تکلیف چهارم

مهدی حق‌وردی

۸ تیر ۱۴۰۳

فهرست مطالب

۱ دیفی–هلمن سه نفره

One possible protocol could be the following:

1. A, B, C each generate their private keys x_A, x_B, x_C
2. A, B, C each calculate $y_A = g^{x_A}$, $y_B = g^{x_B}$, $y_C = g^{x_C}$
3. A sends y_A to B, B sends y_B to C, C sends y_C to A.

4. A calculates $z_{CA} = y_C^{x_A}$, B calculates $z_{AB} = y_A^{x_B}$, C calculates $z_{BC} = y_B^{x_C}$.
5. A sends z_{CA} to B, B sends z_{AB} to C, C sends z_{BC} to A.
6. A calculates $k_{BCA} = z_{BC}^{x_A}$, B calculates $k_{CAB} = z_{CA}^{x_B}$, C calculates $k_{ABC} = z_{AB}^{x_C}$.

The above equality means that the three parties now know a common secret $k_{ABC} = k_{CAB} = k_{BCA}$

۲ رمزنگاری بهینه در برقراری یک نشست (session)

۳ معکوس ضربی

Find $19^{-1} \mod 999$ using EEA.

- $999 \overset{999}{\equiv} 0 \times 19$
- $19 \overset{999}{\equiv} 1 \times 19$
- $11 = 999 - (52 \times 19) \overset{999}{\equiv} -52 \times 19$
- $8 = 19 - (1 \times 11) \overset{999}{\equiv} (1 \times 19) - (-52 \times 19) = 53 \times 19$
- $3 = 11 - (1 \times 8) \overset{999}{\equiv} (-52 \times 19) - (53 \times 19) = -105 \times 19$
- $2 = 8 - (2 \times 3) \overset{999}{\equiv} (53 \times 19) - (2 \times (-105 \times 19)) = 263 \times 19$
- $1 = 3 - (1 \times 2) \overset{999}{\equiv} (-105 \times 19) - (263 \times 19) = -368 \times 19$
- $\Rightarrow -368 \mod 999 = 631$ `<-- answer`
- checking the answer
  $19 \times 631 = 11989 \mod 999 = 1$

۴ در RSA

۱.۴ پیدا کردن d

$d = 17^{-1} \mod \Phi(3937)$

$\Phi(3937) = \Phi(31 \times 127) = 30 \times 126 = 3780$

$3780 \overset{3780}{\equiv} 0 \times 17$

$17 \overset{3780}{\equiv} 1 \times 17$

$6 = 3780 - (222 \times 17) \overset{3780}{\equiv} -222 \times 17$

$5 = 17 - (2 \times 6) \overset{3780}{\equiv} (1 \times 17) - (2 \times (-222 \times 17)) = 445 \times 17$

$1 = 6 - (1 \times 5) \overset{3780}{\equiv} (-222 \times 17) - (445 \times 17) = -667 \times 17$

$-667 \mod 3780 = 3113$ `<-- d`

check the answer

$17 \times 3113 = 52921 \mod 3780 = 1$

۲.۴ پیدا کردن n، d و $\Phi(n)$

$n = pq = 17 \times 23 = 391$ `<-- n`

$\Phi(n) = (p-1)(q-1) = 352$ `<-- Φ(n)`

$d = 3^{-1} \mod \Phi(n)$

$352 \overset{352}{\equiv} = 0 \times 3$

$3 \overset{352}{\equiv} = 1 \times 3$

$1 = 352 - (117 * 3) \overset{352}{\equiv} = -117 \times 3$

$-117 \mod 352 = 235$ `<-- d`

check the answer

$235 \times 3 = 705 \mod 352 = 1$

۳.۴ چرا e را عدد یک انتخاب نمی‌کنیم؟

برای اینکه در هر مجموعه‌ی Z_n^* عی، معکوس ۱ می‌شود ۰۱.

۴.۴ حمله‌ی chosen-ciphertext روی RSA

چون این فرد متن رمزشده ($c = 57$) و اطلاعات کلید عمومی (e و n) را دارد و در این مثال **مقدار n کوچک است** میتواند آن را تجزیه کند و سپس Φ را محاسبه کند و با مقادیر مختلف کلیدی که برای decryption انتخاب و آزمون و خطا می‌کند به p برسد.[1]

۵.۴ آیا کلید regenrate شده امن است؟

از نظر من جفت کلید جدید امن نیستند. به این دلیل که مهاجم اکنون از معادله‌ی $d = e^{-1} \mod \Phi(n)$ تنها یک مجهول دارد که (چون مطمئن نیستم روش ریاضی دارد یا خیر) می‌تواند با آزمون و خطا هم به فی دست پیدا کرده و از روی کلید عمومی جدید براحتی کلید خصوصی جدید را محاسبه کند.

۵ در Rabin

۱.۵ متن ۱۷ را رمز کنید

$m^2 \mod \Phi(n)$

$n = 47 \times 11 = 517$

$\Phi(n) = 46 \times 10 = 460$

$c = 17^2 \mod 460 = 289$ <-- ciphertext

۲.۵ با استفاده از Chinese remainder theorem چهار متن آشکار احتمالی را پیدا کنید

$$\sqrt{c} \mod n = \left[q \times (\pm c^{\frac{p+1}{4}}) \underbrace{(q^{-1} \mod p)}_{5}\right] + \left[p \times (\pm c^{\frac{q+1}{4}}) \underbrace{(p^{-1} \mod q)}_{4}\right]$$

1. $(11 \times 289^{12} \times 5) + (47 \times 289^3 \times 4)$
2. $(11 \times 289^{12} \times 5) + (47 \times -289^3 \times 4)$
3. $(11 \times -289^{12} \times 5) + (47 \times 289^3 \times 4)$
4. $(11 \times -289^{12} \times 5) + (47 \times -289^3 \times 4)$

۶ امنیت امضای دیجیتال RSA

امنیت این امضا در اینجاست که اگر مهاجم این‌ها را داشته باشد: $(m_i, S_i = m_i^d)$ اما با این رابطه مواجه می‌شود

$$d = \log_{m_i}^{S_i} \mod n$$

که این یک مسئله‌ی لوگاریتم گسسته است.

[1] https://www.geeksforgeeks.org/chosen-ciphertext-attacks-on-rsa/