باسمه تعالی

پوریا طادحمله
۴۰۱۲۰۱۳۸۱

رمزنگاری پیشرفته

تمرین سری دوم

۱) الف)

$$M = (a_1 \dots a_t) \rightarrow H(M) = \sum_{i=1}^{t} a_i \mod n$$

در واقع برای محاسبه‌ی این تابع درهم، عدد دلخواه ورودی را در مبنای n می‌نویسیم و سپس جمع ارقام مبنای n آن را محاسبه می‌کنیم. ویژگی‌های آن را در ادامه بررسی می‌کنیم.

* اندازه ورودی متغیر ✓ : چرا که هر عدد دلخواهی را می‌توانیم به این صورت بازنویسی کنیم و شرطی روی t نداریم.

* اندازه خروجی ثابت ✓ : چون در mod n هستیم می‌توان گفت که $\log n$ بیت هر خروجی را نمایش داده و در صورت کمتر بودن هم درست صفر گذاشته و خروجی را ثابت می‌کنیم.

* محاسبه‌پذیری کارا ✓ : به چرا که صرفاً از t عمل جمع و یک کاهش پیمانه تشکیل شده که به سرعت کارا محاسبه می‌شود.

* یک‌طرفه بودن X : به راحتی برای هر مقدار خروجی دلخواه می‌توان ورودی متناظر یافت. مثلاً برای مقدار خروجی h، پیام $M = (h)$ را در نظر می‌گیریم.

* مقاومت در برابر تصادم نوع دوم X : برای پیام M، می‌توان هر تعداد ۰ دلخواه به دنباله اضافه کرد و خروجی یکسان داشته باشد.

$$M = (a_1 - a_t) \rightarrow M' = (a_1 - a_t\ 0\ 0 \dots 0) \quad H(M) = H(M')$$

* برخورد تابی X : از نتیجه قبل استفاده می‌کنیم، هر پیام دلخواه M و M' توضیح داده شده دارای هش یکسان می‌باشند.

ب)

$$H(M) = \left(\sum_{i=1}^{t} a_i\right)^2 \mod n$$

* ویژگی‌های ۱_۳ به طور مشابهی برقرار هستند. ✓

* یک‌طرفه بودن : در صورتی که n یک عدد مرکب بزرگ انتخاب شود برقرار است؛ چرا که یافتن جذر پیمانه‌ای طرفان در زمان چندجمله‌ای مشکل است. ✓

* مقاومت در برابر تصادم دوم و برخوردتابی : X چرا که M, M^- هش یکسانی دارند.

ج) $h(M) = 955$

۲ـ الف)

$n = m > 1$

$h : \mathbb{Z}_{2^m} \to \mathbb{Z}_{2^m}$

$h(x) = x^2 + ax + b \pmod{2^m}$

فرض کنیم دو x, x' که $x \neq x'$ پیدا کنیم که $h(x) = h(x') \Leftarrow$

$$x^2 + ax + b \overset{2^m}{\equiv} x'^2 + ax' + b \Rightarrow x^2 - x'^2 \overset{2^m}{\equiv} a(x' - x) \Rightarrow (x-x')(x+x') \overset{2^m}{\equiv} a\,x \, -(x-x')$$

پس اگر $\gcd(x - x', 2^m) = 1$ می‌توان معادله همنهشتی را ساده کرد:

$$x + x' \overset{2^m}{\equiv} -a \Rightarrow x' = 2^m - x - a$$

یعنی کافی است تابع $g(x)$ را برابر $g(x) := 2^m - x - a$ تعریف کنیم و برای همه x در دامنه محاسبه کرده و اگر $\gcd(g(x) - x, 2^m) = 1$ شد آنگاه $h(g(x)) = h(x)$ شده و پیش تصویر دوم برای

هش فوق می‌یابیم.

ب)

$n > m$

$h : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^m}, \quad h(x) = \sum_{i=0}^{d} a_i x^i \pmod{2^m}, \quad a_i \in \mathbb{Z}_{2^m} \quad 0 \le i \le d$

در این قسمت نشان می‌دهیم دو ورودی x و $2^m + x$ دارای هش یکسان می‌باشند:

$$h(x + 2^m) = \sum_{i=0}^{d} a_i (x + 2^m)^i \pmod{2^m} \xrightarrow[\text{در بسط آن } 2^m \text{ سایر جملات صفر می‌شوند}]{(x+2^m)^i \overset{2^m}{\equiv} x^i \times (2^m)^0} = \sum_{i=0}^{d} a_i x^i = h(x)$$

$\Rightarrow h(x) = h(x + 2^m), \quad x \neq x + 2^m \Rightarrow$

بنابراین پیش تصویر دوم برای هش یافتیم. ■

Scanned by CamScanner

۳- الف) بله برخوردتاب است؛ با برهان خلف نشان می‌دهیم. فرض کنید $x_1 \neq x_2$ ، $\hat{H}(x_1)=\hat{H}(x_2)$ پیدا شوند.

در این صورت اگر $H(x_1)=H(x_2)$ باشد که خلاف برخوردتاب بودن تابع H است. بنابراین فرض می‌کنیم

$x'_1 = H(x_1) \neq H(x_2) = x'_2$ باشند. بنابراین طبق فرض خلف $\hat{H}(x_1) = H(x'_1) = H(x'_2) = \hat{H}(x_2)$ ✗.

یعنی $x'_1 \neq x'_2$ یافتیم که $H(x'_1) = H(x'_2)$ در این صورت خلاف برخوردتاب بودن H است و تناقض می‌باشد

=> بنابراین $\hat{H}(x)$ نیز برخوردتاب است.

ب) خیر برخوردتاب نیست؛ کافی است دو ورودی $(\overset{i}{01}\|y_1)$ و $(\overset{j}{01}\|y_2)$

انتخاب کنیم که خروجی یکسان داشته باشند. به عنوان مثال قرار می‌دهیم $\begin{cases} j=1 \\ i=2 \end{cases}$ و $y_2 = H(y_1)$.

$\Rightarrow \hat{H}(\overset{2}{01}\|y_1) \overset{?}{=} \hat{H}(\overset{1}{01}\|H(y_1))$ بنابراین ساختار برخوردتاب نمی‌باشد. =>

$= H(H(y_1)) \overset{\checkmark}{=} H(H(y_1))$ تعریف

طبق تعریف

ج) اره تابع فوق یکطرفه می‌باشد چرا که اگر ما نیاز داریم که بیت اول صفر دارند، ورودی برابر ادامه‌ی خروجی تابع می‌باشد.

$y = 0x_1x_2\cdots x_n \Rightarrow x = x_1\cdots x_n \;;\; y = \hat{H}(x)$

ثانیاً برخوردتاب می‌باشد. (با برهان خلف) اگر $x_1 \neq x_2$ و $\hat{H}(x_1)=\hat{H}(x_2)$ اولاً خروجی از حالت اول نمی‌تواند باشد

چرا که اگر از حالت اول یعنی $(0\|x)$ باشد آنگاه $(0\|x_1)=(0\|x_2) \Rightarrow x_1 = x_2$ ✗.

بنابراین حالت دوم است و یعنی $(1\|H(x_2))=(1\|H(x_1)) \Rightarrow H(x_1)=H(x_2)$ ✗ یعنی برخوردتاب

بودن H نقض می‌شود. => بنابراین $\hat{H}$ برخوردتاب می‌باشد. => بنابراین برخوردتاب بودن لزوماً به معنی یکطرفه بودن نیست.

د) در کتاب‌هایی که پیش‌تصویر تابع درهم را آشنایی برای پیش‌تصویر‌یابی می‌گیرند می‌گویند اگر با داشتن x_1 و $h(x_1)$ معلوم بتوان

x_2 پیدا کرد که $x_1 \neq x_2$ و $h(x_1)=h(x_2)$ آنگاه مقاومت برای $h(x_1)$ نیز می‌توان x_1 پیدا کرد. در صورتی که

ممکن است با داشتن y بتوان به راحتی x ای پیدا کرد که $h(x)=y$ ولی نتوان x دیگری یافت که این

خروجی را بدهد. همان مثالی که در قسمت قبل دیدیم: با داشتن $h(x)=0x$ به راحتی x خروجی $0x$ را می‌دهد

ولی نمی‌توان $x \neq y$ یافت که $h(y)=0x$.

تفاوت اصلی هم در این روش صرفاً برای توابع چندضابطه‌ای خاص است که در تعریف مطرح می‌کنیم و در عمل، برای همه توابع برخورد نمی‌کنیم

و همان روش را می‌توان در اکثر مواقع به کار برد. ☐

(*) با توجه به تعاریف موجود در تمامی قسمت ۲، بعضی‌ها اشتباه از صحت سؤال

۷) الف) فرض می‌کنیم H_1 برخوردتاب باشد و نسبت به برخوردتابی H_2 نیست.

بله برخوردتاب است؛ از آن جایی که خروجی‌های n بیتی است، اگر $x_1 \neq x_2$ یافت شود که

$\hat{H}(x_1)=\hat{H}(x_2)$ باشد، باید n بیت اول برابر و n بیت دوم نیز برابر باشند ⇐

$$\hat{H}(x_1)=\hat{H}(x_2) \Rightarrow \overline{\quad|\quad}.\overline{\quad||\quad} = \overline{\quad|\quad}.\overline{\quad||\quad} \Rightarrow \begin{cases} H_1(x_1)=H_2(x_2) \\ H_2(x_1)=H_2(x_2) \end{cases}$$

که با برخوردتابی H_1 تناقض دارد. پس فرض اولیه اشتباه بوده و $\hat{H}(x)$ برخوردتاب می‌باشد.

ب) x خیر لزومی ندارد برخوردتاب باشد؛ فرض کنیم $x_1 \neq x_2$ که $\hat{H}(x_1)=\hat{H}(x_2)$ ⇐ n بیت اول

$$\begin{cases} H_1(H_2(x_1)) = H_1(H_2(x_2)) \xrightarrow[\text{است}]{\text{برخوردتاب } H_1} H_2(x_1)=H_2(x_2) \\ H_2(\underbrace{H_1(x_1)}_{x_1'}) = H_2(\underbrace{H_1(x_2)}_{x_2'}) \xrightarrow[\text{برخوردتاب } H_1]{x_1' \neq x_2'} H_2(x_1')=H_2(x_2') \end{cases}$$

n بیت دوم

یعنی کافیست $H_2(x_1)=H_2(x_2)$ و $H_2(x_1')=H_2(x_2')$ باشد

که چون H_2 برخوردتاب نیست می‌توان در زمان چندجمله‌ای به این هدف رسید.

ادامه ۴ - ج) بله برخوردناپذیر است : (فرض خلف) $x_1 \neq x_2$: $\hat{H}(x_1)=\hat{H}(x_2)$

n بیت اول

$$\begin{cases} H_1(H_2(x_1) \| x_1) = H_1(H_2(x_2) \| x_2) \xrightarrow[\text{است}]{\text{برخوردناپذیر } H_1} \underbrace{H_2(x_1)}_{n \text{ بیت}} \| x_1 = \underbrace{H_2(x_2)}_{n \text{ بیت}} \| x_2 \\ H_2(H_1(x_1) \| x_1) = H_2(H_1(x_2) \| x_2) \end{cases}$$

برای برقراری این تساوی باید بیت‌ها نظیر به نظیر برابر باشند و چون خروجی H_2 ثابت n بیتی است می‌توان آن را حذف کرد و نتیجه گرفت سایر بیت‌ها برابرند.

$\Rightarrow x_1 = x_2$

که خلاف فرض اولیه تمایز x_1 و x_2 است. بنابراین $\hat{H}$ برخوردناپذیر است. ∎

۵- الف) خیر برخوردناپذیر نیست؛ چرا که هر ورودی که طول آن مضرب صحیح از طول مطلوب نیست را اگر در نظر بگیریم مانند x، آن 00 و $x' := x \| 0$ نیز خروجی هش یکسانی خواهد داشت.

* اگر هر ورودی ؟ را بپذیرد: آن 00 برخوردها آن شبیه به برخوردهای h خواهد داشت. چنانچه بتوان برای h $x^1 \neq x^2$ برخورد یافت H نیز شکسته می‌شود:

$$H(x^1) = H(x^2) \Rightarrow h(z^1_{B-1} \| x^1_B) = h(z^2_{B-1} \| x^2_B)$$

$$\xrightarrow[\text{و } h \text{ برخوردناپذیر}]{\text{طول خروجی } h \text{ ثابت}} \begin{cases} x^1_B = x^2_B \\ z^1_{B-1} = z^2_{B-1} \Rightarrow h(z^1_{B-2} \| x^1_{B-1}) = h(z^2_{B-2} \| x^2_{B-1}) \Rightarrow \dots \end{cases}$$

ب) بله برخوردناپذیر است. اثبات مشابه قسمت دوم قبل: فرض خلف) $H(x^1)=H(x^2)$, $x^1 \neq x^2$

$\Downarrow$

$$z^1_B \| L^1 = z^2_B \| L^2 \xrightarrow[\text{(تساوی نظیر به نظیر بیت‌ها)}]{\text{طول خروجی هش } h \text{ (یعنی } z_B\text{) ثابت است (n بیت)}} \begin{cases} L^1 = L^2 \rightarrow \text{به شکل این طول‌ها باید قطعاً برابر باشند.} \\ z^1_B = z^2_B \Rightarrow h(z^1_{B-1} \| x^1_B) = h(z^2_{B-1} \| x^2_B) \end{cases}$$

$$\xRightarrow{\text{برخوردناپذیر}} \begin{cases} x^1_B = x^2_B \checkmark \\ z^1_{B-1} = z^2_{B-1} \end{cases} \Rightarrow$$

و از آن جایی که طول‌ها برابرند، هر دو به اندازه مساوی ادامه پیدا می‌کنند و تمام قسمت‌های x^1 و x^2 یکسان می‌شوند.

۵-ج) بله برخوردتاب است و اثبات هم که قسمت‌های قبل داده شده ✓

د) خیر لزوما برخوردتاب نیست. تابع هش برخوردتاب h را به گونه‌ای در نظر می‌گیریم که بتوان در زمان چندجمله‌ای L و $x \in \{0,1\}^n$ یافت که $h(L,x)=L-n$ باشد، بنابراین به ازای این h، خروجی تابع کلی هش H به ازای همه پیام‌های y از طول L-1 برابر است با خروجی پیام (x,y) از طول L.

بنابراین برخوردتاب نمی‌باشد.

ه) تابع فشرده‌ساز برخوردتاب $\hat{h} : \{0,1\}^{2n-1} \to \{0,1\}^{n-1}$ را در نظر می‌گیریم و تابع غیر برخوردتاب h را

به این صورت تعریف می‌کنیم، $h: \{0,1\}^{2n} \to \{0,1\}^n$,
$$\begin{cases} h(0\|x) = 0\|\hat{h}(x) \\ h(1\|x) = 1^n \end{cases}$$

واضح است که برخوردتاب نیست و به ازای هر x دلخواه، $h(1\|x)$ خروجی 1^n می‌دهد.

حال تابع H را از h فوق می‌سازیم و نشان می‌دهیم برخوردتاب است.

* تنها شرط این است که IV الزاما که انتخاب می‌کنیم بیت اول باید صفر باشد تا خروجی ثابت 1^n تولید نشود.

⇐ در این صورت در مرحله اول داریم،

$h(IV^2\|x_1^2) = h(IV^1\|x_1^1)$

بیت اول صفر است ⇐ $z_1^1 = 0\|\hat{h}(IV'\|x_1^1) = 0\|\hat{h}(IV'\|x_1^2) = z_1^2$ ⇐ $0=0$, $x_1^1 = x_1^2$, $IV'^1 = IV'^2$ ✓✓ (برخوردتاب بودن $\hat{h}$)

(مقدار IV بدون بیت اول)

همچنین برای مرحله دوم داریم:

$h(z_1^1\|x_2^1) = h(z_1^2\|x_2^2)$ —(در مرحله قبل دیدیم بیت اول z_1 صفر است)→ $z_2 = 0\|\hat{h}(z_1'^1\|x_2^1) = 0\|\hat{h}(z_1'^2\|x_2^2)$ → صفر صفر

(مقدار z_1 بدون بیت اول)

Scanned by CamScanner

$\xrightarrow[\hat{h}]{\text{بخود ترتیب موجود}}$ $\begin{cases} x_2^1 = x_2^2 \\ z_1^1 = z_2^2 \end{cases}$ → همین ترتیب تا z_B نیز همین نتیجه می‌رسد.

و همینطور به ازای دو $x^1 \neq x^2$، $H(x^1) \neq H(x^2)$ خواهند بود و تابع برخورد تاب نمی‌باشد.

و) * بدون پیش تصویر تاب باید یک طول ورودی مشخص کنیم که ما آن را L در نظر بگیریم.

درحالت کلی غلط است؛ برای مثال تابع هش ما را طوری می‌سازیم که پیش تصویر تاب باشد ولی به ازای هر x دلخواه $x \in \{0,1\}^n$، داشته باشیم $h(x\|L) = 0^n$.

بنابراین H ساخته شده از این تابع هش به ازای هر ورودی x با طول L خروجی 0^n را می‌دهد و یکطرفه نیست.

ز) درحالت کلی غلط است؛ تابع هش کلیددار h^s (کلید s) را به شکلی می‌سازیم که پیش تصویر تاب دوم باشد

و برای هر $x \in \{0,1\}^n$ داشته باشیم،

$h^s([s]_n \| x) = h^s(x \| [s]_n) = 0^n$ و $h^s(0^{2n}) = [s]_n$

که در آن $[s]_n$ برابر n بیت اول s می‌باشد. با این ترتیب تابع H ای که از این h ساخته می‌شود

را می‌توان با این حمله پیش تصویر دوم آن را یافت:

۱) به دست آوردن خروجی 0^n ؛ ۲) مشخص کردن کلید s ۳) خروجی $[s]_n$ [illegible] با احتمال ۱ موفق می‌شود

چرا که * تک انکودینگ n بیتی از n.

$$\begin{cases} H^s(0^n) = h^s(h^s(0^n, 0^n), \langle n \rangle) = h^s([s]_n, \langle n \rangle) = 0^n \\ H^s([s]_n) = h^s(h^s(0^n, [s]_n), \langle n \rangle) = h^s([s]_n, \langle n \rangle) = 0^n \end{cases}$$

۶_ الف) خیر امکان‌پذیر نیست چون اولاً همان‌طور که گفته شده تابع چکیده‌ساز یک‌طرفه است و ثانیاً برد توابع چکیده‌ساز بسیار کوچک‌تر از دامنه است و پوشایی بین اعضا باید تناظر یک‌به‌یک ممکن نیست.

برای این کار باید اولاً طول خروجی حداقل به اندازه طول ورودی باشد و ثانیاً عملیات‌های انجام شده برگشت‌پذیر باشند که عملاً یک‌طرفه بودن را از بین ببرد!

ب)

$$m = (m_1, m_2, \cdots, m_8)$$

$$\xrightarrow[\text{مرحله اول}]{E(m_1)} C_1 \xrightarrow[\text{مرحله ۲}]{} C_1 \oplus m_2 \xrightarrow{\text{مرحله ۳}} E(C_1 \oplus m_2) \longrightarrow \cdots$$

$$M = (B_1, B_2) \xrightarrow{\text{چکیده}} RSAH(B_1, B_2) = RSA(RSA(B_1) \oplus B_2)$$

می‌خواهیم C_1, C_2 را طوری بیابیم که:

$$RSAH(C_1, C_2) = RSAH(B_1, B_2)$$

* از ضعف عمل XOR استفاده می‌کنیم که می‌دانیم $X \oplus (A \oplus X) = A$!

یعنی با داشتن C_1، C_2 را تعریف می‌کنیم:

$$C_2 := RSA(C_1) \oplus RSA(B_1) \oplus B_2$$

$$\Rightarrow RSAH(C_1, C_2) = RSA(RSA(C_1) \oplus RSA(C_1) \oplus RSA(B_1) \oplus B_2)$$

$$= RSA(RSA(B_1) \oplus B_2) = RSAH(B_1, B_2)$$

یعنی حاصل هش یکسان با B_1, B_2 دارند. ✓

۷- الف) در این ساختار داریم:

$$E(\overline{M_i}, \overline{H_{i-1}}) = \overline{E(M_i, H_{i-1})} \oplus \overline{H_{i-1}} = E(M_i, H_{i-1}) \oplus H_{i-1}$$

خاصیت DES ، خاصیت XOR

یعنی خروجی هش برای پیام M با IV اولیه "I" برابر است با خروجی هش پیام N با IV اولیه $\overline{I}$

که N این گونه ساخته می‌شود: $M = M_1 \| M_2 \| \cdots \| M_n \rightarrow N = \overline{M_1} \| M_2 \| M_3 \| \cdots \| M_n$

و به صورت تصادفی نیست.

ب) به طور مشابه داریم:

$$\overline{M_i} \oplus E(M_i, H_{i-1}) = \overline{M_i} \oplus \overline{E(M_i, H_{i-1})} = \overline{M_i} \oplus E(\overline{M_i}, \overline{H_{i-1}})$$

یعنی خروجی هش M با $IV = I$ برابر خروجی هش N با $IV' = \overline{I}$ می‌باشد که N برابر است با:

$M = M_1 \| M_2 \| \cdots \| M_n \longrightarrow N = \overline{M_1} \| M_2 \| M_3 \| \cdots \| M_n$

۸- الف) اگر برخورد پیدا شود یعنی به ازای $i \neq j$ ، $y_i = y_j \Leftarrow$ تعریف CBC :

$$y_{i-1} \oplus x_i = y_{j-1} \oplus x_j \xrightarrow[\text{را هم معلوم هستند}]{\text{مقادیر } y_{i-1} \text{ و } y_{j-1}} x_i \oplus x_j = y_{i-1} \oplus y_{j-1}$$

← اطلاعاتی راجع به ورودی به دست می‌آید ✓

Scanned by CamScanner

ب) با توجه به ورودی‌های تولید اگر به اندازه 2^{32} تعداد را داشته باشیم، احتمال برخورد برابر می‌شود با:

$$1-e^{-\frac{(O(\frac{32}{2}))^2}{2^2}} \simeq 1-e^{-\frac{2^2}{2\cdot 2^2}} = 1-e^{-4^2}$$

ج) n: تعداد اسامی

$$P(n;H) \simeq 1-e^{-\frac{n^2}{2H}} \Rightarrow n(P;H) = \sqrt{2H\ln\frac{1}{1-p}}$$

$$1 \simeq 1-e^{-\frac{n^2}{32}} \Rightarrow e^{-\frac{n^2}{2\times 2^{64}}} \simeq 0$$

اگر خروجی تا چند رقم اعشار، تقریب بزنیم، $e^{-8} \simeq 0 \Leftarrow$

$$-8 > \frac{-n^2}{2\times 2^{64}}$$

$$2^{68} \leq n^2 \Rightarrow 2^{34} \leq n$$

2^{34} تعداد برخورد رخ می‌دهد.

از ۲ قسمت ب و ج می‌بینیم طبق انتظار احتمال یافتن برخورد بیشتر از پیش‌بینی‌ها است چرا که در برخورد هر زوج (m, t) قبول است ولی در پیش‌بینی به داده شده و احتمال یافتن خروجی ورودی قسمتم کاهش می‌یابد.

۹- الف)

$$|R| = 2^k \Rightarrow P(H(m) = y) = 1-\left(1-\frac{1}{|R|}\right)^t \simeq 1-e^{-t/2^k}$$

ب) معادله مشابه داریم. $P = 1-e^{-\frac{t}{2^k}}$ / (m از قبل مشخص است)

ج) احتمال برخورد برابر $P \simeq 1-e^{-\frac{t^2}{2^k}}$ است وقتی حالات 2^k باشد $\Leftarrow$ بنابراین احتمال انتخاب ۲ خروجی از t، $\binom{t}{2}$ که برخورد دارند برابر

$$\frac{N-1}{N}\times\frac{N-2}{N}\times\cdots\times\frac{N-(t-1)}{N} \simeq O\left(\frac{-t(t-1)}{2\times 2^k}\right) \,\%\, \frac{t(t-1)}{2^k}$$