مهیار عنصری ۹۶۳۲۰۹۳

سوال اول: $x \equiv b \bmod m_2$ و $x \equiv a \bmod m_1$ و m_1 و m_2 نسبت به هم اول

اگر فرض کنیم X_1 و X_2 دو جواب سیستم فوق باشند داریم:

$$\begin{cases} X_1 \equiv X_2 \equiv a \bmod m_1 \\ X_1 \equiv X_2 \equiv b \bmod m_2 \end{cases} \Longrightarrow \begin{cases} m_1 \mid (X_1 - X_2) \\ m_2 \mid (X_1 - X_2) \end{cases}$$

همچنین می توانیم طبق قواعد عاد کردن داریم:

$$[m_1 , m_2] \mid (X_1 - X_2)$$

m_1 و m_2 نسبت به هم اول $\Longrightarrow [m_1 , m_2] = m_1 m_2 \Longrightarrow m_1 m_2 \mid (X_1 - X_2)$

$$\Longrightarrow X_1 \equiv X_2 \bmod (m_1 m_2)$$

Scanned by CamScanner

سوال دوم $a^p \equiv a \mod p$

برای اثبات از استقرا کمک می‌گیریم:

حالت اولیه: $1^p \equiv 1 \mod p$

فرض استقرا: $a^p \equiv a \mod p$

حکم استقرا: $(a+1)^p \equiv a+1 \mod p$

می‌دانیم:

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a + 1$$

همچنین می‌دانیم $\binom{p}{n} = \frac{p!}{n!\,(n-p)!}$ پس به جز جمله اول و آخر در سایر جملات، ضریب خود مضربی از p است و در پیمانه p صفر می‌شود و خواهیم داشت:

$$(a+1)^p \equiv a^p + 1 \mod p$$

از طرفی فرض کردیم در استقرا که $a^p \equiv a \mod p$ پس داریم:

$$a^p \equiv a \mod p \Longrightarrow a^p + 1 \equiv a+1 \mod p \Longrightarrow (a+1)^p \equiv a+1 \mod p$$

حکم استقرا ثابت شد و بنابراین برای هر عدد مثبت a و عدد اول p داریم:

$$\boxed{a^p \equiv a \mod p}$$

Scanned by CamScanner

همان طور که در بخش قبل گفتیم، به جز جملات اول و آخر بسط دو جمله ای، سایر ضرایب بر P بخش‌پذیر هستند و در پیمانه P صفر می‌شوند. حال داریم:

$$(x+y)^P = \sum_{K=0}^{P} x^{P-K} y^K \equiv \binom{P}{P} x^{P-P} y^P + \binom{P}{0} x^{P-0} y^0 \mod P$$

$$\equiv 1 \times y^P + 1 \times x^P \pmod P \equiv y^P + x^P \mod P$$

$$\Longrightarrow \boxed{(x+y)^P \equiv x^P + y^P \mod P}$$

سوال سوم

اگر کلید خصوصی یکی از دو مقدار 1 و P-1 کلید عمومی حاصل از رابطه زیر باشد: $K_{pub} = \alpha^d \mod P$ باشد، نتیجه یک عدد ثابت است و حمله کننده می‌تواند به راحتی به کلید خصوصی دسترسی پیدا کند:

$$\alpha^1 \mod P \equiv \alpha \mod P$$

$$\alpha^{P-1} \mod P \equiv 1 \mod P$$

(Fermut's little Theorem)

Scanned by CamScanner

سوال چهارم: بخش اول:

$P = ۴۶۷$ و $\alpha = ۲$ و $a = ۲۲۸$ و $b = ۵۷$

$K_{Pub,a} = \alpha^{a} \bmod P \Longrightarrow K_{Pub,a} = ۲^{۲۲۸} \bmod ۴۶۷$

$۲۲۸ = (۱۱۱۰۰۰۱۰۰)_{۲}$

برای محاسبه از روش Square and multiply کمک می‌گیریم:

$۱ \times ۲ \bmod ۴۶۷ \longrightarrow ۲^{۲} \times ۲ \bmod ۴۶۷ \longrightarrow ۸^{۲} \times ۲ \bmod ۴۶۷ \longrightarrow$

$۱۲۸^{۲} \equiv ۳۹ \bmod ۴۶۷ \longrightarrow ۳۹^{۲} \equiv ۱۲۰ \bmod ۴۶۷ \longrightarrow ۱۲۰^{۲} \times ۲ \equiv ۳۱۳ \bmod ۴۶۷$

$\longrightarrow ۳۱۳^{۲} \equiv ۳۶۶ \bmod ۴۶۷ \longrightarrow ۳۶۶^{۲} \equiv ۳۹۴ \bmod ۴۶۷ = K_{Pub,a}$

$K_{Pub,b} = ۲^{۵۷} \bmod ۴۶۷ \longrightarrow ۵۷ = (۱۱۱۰۰۱)_{۲}$

$\longrightarrow ۱ \times ۲ \bmod ۴۶۷ \longrightarrow ۲^{۲} \times ۲ \bmod ۴۶۷ \longrightarrow ۸^{۲} \times ۲ \bmod ۴۶۷ \longrightarrow$

$۱۲۸^{۲} \equiv ۳۹ \bmod ۴۶۷ \longrightarrow ۳۹^{۲} \equiv ۱۲۰ \bmod ۴۶۷ \longrightarrow ۱۲۰^{۲} \equiv ۳۱۳ \bmod ۴۶۷$

$K_{Pub,b}$

$K_{AB} = K_{BA} = (K_{Pub,a})^{b} \bmod P = ۳۹۴^{۵۷} \bmod ۴۶۷ \equiv ۲۰۶$

برای انجام محاسبات از سایت dcode.fr بخش modular exponentiation کمک گرفتم.

در سوالات این تمرین

Scanned by CamScanner

سوال چهارم : بخش دوم :

$p = ۴۶۷$ و $q = ۴$ و $a = ۴۰۰$ و $b = ۱۳۴$

برای محاسبه K_{AB} یا K_{BA} نیاز به دانستن $K_{Pub,a}$ یا $K_{Pub,b}$ است زیرا:

$$K_{AB} = (K_{Pub,a})^b \bmod p \equiv (K_{Pub,b})^a \bmod p$$

$$K_{Pub,b} = \alpha^b \bmod p \equiv ۴^{۱۳۴} \bmod ۴۶۷ \equiv ۵۱ \bmod ۴۶۷$$

$$\rightarrow K_{AB} = ۵۱^{۴۰۰} \bmod p \equiv ۵۱^{۴۰۰} \bmod ۴۶۷ \equiv ۱۶۱ \bmod ۴۶۷$$

سوال پنجم

$\phi(11) = 11^1 - 11^0 = 10 = 2 \times 5 \longrightarrow$ توان ها $= \left(\frac{10}{5} = 2 \text{ و } \frac{10}{2} = 5\right)$

$2^2 \equiv 4 \bmod 11$

$2^5 \equiv 10 \bmod 11 \equiv -1 \bmod 11$ $\Longrightarrow$ ۲ برای ۱۱ یک Primitive root است.

چون 4^5 و 5^5 و 9^5 و 10^2 همگی در پیمانه ۱۱ برابر ۱ می‌شوند پس ۲ و ۶ و ۷ و ۸ برای ۱۱ Primitive root محسوب می‌شوند.

$\phi(11)^2 = 11^2 - 11 = 121 - 11 = 110 = 2 \times 5 \times 11 \longrightarrow$ توان ها $= \left(\frac{110}{2} = 55 \text{ و } \frac{110}{5} = 22 \text{ و } \frac{110}{11} = 10\right)$

$2^{55} \equiv 120 \equiv -1 \bmod 121$

$2^{22} \equiv 81 \bmod 121$ $\Longrightarrow$ ۲ یک Primitive root است.

$2^{10} \equiv 56 \bmod 121$

Scanned by CamScanner

$۳^{۵۵} \equiv ۱ \mod ۱۲۱$ ⟶ ۳ یک Primitive root نیست

$۷^{۵۵} \equiv ۱۲۰ \equiv -۱ \mod ۱۲۱$

$۷^{۲۲} \equiv ۲۷ \mod ۱۲۱$ ⟹ ۷ یک Primitive root است

$۷^{۱۰} \equiv ۲۳ \mod ۱۲۱$

$\phi(۲\times ۱۱^{۲}) = (۱۱^{۲}-۱۱)(۲-۱) = ۱۱۰$ ⟶ توان ها $= \left(\frac{۲۲۰}{۲} = ۱۱۰ ,\ \frac{۲۲۰}{۵} = ۴۴ ,\ \frac{۲۲۰}{۱۱} = ۲۰\right)$

$۲^{۱۱۰} \equiv ۱۲۲ \mod ۲۴۲$

$۲^{۴۴} \equiv ۱۴۸ \mod ۲۴۲$ ⟹ ۲ یک Primitive root است.

$۲^{۲۰} \equiv ۲۳۲ \mod ۲۴۲$

$۷^{۱۱۰} \equiv ۱ \mod ۲۴۲$ ⟹ ۷ یک Primitive root نیست

$۵^{۱۱۰} \equiv ۱ \mod ۲۴۲$ ⟹ 〃 〃 〃 〃 ۵

برای $۱۱^{۱۰۰}$ باید ϕ آن را حساب کنیم و فاکتورهای آن را به دست آوریم و $۱۱^{۱۰۰}$ را بر آن ها تقسیم کنیم تا توان ها به دست بیایند. آن گاه هر عدد کوچکتر از $۱۱^{۱۰۰}$ که به توان این توان ها برسد و در این پیمانه $۱۱^{۱۰۰}$ برابر ۱ شود یک Primitive root می باشد.

می توانیم بگوییم چون ۲ برای $۱۱^{۲}$ یک Primitive root است پس برای همه توان های ۱۱ یک Primitive root می باشد. (ایضاً ۷)

Scanned by CamScanner

سوال ششم:

$$b = a^{d} \bmod p \equiv ۷^{۲۲۱۰۵} \bmod ۴۴۹۲۷ \equiv ۴۰۹۰۹ \bmod ۴۴۹۲۷$$

$$\Longrightarrow K_{Pub,BoB} = (۴۴۹۲۷, ۷, ۴۰۹۰۹)$$

یک K به دلخواه از اعداد $۲ \leq K \leq P-۲$ انتخاب می‌کنیم:

با rand ماشین حساب $\rightarrow ۲۷۴۸ = K$

$$\Longrightarrow r = a^{K} = ۷^{۲۷۴۸} \equiv ۹۴۳۹ \bmod ۴۴۹۲۷$$

$$t = b^{K} m = \left((۴۰۹۰۹)^{۲۷۴۸} \times ۱۰۱۰۱\right) \bmod ۴۴۹۲۷ \equiv ۱۳۱۲۲ \times ۱۰۱۰۱ \bmod p$$

$$= (۱۳۲۵۴۵۳۲۲) \bmod (۴۴۹۲۷) \equiv ۱۰۶۷۲ \bmod ۴۴۹۲۷$$

$$\Longrightarrow (r, t) = (۹۴۳۹, ۱۰۶۷۲)$$

برای رمزگشایی،

$$r^{-d} \equiv Z \bmod p \quad , \quad Z \times t \equiv f \bmod p$$

$$(۹۴۳۹)^{-1} \equiv ۲۷۹۱۱ \bmod ۴۴۹۲۷ = Z$$

$$\Longrightarrow (۲۷۹۱۱ \times ۱۰۶۷۲) \bmod ۴۴۹۲۷ \equiv ۴۶۹,۶۳۲,۰۳۲ \bmod ۴۴۹۲۷$$

$$\equiv ۱۰۱۰۱ \bmod ۴۴۹۲۷$$

Scanned by CamScanner

سوال اختیاری:

ابتدا فرض می کنیم که می توانیم الگوریتم ElGamal با پارامترهای (p, a, b, r, t) را رمزگشایی کنیم و می خواهیم الگوریتم Diffie-Hellman را که به حزم $g^{xy} \bmod p$ است حل کنیم. در الگوریتم Diffie-Hellman داریم: $C_x = g^x \bmod p$, $C_y = g^y \bmod p$

اگر به الگوریتم ElGamal مقادیر زیر را بدهیم داریم:

$$a = g \ , \ b = C_x \ , \ r = C_y \ , \ t = 1$$

$$\Longrightarrow m = t \cdot r^{-\log_a b} \bmod p = (y^y)^{-\log_g g^x} \equiv g^{-xy} \bmod p$$

$$\Longrightarrow g^{xy} \equiv m^{-1} \bmod p$$

در حالت دیگر، اگر به الگوریتم Diffie-Hellman مقادیر زیر را بدهیم:

$$g = a \ , \ C_x = b \ , \ C_y = r$$

$$\Longrightarrow (C_x)^{\log_g C_y} = (b)^{\log_a r} \ , \ \log_a r = K = b^K$$

$$\Longrightarrow m = t \cdot b^{-K} \bmod p$$

Scanned by CamScanner