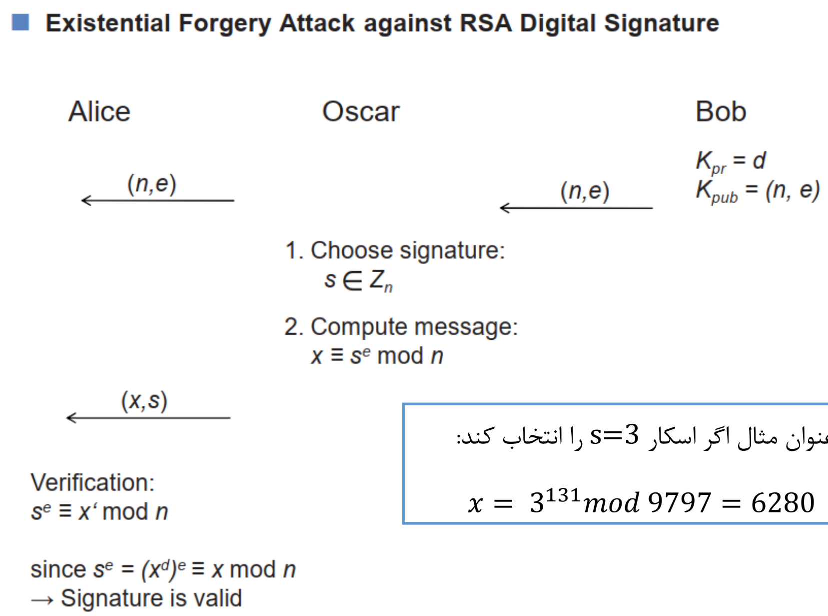
سوال ۱)

طبق اطلاعات مساله و امضای RSA: public key (n = 9797, e = 131)



به عنوان مثال اگر اسکار s=3 را انتخاب کند:

$$x = 3^{131} mod\ 9797 = 6280$$

$s^e\ mod\ 9797 = 3^{131} mod\ 9797 = 6280 = X'$
X = 6280 , X' = 6280 ⇒ X = X' valid signature

سوال ۲)

طبق مراحل زیر محاسبات لازم را انجام می‌دهیم.

Elgamal Signature Generation

1. Choose a random ephemeral key $k_E \in \{0,1,2,\ldots,p-2\}$ such that $\gcd(k_E, p-1) = 1$.
2. Compute the signature parameters:

$$r \equiv \alpha^{k_E} \bmod p,$$
$$s \equiv (x - d \cdot r) k_E^{-1} \bmod p-1.$$

Elgamal Signature Verification

1. Compute the value
$$t \equiv \beta^r \cdot r^s \bmod p$$
2. The verification follows from:

$$t \begin{cases} \equiv \alpha^x \bmod p & \Longrightarrow \text{valid signature} \\ \not\equiv \alpha^x \bmod p & \Longrightarrow \text{invalid signature} \end{cases}$$

۲.۱

$Kpr = (d) = (67)$

$Kpub = (p, \alpha, \beta) = (97, 23, 15)$

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

signature generation:

$r \equiv \alpha^{k_E} \, mod \, p$

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

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

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

signature verification:

$t \equiv \beta^{r} \cdot r^{s} \, mod \, p$

$t \equiv 15^{87} * 87^{20} \, mod\ 97 \ \equiv 78 * 73 \text{ mod } 97 \ \equiv 68$

$\alpha^{x} \, mod \, p \ \equiv \ 23^{17} \, mod\ 97 \ \equiv 68$

$t \ \equiv \ \ \alpha^{x} \, mod \, p \equiv 68 \Rightarrow$ the signature is valid

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

signature generation:

$r \equiv \alpha^{k_E} \, mod \, p$

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

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

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

signature verification:

$t \equiv \beta^{r} \cdot r^{s} \, mod \, p$

$t \equiv 15^{74} * 74^{3} \, mod\ 97 \ \equiv \ 3 * \ 55 \text{ mod } 97 \ \equiv \ 68$

$\alpha^{x} \, mod \, p \ \equiv \ 23^{17} \, mod\ 97 \ \equiv 68$

$t \ \equiv \ \ \alpha^{x} \, mod \, p \equiv 68 \Rightarrow$ the signature is valid

(c) $x = 85$ and $k_E = 77$

signature generation:

$r \equiv \alpha^{k_E} \bmod p$

$r \equiv 23^{77} \bmod 97 \equiv 84$

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

$s \equiv (85 - 67 * 84) * 77^{-1} \bmod 97 - 1 \equiv (85 - 5628) * 5 \bmod 96 \equiv 29$

signature verification:

$t \equiv \beta^r \cdot r^s \bmod p$

$t \equiv 15^{84} * 84^{29} \bmod 97 \equiv 64 * 21 \bmod 97 \equiv 83$

$\alpha^x \bmod p \equiv 23^{85} \bmod 97 \equiv 83$

$t \equiv \alpha^x \bmod p \equiv 83 \Rightarrow$ the signature is valid

۲.۲

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

$t \equiv \beta^r \cdot r^s \bmod p$

$t \equiv 15^{37} * 37^{33} \bmod 97 \equiv 10 * 34 \bmod 97 \equiv 49$

$\alpha^x \bmod p \equiv 23^{22} \bmod 97 \equiv 49$

$t \equiv \alpha^x \bmod p \equiv 49 \Rightarrow$ the signature is valid

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

$t \equiv \beta^r \cdot r^s \bmod p$

$t \equiv 15^{13} * 13^{65} \bmod 97 \equiv 26 * 17 \bmod 97 \equiv 54$

$\alpha^x \bmod p \equiv 23^{82} \bmod 97 \equiv 32$

$t \mathrel{!=} \alpha^x \bmod p \Rightarrow$ the signature is not valid $\Rightarrow$ the message is not from Bob!

سوال ۳)

مهاجم از معادلات زیر استفاده کرده و برای x_1 ، x_2 ، s_1 و s_2 شناخته شده ابتدا کلید موقت k_E و سپس کلید خصوصی d را بدست می‌آورد.

$$s_1 \equiv (SHA(x_1) + dr)k_E^{-1} \ \ mod\ q$$

$$s_2 \equiv (SHA(x_2) + dr)k_E^{-1} \ \ mod\ q$$

$$s_1 - s_2 \equiv k_E^{-1}\big(SHA(x_1) - SHA(x_2)\big) \ \ mod\ q$$

$$\Rightarrow \ k_E = \frac{SHA(x_1) - SHA(x_2)}{s_1 - s_2} \quad mod\ q$$

$$\Rightarrow d = \frac{s_1 \cdot k_E - SHA(x_1)}{r} \quad mod\ q$$

سوال ۴)

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

۴	۴.۱	۴.۲
$length$	$\varepsilon = 0.5$	$\varepsilon = 0.1$
$64\ bit$	$\approx \sqrt{2^{64+1} \cdot \ln\left(\frac{1}{1-0.5}\right)}$ $= 2^{32}\sqrt{2 \cdot \ln(2)}$ $= 2^{32} \times 1.18$	$\approx \sqrt{2^{64+1} \cdot \ln\left(\frac{1}{1-0.1}\right)}$ $= 2^{32}\sqrt{2 \cdot \ln(10/9)}$ $= 2^{32} \times 0.46$
$128\ bit$	$\approx \sqrt{2^{128+1} \cdot \ln\left(\frac{1}{1-0.5}\right)}$ $= 2^{64}\sqrt{2 \cdot \ln(2)}$ $= 2^{64} \times 1.18$	$\approx \sqrt{2^{128+1} \cdot \ln\left(\frac{1}{1-0.1}\right)}$ $= 2^{64}\sqrt{2 \cdot \ln(10/9)}$ $= 2^{64} \times 0.46$
$160\ bit$	$\approx \sqrt{2^{160+1} \cdot \ln\left(\frac{1}{1-0.5}\right)}$ $= 2^{80}\sqrt{2 \cdot \ln(2)}$ $= 2^{80} \times 1.18$	$\approx \sqrt{2^{160+1} \cdot \ln\left(\frac{1}{1-0.1}\right)}$ $= 2^{80}\sqrt{2 \cdot \ln(10/9)}$ $= 2^{80} \times 0.46$

سوال ۵)

۵.۱

$$P(at\ least\ one\ Collision) = 1 - P(no\ Collision) =$$

$$1 - \prod_{i=1}^{n}\left(1 - \frac{i-1}{365}\right) \geq \frac{1}{2} \Rightarrow \prod_{i=1}^{n}\left(1 - \frac{i-1}{365}\right) \leq \frac{1}{2} \Rightarrow n = 23$$

$$\Rightarrow \prod_{i=1}^{23}\left(1 - \frac{i-1}{365}\right) = 0.49 \leq \frac{1}{2} \qquad \Rightarrow n \geq 23$$

بنابراین باید حداقل ۲۳ نفر در یک کلاس وجود داشته باشند، تا حداقل دو دانش‌آموز با احتمال بیش‌تر از 0.5 تاریخ تولد یکسانی داشته باشند.

۵.۲

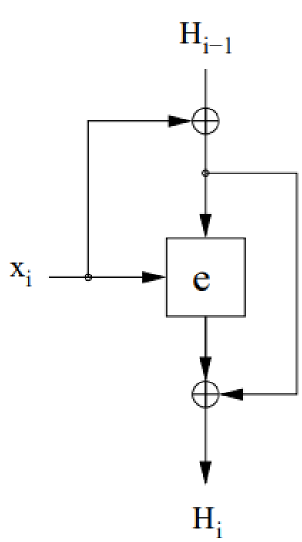
$$P(at\ least\ one\ Collision) = 1 - P(no\ Collision)$$

$$= 1 - \prod_{i=1}^{K}\left(1 - \frac{i-1}{N}\right) = 1 - \prod_{i=0}^{K-1}\left(1 - \frac{i}{N}\right)$$

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

سوال ۶)

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



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