Subject:

Year. Month. Date. ( )

٩٥٢٠٤١٣ علي حاتمي

سوال ١

a) $K^5 \bmod 10 = ?$

$10 = 2 \times 5 \Rightarrow \phi(10) = 4$

$p \quad q$

$5 = 1 \bmod 4$

$\Rightarrow K^5 \bmod 10 = K$ طبق قضیه

b) $pq = n \longrightarrow \phi(n) = (p-1)(q-1)$

$ed = a = 1 \bmod \phi(n) \Rightarrow m^{ed} = m^a \bmod n$

طبق قضیه $= m$

$\longrightarrow$ correct msgs

c) $n = p \longrightarrow \phi(n) = p-1$

$a = 1 \bmod p-1$

طبق قضیه $\Rightarrow m^a = m \bmod p$

e) $a = 1 \bmod \phi(n) \Rightarrow a = q\phi(n) + 1$

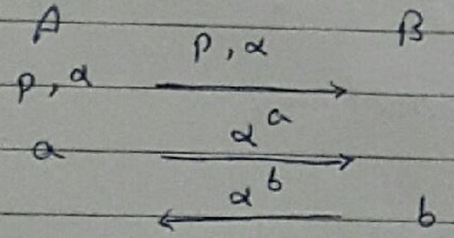
$m^a = m^{q\phi(n)+1} = m \times (m^{\phi(n)})^q \bmod n$

$= m \times 1^q = m \bmod n$

Puzzle

سوال ۲) اگر m با n فاکتور مشترک داشته باشند، در نتیجه n , m^e نیز همان فاکتور مشترک را خواهند داشت.

حال اگر m یک عدد اول باشد یا p است یا q و می‌توان با محاسبه‌ی $gcd(m^e, n)$ یکی از عوامل اول n را یافت و سپس با تقسیم این عامل، عامل بعدی n را می‌توان یافت و n را می‌توان تجزیه کرد و در نتیجه پس از تجزیه‌ی n می‌توان کلید خصوصی رمزنگاری را پیدا کرد.



سوال ۳) با توجه به شبه کد الگوریتم

اگر $a = 1$ باشد بنابراین $\alpha = \alpha^a$ می‌شود و .Adv به راحتی با مشاهده‌ی این حالت متوجه مقدار a که کلید خصوصی است می‌شود.

اگر $a = p-1$ باشد $\alpha^{p-1} = \alpha$ طبق فرما

و باز هم .Adv با مشاهده‌ی این حالت ($\alpha^a = \alpha$) می‌تواند a که کلید خصوصی است را حدس بزند.

Subject:

Year. Month. Date. ( )

سوال 4)

A $\xrightarrow{P, \alpha}$ B

$p = 467, \alpha = 2$

$d_A = 105, \alpha^{d_A} = 444 = \beta \xrightarrow{\alpha^d = \beta}$

$d_B = 213, \alpha^{d_B} = \gamma = 29$

$y = x \cdot \beta^{d_B} = 296$

در این مرحله رمزنگاری انجام شد

$(\gamma, y) \leftarrow$

$(29, 296)$

$y = 296$

$K = \gamma^{d_A} = 292$

$x = y \cdot K^{-1} = 33$

در این مرحله شکستن متن رمز شده انجام شد

سوال 5)

حاصل جواب سوال ۲۲۳۹۲ است.

سوال 6) مشاهده شد پس از تولید عددهای اولیه اقدام به تولید کلیدهای عمومی و خصوصی کرد و با استفاده از آن به شکل x^e ، y^d اقدام به رمزنگاری و شکستن رمز و نتیجه‌ی x^e نیز عدد نیری بود.