سوال ۱)

ابتدا پیام را Encrypt کرده و سپس با انجام Decryption صحت آن را بررسی می‌کنیم.

۱. $p = 7, q = 13, d = 5, x = 9$

$$n = p \cdot q \quad \Rightarrow \quad n = 7 \cdot 13 = 91$$

$$\varphi(n) = (p-1)(q-1) \; \Rightarrow \; \varphi(n) = (7-1)(13-1) = 6 \cdot 12 = 72$$

با توجه به این‌که مقدار $d = 5$ داده شده است، e باید در شرط زیر صدق کند؛ که با استفاده از الگوریتم اقلیدس تعمیم یافته، مقدار آن را بدست می‌آوریم.

$$e \cdot d \equiv 1 \left(mod\ \varphi(n)\right) \; \Rightarrow \; e \cdot 5 \equiv 1\ (mod\ 72) \; \Rightarrow \; e = d^{-1} = 29$$

$$\text{Encryption:} \qquad y \equiv x^e\ (mod\ n) = 9^{29}\ (mod\ 91) = 81$$

$$\text{Decryption:} \qquad x \equiv y^d\ (mod\ n) = 81^5\ (mod\ 91) = 9$$

۲. $p = 11, q = 13, e = 7, x = 4$

$$n = p \cdot q \quad \Rightarrow \quad n = 11 \cdot 13 = 143$$

$$\varphi(n) = (p-1)(q-1) \; \Rightarrow \; \varphi(n) = (11-1)(13-1) = 10 \cdot 12 = 120$$

با توجه به این‌که مقدار $e = 7$ داده شده است، d باید در شرط زیر صدق کند؛ که با استفاده از الگوریتم اقلیدس تعمیم یافته، مقدار آن را بدست می‌آوریم.

$$e \cdot d \equiv 1 \left(mod\ \varphi(n)\right) \; \Rightarrow \; 7 \cdot d \equiv 1\ (mod\ 120) \; \Rightarrow \; d = e^{-1} = 103$$

$$\text{Encryption:} \qquad y \equiv x^e\ (mod\ n) = 4^7\ (mod\ 143) = 82$$

$$\text{Decryption:} \qquad x \equiv y^d\ (mod\ n) = 82^{103}\ (mod\ 143) = 4$$

سوال ۲)

۱. $x = 5,\ e = 117,\ m = 113$

ابتدا عدد $e = 117$ را به صورت باینری می‌نویسیم: $e = 1110101$

$$Bit = 1 \; \Rightarrow \; \text{Square \& Multiply} \; \Rightarrow \; x^0 \cdot x = x^{1_2} \; \Rightarrow 1 \cdot 5 = 5$$

$$Bit = 1 \; \Rightarrow \; \text{Square \& Multiply} \; \Rightarrow \; (x^{1_2})^2 \cdot x = x^{11_2} \; \Rightarrow 5^2 \cdot 5 \equiv 12\ \ mod\ 113$$

$$Bit = 1 \; \Rightarrow \; \text{Square \& Multiply} \; \Rightarrow \; (x^{11_2})^2 \cdot x = x^{111_2} \; \Rightarrow 12^2 \cdot 5 \equiv 42\ \ mod\ 113$$

$$Bit = 0 \; \Rightarrow \; \text{Square} \; \Rightarrow \; (x^{111_2})^2 = x^{1110_2} \; \Rightarrow 42^2 \equiv 69\ \ mod\ 113$$

$$Bit = 1 \; \Rightarrow \; \text{Square \& Multiply} \; \Rightarrow \; (x^{1110_2})^2 \cdot x = x^{11101_2} \; \Rightarrow 69^2 \cdot 5 \equiv 75\ \ mod\ 113$$

$$Bit = 0 \; \Rightarrow \; \text{Square} \; \Rightarrow \; (x^{11101_2})^2 = x^{111010_2} \; \Rightarrow 75^2 \equiv 88\ \ mod\ 113$$

$Bit = 1 \Rightarrow \text{Square \& Multiply} \Rightarrow (x^{111010_2})^2 \cdot x = x^{1110101_2} \Rightarrow 88^2 \cdot 5 \equiv 74 \ mod\ 113$

بنابراین حاصل $5^{117} \equiv 74 \quad mod\ 113$ بدست می‌آید.

۲. $x = 7,\ e = 202,\ m = 123$

ابتدا عدد $e = 202$ را به صورت باینری می‌نویسیم: $e = 11001010$

$Bit = 1 \Rightarrow \text{Square \& Multiply} \Rightarrow x^0 \cdot x = x^{1_2} \Rightarrow 1 \cdot 7 = 7$

$Bit = 1 \Rightarrow \text{Square \& Multiply} \Rightarrow (x^{1_2})^2 \cdot x = x^{11_2} \Rightarrow 7^2 \cdot 7 \equiv 97 \ mod\ 123$

$Bit = 0 \Rightarrow \text{Square} \Rightarrow (x^{11_2})^2 = x^{110_2} \Rightarrow 97^2 \equiv 61 \ mod\ 123$

$Bit = 0 \Rightarrow \text{Square} \Rightarrow (x^{110_2})^2 = x^{1100_2} \Rightarrow 61^2 \equiv 31 \ mod\ 123$

$Bit = 1 \Rightarrow \text{Square \& Multiply} \Rightarrow (x^{1100_2})^2 \cdot x = x^{11001_2} \Rightarrow 31^2 \cdot 7 \equiv 85 \ mod\ 123$

$Bit = 0 \Rightarrow \text{Square} \Rightarrow (x^{11001_2})^2 = x^{110010_2} \Rightarrow 85^2 \equiv 91 \ mod\ 123$

$Bit = 1 \Rightarrow \text{Square \& Multiply} \Rightarrow (x^{110010_2})^2 \cdot x = x^{1100101_2} \Rightarrow 91^2 \cdot 7 \equiv 34 \ mod\ 123$

$Bit = 0 \Rightarrow \text{Square} \Rightarrow (x^{1100101_2})^2 = x^{11001010_2} \Rightarrow 34^2 \equiv 49 \ mod\ 123$

بنابراین حاصل $7^{202} \equiv 49 \quad mod\ 123$ بدست می‌آید.

سوال ۳)

.۱

$$\Phi(n) = (p-1)(q-1) = 42 \cdot 18 = 756$$

مقدار e باید به گونه‌ای انتخاب شود که $gcd(e, \Phi(n)) = 1$ باشد:

$$e_1 = 45 \Rightarrow gcd(45, 756) = 9 \quad \times$$

$$e_2 = 61 \Rightarrow gcd(61, 756) = 1$$

.۲

$$756 = 12 \cdot 61 + 24$$

$$61 = 2 \cdot 24 + 13$$

$$24 = 1 \cdot 13 + 11$$

$$13 = 1 \cdot 11 + 2$$

$$11 = 5 \cdot 2 + 1$$

$$\Rightarrow 1 = 11 - 5 \cdot 2 = 11 - 5(13 - 1 \cdot 11) = 6 \cdot 11 - 5 \cdot 13$$

$$= 6(24 - 1 \cdot 13) - 5 \cdot 13 = 6 \cdot 24 - 11 \cdot 13$$

$$= 6 \cdot 24 - 11(61 - 2 \cdot 24) = 28 \cdot 24 - 11 \cdot 61$$

$$= 28(756 - 12 \cdot 61) - 11 \cdot 61 = 28 \cdot 756 - 347 \cdot 61$$

$$\Rightarrow\ 61^{-1}\ mod\ 756 = -347 = 409$$

$$\Rightarrow\ k_{pr} = (p, q, d) = (43, 19, 409)$$

سوال ۴)

$$n = 31 \cdot 37 = 1147$$

$$\Phi(n) = (p-1)(q-1) = 30 \cdot 36 = 1080$$

$$\Rightarrow\ d = e^{-1}\ mod\ \Phi(n) = 17^{-1}\ \ mod\ 1080\ = 953$$

$$y_p = y\ \ mod\ p = 2\ \ mod\ 31 = 2$$

$$y_q = y\ \ mod\ q = 2\ \ mod\ 37 = 2$$

$$d_p = d\ \ mod\ (p-1) = 953\ \ mod\ 30 = 23$$

$$d_q = d\ \ mod\ (q-1) = 953\ \ mod\ 36 = 17$$

$$x_p = y_p^{d_p}\ \ mod\ p = 2^{23}\ mod\ 31 = 8$$

$$x_q = y_q^{d_q}\ \ mod\ q = 2^{17}\ mod\ 37 = 18$$

$$c_p = q^{-1}\ mod\ p = 37^{-1}\ mod\ 31 = 26$$

$$c_q = p^{-1}\ mod\ q = 31^{-1}\ mod\ 37 = 6$$

بنابراین مقدار متن اصلی (Plain text) برابر است با:

$$x = \left(q \cdot c_p \cdot x_p\right) + \left(p \cdot c_q \cdot x_q\right)\ mod\ n$$

$$\Rightarrow\ x = (37 \cdot 26 \cdot 8) + (31 \cdot 6 \cdot 18)\ \ mod\ 1147$$

$$= 8440\ \ mod\ 1147 = 721$$

سوال ۵)

.۱

توابع یک طرفه در رمزنگاری، توابعی هستند که محاسبه آن‌ها از ورودی به خروجی آسان است، اما محاسبه وارون آن‌ها بدون داشتن اطلاعات اضافی (مانند یک کلید خصوصی) عملاً غیرممکن است. این ویژگی باعث می‌شود که بتوان از این توابع برای ایجاد امنیت در سیستم‌های رمزنگاری استفاده کرد. به عنوان مثال، در الگوریتم‌های مبتنی بر فاکتورگیری، ضرب دو عدد اول بزرگ ساده است، اما فاکتورگیری عدد حاصل دشوار و زمان‌بر است.

.۲

الگوریتم‌های مبتنی بر لگاریتم گسسته بر اساس دشواری محاسبه لگاریتم گسسته در یک گروه خاص کار می‌کنند، در حالی که الگوریتم‌های مبتنی بر فاکتورگیری اعداد صحیح، به سختی فاکتورگیری یک عدد بزرگ متکی هستند. هر دو دسته از الگوریتم‌ها امنیت خود را از پیچیدگی و زمان‌بر بودن حل مسائل ریاضیاتی که مبنای آن‌هاست، تامین می‌کنند. به عنوان مثال، الگوریتم Diffie-Hellman از لگاریتم گسسته استفاده می‌کند، در حالی که RSA از فاکتورگیری اعداد صحیح بهره می‌گیرد.