سؤال اول

تابع چکیده‌ساز H را در نظر بگیرید که طول خروجی آن ۱۱ بیت است. فرض کنید که

$$H(secret) = 01011000101$$

باشد. هدف این است که با انتخاب پیام‌های تصادفی و محاسبه چکیده آنها به پیامی برسیم که مقدار چکیده آن برابر H(secret) باشد. به چه تعداد باید تلاش کنیم که به احتمال ۵۰ درصد یک برخورد ایجاد شود.

فرض می‌کنیم که خروجی این تابع هش **یکنواخت** باشد یعنی احتمال اینکه خروجی هش برای پیامی برابر 01011000101 باشد برابر $p = 1/2^{11}$ باشد. احتمال اینکه در n بار آزمایش **حداقل** یک برخورد باشد را با روش متمم حل می‌کنیم:

$$1 - (1-p)^{n-1} = P(n)$$

$$P(n) \geq 0.5 \Rightarrow n{\sim}1420$$

سؤال دوم

اگر تابع چکیده‌ساز H برخوردتاب باشد، آیا لزوما تابع $H\big(H(x)\big)$ نیز برخوردتاب است.

فرض کنیم تابع $H(H(x))$ برخوردتاب نباشد یعنی می‌توان پیام‌های x و x' را یافت که:

$$x \neq x' \text{ and } H\big(H(x)\big) = H\big(H(x')\big)$$

در این صورت با تعریف $y_1 = H(x)$ و $y_2 = H(x')$ دو حالت رخ می‌دهد:

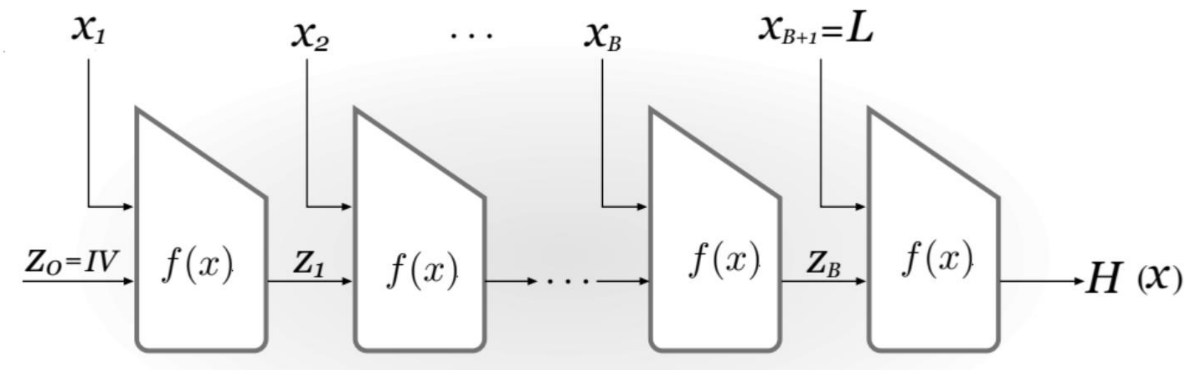
$$y_1 = y_2 \Rightarrow H(x) = H(x') \Rightarrow x \text{ and } x' \text{ are } a \text{ collision under } H$$

$$`y_1 \neq y_2 \Rightarrow y_1 \text{ and } y_2 \text{ are } a \text{ collision under } H$$

در هر دو حالت به تناقض می‌رسیم و در نتیجه فرض خلف باطل و حکم اثبات می‌شود.

سؤال سوم

در ساختار مرکل دامگارد زیر فرض کنید که بلوک آخر یعنی طول پیام حذف شود آیا می‌توان برای تابع چکیده‌ساز متناظر یک برخورد پیدا کرد.



با حذف بلوک طول (x_{B+1})، هر پیام و پد شده پیام دارای هش یکسان خواهند بود و یک برخورد رخ خواهد داد.

سؤال پنجم

برای m هایی که $gcd(m,n) \neq 1$ است، نشان دهید که رابطه رمز گشایی RSA درست است.

$$ed = k\phi(n) + 1$$

$$\phi(n) = (p-1)(q-1)$$

$$\gcd(m, n = pq) \neq 1 \Rightarrow p|m \vee q|m$$

بدون از دست دادن کلیت مسئله فرض می‌کنیم که $p|m$ و $q \nmid m$

$$m^e \bmod n = C \Rightarrow n|C - m^e \Rightarrow pq|C - m^e \Rightarrow p|C - m^e \wedge q|C - m^e$$

برای حالت $p|C - m^e$

$$m^e \bmod p = C \Rightarrow C \bmod p = m \bmod p = 0, \textbf{since } p|m$$

برای حالت $q|C - m^e$

$$m^e \bmod q = C$$

$$m^{ed} \bmod q = C^d \Rightarrow m^{k\phi(n)+1} \bmod q = m^{k\phi(n)} m \bmod q \Rightarrow m$$

$$\textbf{since } \gcd(m,q) = 1, m^{k\phi(n)} \bmod q \underbrace{\Rightarrow}_{Euler's\ theorem} m^{k(p-1)(q-1)} \bmod q = 1$$

در نتیجه داریم:

$$C^d \bmod p = 0 \bmod p = m$$

$$C^d \bmod q = m$$

در نتیجه

$$p|C^d - m \wedge\ q|C^d - m$$
$$\Rightarrow n|C^d - m \Rightarrow C^d \bmod n = m$$

به طور مشابه برای حالت $q|m$ هم می‌توان نوشت.