] = 26^{-l}
ומפני שקיימות 26^{t} אופציות לבחירת c אזי 26^{-t-l} = Pr[C=c | M=m].

ההסתברויות שונות בסתירה להגדרה הנ"ל, מ.ש.ל.

שאלה 3

א.

2. א. $g_1(n)$, $g_2(n)$ פונ' זניחות.

לפי הגדרה $g(n)$ פונ' זניחה אזי לכל פולינום $p(n)$ קיים $n_0 \in \mathbb{N}$ כך שלכל $n > n_0$ מתקיים $g(n) < \frac{1}{p(n)}$

$\forall p_1(n), p_2(n) \in$ פולינום , $\exists n_0 \in \mathbb{N}, \forall n > n_0 \mid g_1(n) + g_2(n) < \frac{1}{p_1(n)} + \frac{1}{p_2(n)} = \frac{2}{p(n)}$

$\Rightarrow$ ~~[illegible]~~ $\exists p'(n) \in$ {פולינום} $: p'(n) = 2p(n)$

$\Rightarrow g_1(n) + g_2(n) < \frac{1}{p'(n)} \Rightarrow$ לפי הגדרה

כי $p'(n) \in$ {פולינום}

ב.

3.ב. נוכיח באינד' על t.

$t=0$ מקרה ברור,

$t=1$ מקרה ברור, $t=2$ הוכח בסעיף א'.

נניח עבור $t=k$, $k\in\mathbb{N}$: $(g_1(n)+\dots+g_k(n)) \in$ {פונ' זניחות}

נוכיח עבור $t=k+1$: $\underbrace{g_1(n)+\dots+g_k(n)}+g_{k+1}(n)$

פונ' זניחה מהנחה. $\Leftarrow$ $g_1(n)+\dots+g_k(n) = g'(n) \in$ {פונ' זניחה}

נותר להוכיח: $g'(n)+g_{k+1}(n) \in$ {פונ' זניחות}

ומפני ש $g'(n), g_{k+1}(n) \in$ {פונ' זניחות} אזי מההוכחה בסעיף א' סכומם גם פונ' זניחה.

לכן לפי האינדוקציה. מ.ש.ל.

ג. נציג את הסדרת הפונקציות $g(n) = 3^{-n}$ כאשר n שייך ל [0...infinity]

הפונ' מקיימת כי לכל פולינום p(n) קיים n0 כך שלכל n > n0 מתקיים g(n) < 1/p(n)

אך בנוסף מתקיים

$$\sum_{i=1}^{\infty} 3^{-i} = \frac{1}{2}$$

בסתירה לכך שהסכום זניח.

התוצאה עבור t(n) פונקציות שאינו מוגבל שונה מהתוצאה עבור n סופי מפני שאנו יכולים להשתמש בסכום סדרה אינסופי, ולפי חוקי הגבולות באינסוף מתקבל סכום שאינו זניח. מ.ש.ל

ד. לפי הגדרה g(n) אינה פונקציה זניחה אם"ם קיים פולינום כלשהו p(n) וקיים n0 כך שלכל n > n0 מתקיים g(n) > 1/p(n) (שלילה ההגדרה).

<u>שאלה 4</u>

א. נציג אלגוריתם לפתרון הבעיה:

```
Arr is our Array
X = Arr[0]
For (i=1, i< (|Arr|/2), i++)
        If x != Arr[i]
        Return [0,i]
```

האלגוריתם פועל בסיבוכיות O(n/2) = O(n).

ב. מפני שנתון כי לכל x={0,1} קיימים n איברים במערך שלנו אשר אינם פותרים את הבעיה, על סמך הנתון, לכל אלגוריתם לפתרון הבעיה נוכל ליצור תרחיש ובו ב n הפניות הראשונה למערך האלגוריתם לא מגיע לפתרון הבעיה.

ג. ללא הגבלת הכלליות ניגש למקום הראשון המערך, ונניח כי נמצא שם 1.
נבדוק log(n)^t איברים אקראיים שונים במערך, עבור t=1.1.
הסתברות שכל log(n)^t האיברים הם 0 היא $½^{\log(n)^t}$
וזו הסתברות שגיאה זניחה כמו שהוזכר בסוגריים.
זמן ריצת האלגוריתם הוא O(log(n)^t)

<u>שאלה 5</u>

נגדיר (x = upperCast(Min[n/4,log(n-1)]
נציג אלגוריתם עבור n כלשהו אשר בודק האם n אינו ראשוני.
נגריל מערך Arr של x איברים בין 1 ל n,

```
If n%2 == 0 && Arr[y]!=2
        Return true;
Else
        y = rand(n-2);
        For i=0, i<x, i++
                a = Arr[y];
                If gcd(n,Arr[y])==1
                        If  a^(n-1) = 1 mod n or a^(2^r d) = -1 mod n for some 0 ≤ r < s
                        Return false;
                Return true;
```

האלגוריתם פועל בסיבוכיות של O(2+1+(1+1+2)x) = O(x), אשר קטנה מסיבוכיות האלגו' הנאיבי למציאת מס' ראשוני = $O(n^{1/2})$.
הסתברות השגיאה היא $1/4^x$, זאת ע"פ הנתון השני בשאלה כי אם n אינו ראשוני אזי לפחות ¾ מהאיברים מתוך x = [1..n] אשר מקיימים gcd(n,x) = 1 מקיימים גם כן את התנאי $a^{n-1} = 1 \bmod n \text{ or } a^{2^r d} = -1 \bmod n \text{ for some } 0 \le r < s$
ז"א שעבור כל Arr[y] שהוגרל, ההסתברות שיקיים את נתאי ה gcd, אך אינו מקיים את התנאי השני היא ¼ ,
ובדיקה זו מתבצעת במקרה הגרוע ביותר x פעמים. מ.ש.ל