سوال ۱)

اسکار برای انجام حمله‌ی موفق باید مراحل زیر را انجام دهد:

- اسکار باید کلید عمومی باب (n, e) را با کلید عمومی خودش جایگزین کند. این کار را با دستکاری کانال ارتباطی انجام می‌دهد تا وقتی باب کلید عمومی خود را به آلیس می‌فرستد، در واقع کلید عمومی اسکار به آلیس ارسال شود.
- اسکار پیام‌هایی که باب به آلیس می‌فرستد را دریافت کرده و آن‌ها را تغییر می‌دهد. سپس پیام‌های تغییر یافته را با استفاده از کلید خصوصی خود امضا می‌کند.
- اسکار پیام‌های تغییر یافته و امضاهای جعلی خود را به آلیس ارسال می‌کند. از آنجا که آلیس فکر می‌کند که کلید عمومی اسکار در واقع کلید عمومی باب است، امضاهای جعلی اسکار را تأیید می‌کند.

آلیس پیام‌های دریافت شده را با استفاده از کلید عمومی اسکار (که فکر می‌کند کلید عمومی باب است) بررسی می‌کند و امضاهای جعلی را تأیید می‌کند. به این ترتیب، آلیس نمی‌تواند تشخیص دهد که پیام‌ها تغییر یافته‌اند و از صحت آن‌ها اطمینان حاصل می‌کند.

سوال ۲)

.۱

$$k_{pr} = (d) = (67) \quad , \quad k_{pub} = (p.\alpha.\beta) = (97, 23, 15)$$

$x = 17 , k_E = 31$ (a)

Signature Generation:

$$r \equiv \alpha^{k_E} \mod p \equiv 23^{31} \mod 97 \equiv 87$$

$$s \equiv (x - d \cdot r) \cdot {k_E}^{-1} \mod p - 1$$

$$\Rightarrow \quad s \equiv (17 - 67 \cdot 87) \cdot 31^{-1} \mod (97-1) \equiv (17 - 5829) \cdot 31 \quad \mod 96 \equiv 20$$

Signature Verification:

$$t \equiv \beta^r \cdot r^s \mod p \equiv 15^{87} \cdot 87^{20} \mod 97 \equiv 78 \cdot 73 \mod 97 \equiv 68$$

$$\alpha^x \mod p \equiv 23^{17} \mod 97 \equiv 68 \equiv t \Rightarrow valid\ signature$$

$x = 17 , k_E = 49$ (b)

Signature Generation:

$$r \equiv \alpha^{k_E} \mod p \equiv 23^{49} \mod 97 \equiv 74$$

$$s \equiv (x - d \cdot r) \cdot {k_E}^{-1} \mod p - 1$$

$$\Rightarrow \quad s \equiv (17 - 67 \cdot 74) \cdot 49^{-1} \mod (97-1) \equiv (17 - 4958) \cdot 49 \quad \mod 96 \equiv 3$$

Signature Verification:

$$t \equiv \beta^r \cdot r^s \quad mod\ p \equiv 15^{74} \cdot 74^3 \quad mod\ 97 \ \equiv 3 \cdot 55 \quad mod\ 97 \ \equiv 68$$

$$\alpha^x\ mod\ p \ \equiv \ 23^{17} \quad mod\ 97 \ \equiv 68 \equiv t \ \Rightarrow \ valid\ signature$$

$x = 85\ , k_E = 77$ (c)

Signature Generation:

$$r \equiv \alpha^{k_E} \ \ mod\ p \ \equiv 23^{77} \ \ mod\ 97 \ \equiv 84$$

$$s \equiv (x - d \cdot r) \cdot {k_E}^{-1} \ \ mod \ \ p - 1$$

$$\Rightarrow \ \ s \equiv (85 - 67 \cdot 84) \cdot 77^{-1} \quad mod\ (97 - 1) \ \equiv (85 - 5628) \cdot 5 \quad mod\ 96 \ \equiv 29$$

Signature Verification:

$$t \equiv \beta^r \cdot r^s \quad mod\ p \equiv 15^{84} \cdot 84^{29} \quad mod\ 97 \ \equiv 64 \cdot 21 \quad mod\ 97 \ \equiv 83$$

$$\alpha^x\ mod\ p \ \equiv \ 23^{85} \quad mod\ 97 \ \equiv 83 \equiv t \ \Rightarrow \ valid\ signature$$

.۲

$$(x_1, r_1, s_1) \ = \ (22, 37, 33)$$

$$t \equiv \beta^r \cdot r^s \quad mod\ p \equiv 15^{37} \cdot 37^{33} \quad mod\ 97 \ \equiv 10 \cdot 34 \quad mod\ 97 \ \equiv 49$$

$$\alpha^x\ mod\ p \ \equiv \ 23^{22}\ mod\ 97 \ \equiv 49 \equiv t \ \Rightarrow \ valid\ signature$$

$$(x_2, r_2, s_2) \ = \ (82, 13, 65)$$

$$t \equiv \beta^r \cdot r^s \quad mod\ p \equiv 15^{13} \cdot 13^{65} \quad mod\ 97 \ \equiv 26 \cdot \ 17 \quad mod\ 97 \ \equiv 54$$

$\alpha^x\ mod\ p \ \equiv \ 23^{82}\ mod\ 97 \ \equiv 32 \ \neq t \ \Rightarrow \ invalid\ signature \Rightarrow$ the message is not from Bob!

سوال ۳)

۱. $h(x) = 17, \ \ k_E = 25$

Signing Process (Bob):

$$r \equiv (\alpha^{k_E} \ \ mod\ p) \ \ mod\ q \ \ \equiv (3^{25} \ \ mod\ 59) \ \ mod\ 29 \equiv 51 \quad mod\ 29 \equiv 22$$

$$k_E^{-1} \ \ mod\ q \equiv 25^{-1} \ \ mod\ 29 \equiv 7$$

$$\Rightarrow \ \ s \equiv (h(x) + d \cdot r) k_E^{-1} \ \ mod\ q \equiv (17 + 23 \cdot 22) 7 \quad mod\ 29 \ \ \equiv 3661 \quad mod\ 29 \equiv 7$$

Signature Verification (Alice):

$$w \equiv s^{-1}\ mod\ q \equiv 7^{-1} \ \ mod\ 29 = 25$$

$$u_1 \equiv w \cdot h(x) \ \ mod\ q \equiv 25 \cdot 17 \ \ mod\ 29 \equiv 19$$

$$u_2 \equiv w \cdot r \ \ mod\ q \equiv 25 \cdot 22\ \ mod\ 29 \equiv 28$$

$$\beta \equiv \alpha^d \ \ mod\ p \equiv 3^{23} \ \ mod\ 59 \ \equiv 45$$

$$\Rightarrow v \equiv (\alpha^{u_1} \cdot \beta^{u_2} \ \ mod\ p)\ mod\ q \equiv (3^{19} \cdot 45^{28} \ \ mod\ 59)\ mod\ 29 \equiv 51\ \ mod\ 29 \ \equiv 22$$

$$\Rightarrow v \equiv r \ \ mod\ q \equiv 22 \quad \Rightarrow \quad valid\ signature$$

۲. $h(x) = 2,\ \ k_E = 13$

Signing Process (Bob):

$$r \equiv (\alpha^{k_E} \ \ mod\ p)\ \ mod\ q \ \equiv (3^{13} \ \ mod\ 59)\ \ mod\ 29 \equiv 25 \ \ mod\ 29 \equiv 25$$

$$k_E^{-1} \ \ mod\ q \equiv 13^{-1} \ \ mod\ 29 \equiv 9$$

$$\Rightarrow \ s \equiv (h(x) + d \cdot r)k_E^{-1} \ \ mod\ q \equiv (2 + 23 \cdot 25)9 \ \ mod\ 29 \ \equiv 5193 \ \ mod\ 29 \equiv 2$$

Signature Verification (Alice):

$$w \equiv s^{-1}\ mod\ q \equiv 2^{-1} \ \ mod\ 29 = 15$$

$$u_1 \equiv w \cdot h(x) \ \ mod\ q \equiv 15 \cdot 2 \ \ mod\ 29 \equiv 1$$

$$u_2 \equiv w \cdot r \ \ mod\ q \equiv 15 \cdot 25 \ \ mod\ 29 \equiv 27$$

$$\beta \equiv \alpha^d \ \ mod\ p \equiv 3^{23} \ \ mod\ 59 \ \equiv 45$$

$$\Rightarrow v \equiv (\alpha^{u_1} \cdot \beta^{u_2} \ \ mod\ p)\ mod\ q \equiv (3^{1} \cdot 45^{27} \ \ mod\ 59)\ mod\ 29 \equiv 25\ \ mod\ 29 \ \equiv 25$$

$$\Rightarrow v \equiv r \ \ mod\ q \equiv 25 \quad \Rightarrow \quad valid\ signature$$

۳. $h(x) = 21,\ \ k_E = 8$

Signing Process (Bob):

$$r \equiv (\alpha^{k_E} \ \ mod\ p)\ \ mod\ q \ \equiv (3^{8} \ \ mod\ 59)\ \ mod\ 29 \equiv 12 \ \ mod\ 29 \equiv 12$$

$$k_E^{-1} \ \ mod\ q \equiv 8^{-1} \ \ mod\ 29 \equiv 11$$

$$\Rightarrow \ s \equiv (h(x) + d \cdot r)k_E^{-1} \ \ mod\ q \equiv (21 + 23 \cdot 12)11 \ \ mod\ 29 \ \equiv 3267 \ \ mod\ 29 \equiv 19$$

Signature Verification (Alice):

$$w \equiv s^{-1}\ mod\ q \equiv 19^{-1} \ \ mod\ 29 = 26$$

$$u_1 \equiv w \cdot h(x) \ \ mod\ q \equiv 26 \cdot 21 \ \ mod\ 29 \equiv 24$$

$$u_2 \equiv w \cdot r \ \ mod\ q \equiv 26 \cdot 12 \ \ mod\ 29 \equiv 22$$

$$\beta \equiv \alpha^d \ \ mod\ p \equiv 3^{23} \ \ mod\ 59 \ \equiv 45$$

$$\Rightarrow v \equiv (\alpha^{u_1} \cdot \beta^{u_2} \ \ mod\ p)\ mod\ q \equiv (3^{24} \cdot 45^{22} \ \ mod\ 59)\ mod\ 29 \equiv 12\ \ mod\ 29 \ \equiv 12$$

$$\Rightarrow v \equiv r \ \ mod\ q \equiv 12 \quad \Rightarrow \quad valid\ signature$$

سوال ۴)

.۱

$$P(at\ least\ one\ Collision) = 1 - P(no\ Collision) = 1 - \prod_{i=1}^{K}\left(1 - \frac{i-1}{N}\right) = 1 - \prod_{i=0}^{K-1}\left(1 - \frac{i}{N}\right)$$

$$\xRightarrow{1-x \approx e^{-x}} 1 - \prod_{i=1}^{K-1} e^{-\frac{i}{N}} = 1 - e^{-\frac{1+2+\cdots+(K-1)}{N}} = 1 - e^{-\frac{K(K-1)}{2N}}$$

.۲

$$t \approx \sqrt{2^{n+1} \cdot ln\left(\frac{1}{1-\varepsilon}\right)} \quad , \quad \varepsilon = 0.5$$

$$64\ bit: \quad t \approx \sqrt{2^{64+1} \cdot ln\left(\frac{1}{1-0.5}\right)} = 2^{32}\sqrt{2 \cdot ln(2)} = 2^{32} \times 1.18$$

$$128\ bit: \quad t \approx \sqrt{2^{128+1} \cdot ln\left(\frac{1}{1-0.5}\right)} = 2^{64}\sqrt{2 \cdot ln(2)} = 2^{64} \times 1.18$$

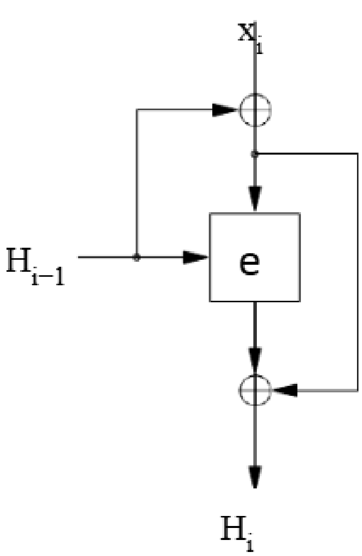
$$160\ bit: \quad t \approx \sqrt{2^{160+1} \cdot ln\left(\frac{1}{1-0.5}\right)} = 2^{80}\sqrt{2 \cdot ln(2)} = 2^{80} \times 1.18$$

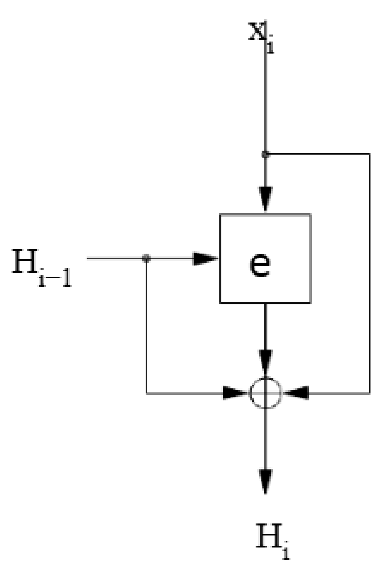
سوال ۵)

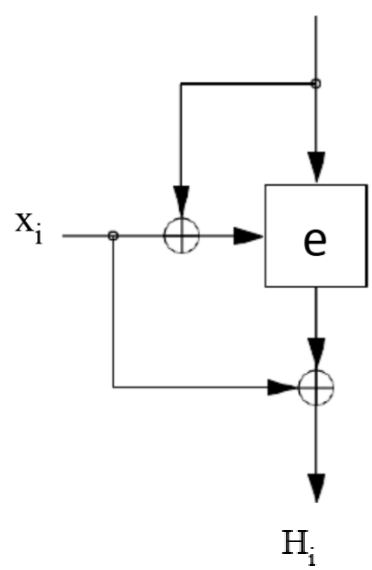
1: $e(H_{i-1}, x_i \oplus H_{i-1}) \oplus x_i \oplus H_{i-1}$

2: $e(H_{i-1}, x_i) \oplus x_i \oplus H_{i-1}$

3: $e(x_i \oplus H_{i-1}, H_{i-1}) \oplus x_i$







سوال ۶)

۱. مقدار y_i که نتیجه تابع $h(PW_i)$ است، از یک رمز بلوکی با طول بلوک ۶۴ بیت و کلید ۱۲۸ بیتی استفاده می‌کند. خروجی این رمز در تابع هش با ساختار Hirose به‌گونه‌ای طراحی شده که دو مقدار ۶۴ بیتی تولید کند و این دو مقدار کنار هم یک خروجی ۱۲۸ بیتی را تشکیل می‌دهند. بنابراین، هر مقدار y_i دارای طول ۱۲۸ بیت است.

۲.

اگر $\mathrm{c} = 0$، هر دو نیمه خروجی دقیقاً یک مقدار ۶۴ بیتی یکسان را تولید می‌کنند. این بدان معناست که خروجی y_u تنها دارای آنتروپی ۶۴ بیت است، نه ۱۲۸ بیت. شما به عنوان یک مهاجم می‌توانید مقادیر اولیه‌ای مثل $(H_{0,L}, H_{0,R})$ را همراه با یک مقدار شروع مانند ۶۴ صفر به تابع هش بدهید و به جستجوی مقادیر احتمالی برای x_i ادامه دهید. این کار با افزایش x_i به شما امکان می‌دهد خروجی‌های شبه‌تصادفی y تولید کنید. احتمال تولید دقیق y_u ممکن است کم باشد، اما فرآیند جستجوی تصادفی تنها حدود 2^{64} تلاش نیاز دارد.

۳. نوع حمله: (Second-preimage attack)

در اینجا، به دلیل کاهش آنتروپی به ۶۴ بیت (زمانی که $\mathrm{c} = 0$)، پیدا کردن Second-preimage بسیار ساده‌تر می‌شود زیرا فضای جستجو به شدت کوچک‌تر است.

۴.

هنگامی که $\mathrm{c} \neq 0$، هر نیمه از خروجی مقادیر کاملاً متفاوتی را تولید می‌کند. در نتیجه، آنتروپی خروجی برابر ۱۲۸ بیت باقی می‌ماند. این افزایش آنتروپی به این معنا است که تلاش برای جستجوی مقادیر هش با استفاده از حمله‌های رایج مانند Second-preimage attack نیاز به قدرت محاسباتی بسیار زیادی دارد و عملاً غیرعملی می‌شود.