دانشگاه تهران

پردیس دانشکده‌های فنی

دپارتمان مهندسی برق و کامپیوتر

امنیت شبکه پیشرفته

تمرین تحلیلی سری اول

محمدحسین بدیعی

شماره دانشجویی 810199106

استاد : دکتر محمد صیاد حقیقی

پاییز 1400-1401

پاسخ سوال اول)

پاسخ این سوال خیر است و این جمله درست نیست. ابتدا دو مرجع اسلاید استاد و ویکی‌پدیا را بررسی می‌کنیم. سپس توضیحات را ارائه می‌نماییم.

مرجع اول: اسلاید سوم استاد صفحه 13

➡**6.** It is computationally infeasible to find any pair (x, y) such that $H(x)=H(y)$.
(A hash function with this property is referred to as **collision resistant**. This is sometimes referred to as **strong collision resistant**)

مرجع دوم: ویکی‌پدیا

In cryptography, **collision resistance** is a property of cryptographic hash functions: a hash function *H* is collision-resistant if it is hard to find two inputs that hash to the same output; that is, two inputs *a* and *b* where $a \neq b$ but $H(a) = H(b)$.[1]:136 The pigeonhole principle means that any hash function with more inputs than outputs will necessarily have such collisions;[1]:136 the harder they are to find, the more cryptographically secure the hash function is.

توضیحات:

با توجه به مراجع فوق این جمله درست نیست. در واقع هر دو مرجع بیان می‌دارند که collision resistant بدین معنی است که احتمال یافتن زوجی که هش‌های یکسانی داشته باشند بسیار کم است یا به بیان ویکی‌پدیا دشوار است. این جملات اصلا بدین معنا نیست که احتمال یافتن چنین زوجی صفر (0) است بلکه بدین معناست که این احتمال بسیار کم است و لذا جمله‌ی مسأله طبق استدلال‌های اینجانب نمی‌توانند صحیح باشد.

از نظر تحلیلی نیز این موضوع کاملا قابل اثبات است. به فرض، این حالت را در نظر بگیرید که ما برای تمامی حالاتی که هش‌های n بیتی (طبق صورت سوال) وجود دارد، یک پیام متناظرشان را در نظر گرفته‌ایم(پیمایش کردیم و تناظر یک به یک را ایجاد نمودیم)؛ به عنوان نمونه با توجه به آنکه طول پیام می‌تواند بیشتر از n بیت هم باشد، ما یک پیام با سایزی بزرگتر از n بیت در نظر می‌گیریم که طبیعتا در مجموعه پیام‌های قبلی نبوده باشد؛ آنگاه چونکه ذکر کردیم یکبار تمامی هش‌ها با یک پیامِ متناظرشان پیمایش شده‌اند لذا هش این پیام جدید باید یکی از هش‌های همان مجموعه‌ی پیمایش شده باشد و طبیعتا تکراری است. لذا احتمال صفر نیست و طبق تعریف، فقط یافتن این زوج دشوار است.

پاسخ سوال دوم)

این سوال را با توجه به صحبت‌های پایانی استاد در session 6 پاسخ می‌دهیم.

مسأله را با در نظر داشتن آنکه تعداد تلاش‌های لازم به جهت آنکه احتمال collision بالای 50% داشته باشیم را برابر k در نظر می‌گیریم. آنگاه با توجه به روندی که در birthday paradox طی کردیم، داریم:

$$\bar{P}(k) = 1 \times \left(1-\frac{1}{2^n}\right) \times \left(1-\frac{2}{2^n}\right) \times \cdots \times \left(1-\frac{k-1}{2^n}\right)$$

$$e^{x} \approx 1+x \quad \underset{x \ll 1}{(\text{با توجه به بسط تیلور})} \Rightarrow e^{-mx} \approx (1-x)^m \quad \text{for } x \ll 1$$

$$\xrightarrow[\text{نکات فوق}]{\text{با استفاده از}} \bar{P}(k) = 1 \times e^{-\frac{1}{2^n}} \times e^{-\frac{2}{2^n}} \times e^{-\frac{3}{2^n}} \times \cdots \times e^{-\frac{k-1}{2^n}}$$

$$\bar{P}(k) = e^{-\frac{1}{2^n}\left(1+2+3+\cdots+(k-1)\right)}$$

$$\bar{P}(k) = e^{-\frac{1}{2^n}\left(\frac{k(k-1)}{2}\right)} \approx e^{-\frac{k^2}{2^{n+1}}}$$

$$\Longrightarrow 1-\bar{P}(k) = 1-e^{-\frac{k^2}{2^{n+1}}}$$

به جهت آنکه خواسته‌ی حالت رخ دهد می‌بایست $1-\bar{P}(k) > \frac{1}{2}$ شود.

$$1-\bar{P}(k) > \frac{1}{2} \Longrightarrow 1-e^{-\frac{k^2}{2^{n+1}}} > \frac{1}{2} \Rightarrow e^{-\frac{k^2}{2^{n+1}}} < \frac{1}{2}$$

$$\xrightarrow{\text{از طرفین ln می‌گیریم}} -\frac{k^2}{2^{n+1}} < -\ln 2 \Rightarrow k^2 > 2^{n+1}\ln 2$$

$$\begin{cases} k^2 > 2^{n+1}\ln 2 \\ \ln 2 > \frac{1}{2} \end{cases} \Rightarrow k^2 > 2^{n+1}\left(\frac{1}{2}\right) \Rightarrow k^2 > 2^n$$

$$\Rightarrow \boxed{k > 2^{\frac{n}{2}}}$$

با توجه به اینکه تعداد تلاش‌های لازم (بررسی colliding hash از طریق مقایسه هش مسیج‌ها) را بدست اوردیم پس می‌توانیم ادعا کنیم که قدرت یک هش مقاوم برابر است با:

$$\Rightarrow \text{The strength of strong collision resistant hash function: } 2^{\frac{n}{2}}$$

پاسخ سوال سوم)

با توجه به اینکه $n = 64$ است پس 2^{64} مقدار مختلف بلاک ورودی به 2^{64} مقدار مختلف خروجی map می‌شوند.

حال مجموعه‌ی کل جایگشت هایی را که عنصر i ام در آن ثابت است را با $|A_i|$ نشان داده و داریم:

$$|A_i| = (n-1)!$$

$$|A_i \cap A_j| = (n-2)!$$

مجموعه کل جایگشت هایی را که عنصر i و j در آن ثابت است.

$$\vdots$$

بدین ترتیب می‌توانیم تعداد جایگشت هایی را که حداقل یک نقطه‌ی ثابت دارند را به صورت زیر نوشت:

$$M = |A_1 \cup A_2 \cup A_3 \dots \cup A_n| = \left|\bigcup_{k=1}^{n} A_k\right|$$

حال طبق اصل شمول و عدم شمول داریم:

$$M = \left|\bigcup_{k=1}^{n} A_k\right| = \sum |A_i| - \sum |A_i \cap A_j| + \dots + (-1)^{n+1} \left|\bigcap_{k=1}^{n} A_k\right|$$

$$M = \sum_{k=1}^{n} (-1)^{k+1} \binom{n}{k} (n-k)! = \sum_{k=1}^{n} \frac{(-1)^{k+1}\, n!}{k!} = (n!) \sum_{k=1}^{n} \frac{(-1)^{k+1}}{k!}$$

$$\Rightarrow P(\text{حداقل یک fixed point داشته باشیم}) = \frac{\text{تعداد حالات با حداقل یک fixed point}}{\text{تعداد کل حالات}} = \frac{n! \sum_{k=1}^{n} \frac{(-1)^{k+1}}{k!}}{n!} = \sum_{k=1}^{n} \frac{(-1)^{k+1}}{k!} \qquad (*)$$

از طرفی می‌دانیم $e^{-1} = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} \Rightarrow 1 - e^{-1} = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k!}$

همچنین با توجه به اینکه n مقدار بزرگی است $(n \to 2^{64})$ پس داریم:

$$\Rightarrow P = 1 - (e^{-1} + \varepsilon) \simeq 1 - e^{-1} \simeq 0.63 \Rightarrow \boxed{P \simeq 0.63}$$

لذا احتمال اینکه حداقل یک fixed point داشته باشیم 63% است.

پاسخ سوال چهارم)

a)

$$E(k) = E(k') \quad \forall p,c \mid (p,c) \in t \rightarrow \boxed{\text{number of possibilities}: N-t}$$

$$\Longrightarrow \boxed{\text{possible mappings}: (N-t)!}$$

با توجه به آنکه تعداد mappings های ممکن $(N-t)!$ می‌شود پس احتمال آنکه $E(k)$ و $E(k')$ به ازای تمامی $(p,c) \in N-t$ یکی باشند $\frac{1}{(N-t)!}$ می‌شود لذا

$$P(E_k = E_{k'} \quad \forall p,c \mid (p,c) \in \{N-t\}) = \frac{1}{(N-t)!} = \bar{P}^*$$

$$\longrightarrow P^* = P(E_k \neq E_{k'}) = 1 - \bar{P}^* = 1 - \frac{1}{(N-t)!}$$

$$\longrightarrow P^* = 1 - \frac{1}{(N-t)!}$$

---

b) این قسمت از سؤال را شبیه با سؤال سوم حل می‌کنیم:

$$P^*(N-t \text{ ، fixed point تا } t') = \binom{N-t}{t'} P(\text{No fixed point in } N-t-t')$$

$$P(\text{No fixed point in } N-t-t') = \sum_{k=0}^{N-t-t'} \frac{(-1)^k}{k!} \frac{(N-t-t')!}{(N-t)!} = \sum_{k=0}^{N-t-t'} (-1)^k \binom{n}{k} (n-k)!$$

$$\Longrightarrow P^* = \frac{(N-t)!}{t'!\,(N-t-t')!} * \left(\sum_{k=0}^{N-t-t'} \frac{(-1)^k}{k!} \right) * \frac{(N-t-t')!}{(N-t)!}$$

$$\Longrightarrow P^* = \frac{1}{t'!} * \sum_{k=0}^{N-t-t'} \frac{(-1)^k}{k!}$$

پاسخ سوال پنجم)

a] اثبات این بخش با توجه به اول بودن p و q بسیار ساده و به صورت زیر می باشد.

عامل های اول pq تنها p و q می باشد. (چون p و q اول هستند) و از طرفی تعداد اعداد طبیعی کوچکتر از pq برابر با $pq-1$ می باشد. از این تعداد $q-1$ تا مضرب p و $p-1$ تا مضرب q هستند که gcd آنها با pq برابر با یک نمی شود و یا به عبارت دیگر این اعداد نسبت به pq اول نیستند. لذا مجموعاً $(p-1)+(q-1)$ عدد اینگونه هستند و با توجه به اینکه pq دارای تنها دو عامل اول p و q بود پس بقیه اعداد کوچکتر از pq نسبت به pq اول می باشند

لذا داریم:

$$\varphi(pq) = \underbrace{(pq-1)}_{\text{تمامی اعداد طبیعی کوچکتر از } pq} - (p-1) - (q-1) = pq - p - q + 1 = (p-1)(q-1)$$

$$\Longrightarrow \varphi(pq) = (p-1)(q-1)$$

بخش b] ابتدا مساله را به صورت $a^{p-1} \overset{p}{\equiv} 1$ بازنویسی کرده و پس مجموعه باقیمانده‌های $\{ma \mid 1 \le m \le p-1, m \in \mathbb{N}\}$ نسبت به p را که به صورت $\{1, 2, 3, \dots, (p-1)\}$ می شود برای اثبات این بخش استفاده می کنیم به گونه‌ای که:

$$a^{p-1} \overset{p}{\equiv} 1 \quad \text{و} \quad \underbrace{\{a, 2a, 3a, \dots, (p-1)a\}}_{I} \overset{p}{\equiv} \underbrace{\{1, 2, 3, \dots, (p-1)\}}_{II}$$

با توجه به آنکه $a \perp p$ است هم از طریق استقرا و یا هم از طریق استدلال $\left.\begin{matrix} km \overset{p}{\equiv} kn \\ k \perp p \end{matrix}\right| m \overset{p}{\equiv} n$ می توانیم ادعا کنیم که در رابطه‌ی mod p برای مجموعه‌ی (I) و (II)، یک تناظر یک به یک بین عضو های این دو مجموعه نسبت به هم داریم یا به عبارت دیگر هیچ دو تا عضو در مجموعه I به یک عضو در مجموعه‌ی II نگاشت نمی شود.

ادامه b]

حال اعضای مجموعه I و نیز اعضای مجموعه II را در یکدیگر ضرب نموده و رابطه mod P آنها را به صورت زیر می نویسیم :

$$\{a, 2a, \dots, (P-1)a\} \overset{P}{\equiv} \{1, 2, 3, \dots, P-1\}$$

$$\Longrightarrow a \times 2a \times 3a \times \dots \times (P-1)a \overset{P}{\equiv} 1 \times 2 \times 3 \times \dots \times (P-1) \quad ①$$

$$\overset{①}{\Longrightarrow} a^{P-1}(P-1)! \overset{P}{\equiv} (P-1)!$$

از طرفی داریم : $(P-1)! \perp P$ لذا می توانیم با رابطه $\left.\begin{matrix} km \overset{P}{\equiv} kn \\ k \perp P \end{matrix}\right\} m \overset{P}{\equiv} n$ ، $(P-1)!$ را که نسبت به P $\perp$ است حذف کرده و نهایتاً به حکم اول برسیم

$$\left.\begin{matrix} a^{P-1}(P-1)! \overset{P}{\equiv} (P-1)! \\ (P-1)! \perp P \end{matrix}\right\} \Longrightarrow a^{P-1} \overset{P}{\equiv} P$$

بخش c] فرض : $a \perp P$ $(\gcd(a,P)=1)$ حکم : $a^n \overset{P}{\equiv} a^{n \bmod \varphi(P)}$

در ابتدا n را برحسب $\varphi(P)$ می نویسیم و از رابطه موجود در بخش b استفاده می کنیم لذا :

$$a^{\varphi(P)} \overset{P}{\equiv} 1 \quad , \quad n = m\varphi(P) + k \quad , \quad \text{از طرفی } a \perp P \Rightarrow (a)^k \overset{P}{\equiv} (a)^k$$

$$\left\{\begin{matrix} a^{\varphi(P)} \overset{P}{\equiv} 1 \\ a^k \overset{P}{\equiv} a^k \end{matrix}\right. \xrightarrow[*]{a \perp P} a^{\varphi(P)} a^k \overset{P}{\equiv} 1 * a^k \Longrightarrow a^{\varphi(P)+k} \overset{P}{\equiv} a^k$$

$$\Longrightarrow \left\{\begin{matrix} a^{\varphi(P)+k} \overset{P}{\equiv} a^k \\ a^{\varphi(P)} \overset{P}{\equiv} 1 \end{matrix}\right. \Longrightarrow \left\{\begin{matrix} a^{2\varphi(P)+k} \overset{P}{\equiv} a^k \\ a^{\varphi(P)} \overset{P}{\equiv} 1 \end{matrix}\right. \Longrightarrow \dots \Longrightarrow a^{m\varphi(P)+k} \overset{P}{\equiv} a^k$$

$$\Longrightarrow \left\{\begin{matrix} a^{m\varphi(P)+k} \overset{P}{\equiv} a^k \\ m\varphi(P) + k = n \\ k = n \bmod \varphi(P) \end{matrix}\right. \Longrightarrow a^n \overset{P}{\equiv} a^{n \bmod \varphi(P)}$$

بزرگترین کمکی که این روش به ما می‌کند سادگی محاسبات mod اعداد است

به عنوان مثال می‌خواهیم بدانیم $5^{900} \bmod 7$ چه می‌گردد که با این روش داریم:

$$5^{900} \overset{7}{\equiv} 5^{900 \bmod 6} \overset{7}{\equiv} 5^{0} \overset{7}{\equiv} 1$$

مشاهده می‌نمایید به چه سادگی این مسئله با اثباتی که داشتیم و البته شرط $\gcd(5,7)=1$ حل شد.

با تشکر

بدیعی