دانشگاه تهران

پردیس دانشکده‌های فنی

دپارتمان مهندسی برق و کامپیوتر

امنیت شبکه پیشرفته

تمرین تحلیلی سری دوم

محمدحسین بدیعی

شماره دانشجویی 810199106

استاد : دکتر محمد صیاد حقیقی

پاییز 1400-1401

پاسخ سوال ۱]

مطابق با خواسته سوال اثبات می نماییم که امضا الجمال کار می کند.

$$S = (H(m) - xy)\, k^{-1} \bmod p-1 \quad \text{یا} \quad S \overset{P-1}{\equiv} (H(m) - xy)\, k^{-1}$$

با توجه به آنکه $\gcd(k, P-1) = 1$ است پس k^{-1} حتماً وجود است. حال با در نظر گرفتن عبارت فوق داریم:

$$Sk \overset{P-1}{\equiv} (H(m) - xy)\, k^{-1} * k$$

$$\Rightarrow Sk \overset{P-1}{\equiv} (H(m) - xy)$$

$$\Rightarrow H(m) \overset{P-1}{\equiv} Sk + xy \quad (I)$$

از طرفی با استفاده از تئوری فرمت در تمرین ۱ اثبات کردیم که:

$$\text{if } \gcd(a, P) = 1 \Rightarrow a^n \overset{P}{\equiv} a^{n \bmod \varphi(n)}$$

لذا با استفاده از رابطه فوق می توان گفت:

$$a^{H(m)} \overset{P}{\equiv} a^{H(m) \bmod \overbrace{P-1}^{\varphi(P)}} \quad (II)$$

با دانستن روابط (I) و (II) داریم:

$$a^{H(m)} \overset{P}{\equiv} a^{Sk + xy} \Rightarrow a^{H(m)} \overset{P}{\equiv} a^{xy}\, a^{sk} \Rightarrow a^{H(m)} \overset{P}{\equiv} \underbrace{(a^x)^y}_{d}\, \underbrace{(a^k)^s}_{y}$$

$$\Rightarrow \boxed{a^{H(m)} \overset{P}{\equiv} d^y\, y^s}$$

اثبات شد

پاسخ سوال ۲

در ابتدا ثابت می‌کنیم که $M^{ed} \overset{p}{\equiv} M$ و همچنین $M^{ed} \overset{q}{\equiv} M$.

اثبات $M^{ed} \overset{p}{\equiv} M$:

حالت اول ← $gcd(M,P) \neq 1$ $(M \not\perp P)$

$$\begin{cases} gcd(M,P) \neq 1 \\ P \text{ is Prime} \end{cases} \Longrightarrow M^{ed} \overset{P}{\equiv} 0 \overset{P}{\equiv} M \quad , \quad M = k'P$$

(با توجه به این)

$$\Rightarrow M^{ed} \overset{P}{\equiv} M$$

حالت دوم ← $gcd(M,P)=1$ $(M \perp P)$

$$\{gcd(M,P)=1 \Longrightarrow M^{\Phi(P)} \overset{P}{\equiv} 1 \Rightarrow M^{P-1} \overset{P}{\equiv} 1$$

$$\Rightarrow M^{ed} \overset{P}{\equiv} M$$

نتیجه ← $M^{ed} \overset{P}{\equiv} M$

به همین شیوه می‌توانیم استدلال کنیم که $M^{ed} \overset{q}{\equiv} M$.

$$\Rightarrow \begin{cases} M^{ed} \overset{P}{\equiv} M \\ M^{ed} \overset{q}{\equiv} M \end{cases}$$

حال مطابق با قضیه باقیمانده چینی با توجه به اینکه $gcd(P,q)=1$ و نیز روابط فوق اثبات می‌کنیم که $M^{ed} \overset{Pq}{\equiv} M$.

ادامه پاسخ سوال ۲)

حال با در نظر گرفتن تئوری باقی ماند چینی داریم:

$$\begin{cases} d_1 P \overset{q}{\equiv} 1 \Rightarrow d_1 P = k_1 q + 1 \overset{*P}{\Rightarrow} d_1 P^2 = k_1 Pq + P \Rightarrow d_1 P^2 \overset{Pq}{\equiv} P \\ d_2 q \equiv 1 \Rightarrow d_2 q = k_2 P + 1 \overset{*q}{\Rightarrow} d_2 q^2 = k_2 (Pq) + q \Rightarrow d_2 q^2 \overset{Pq}{\equiv} q \end{cases}$$

از طرفی طبق chinese Remainder theorem و نیز در نظر گرفتن d_1 و d_2 که در واقع P^{-1} و q^{-1} هستند داریم:

$$M^{ed} \overset{Pq}{\equiv} M P d_1 + M q d_2$$

$$\Rightarrow M^{ed} \overset{Pq}{\equiv} M (P d_1 + q d_2)$$

حال با فرض اینکه $P d_1 + q d_2 \overset{Pq}{\equiv} r$ می باشد، r را محاسبه می کنیم.

$$\Rightarrow \underbrace{P d_1 + q d_2}_{L} \overset{Pq}{\equiv} R \overset{L*(P+q)}{\Rightarrow} P^2 d_1 + Pq d_1 + q^2 d_2 + Pq d_2 \overset{Pq}{\equiv} q + P$$

$$\Rightarrow R(P+q) = P+q \Rightarrow \boxed{R = 1}$$

حال با توجه به اینکه $R=1$ که برابر از نتیجه گرفته شده از chinese remainder theorem بالا است مساله برد داریم:

$$\begin{cases} P d_1 + q d_2 \overset{Pq}{\equiv} 1 \\ M^{ed} \overset{Pq}{\equiv} M (P d_1 + q d_2) \end{cases} \Rightarrow \boxed{M^{ed} \overset{Pq}{\equiv} M}$$

پاسخ سوال ۳

a. false-accepts : در صورتیکه یک فرد غیر مجاز یا non-authorized توسط سرور به عنوان فرد مجاز شناخته شود و در این حالت خصوص این فرد غیر مجاز اجازه ورود به اتاق را از سرور بگیرد. لذا سرور دچار خطا شده و به این حالت false-accepts گویند

false-rejects : در صورتیکه یک فرد مجاز یا authorized توسط سرور به عنوان یک فرد غیرمجاز شناخته شود و در این حالت خصوص این فرد مجاز اجازه ورود از سرور را به اتاق را نگیرد و در واقع سرور این فرد مجاز را به عنوان یک فرد مجاز احراز هویت نکند به آن false-rejects گویند.

b. در این قسمت چون کاربر مجاز را به اشتباه بلاک کرده لذا احتمال همچین حالتی به این صورت محاسبه می‌شود که سرور ۵ بار خطای false-reject را مرتکب شده باشد:

$$P = \left(\frac{10}{100}\right)^5 = (0.1)^5 = 0.00001$$

احتمال این رخداد 0.001% است

c. حال احتمال اینکه یک invalid user دسترسی پیدا کند را بررسی می‌کنیم

$$P = \underbrace{\frac{0.5}{100}}_{\text{اجازه ورود در بار اول}} + \underbrace{\frac{99.5}{100}\times\frac{0.5}{100}}_{\text{اجازه ورود در بار دوم}} + \underbrace{\left(\frac{99.5}{100}\right)^2\times\frac{0.5}{100}}_{\text{اجازه ورود در بار سوم}} + \underbrace{\left(\frac{99.5}{100}\right)^3\times\frac{0.5}{100}}_{\text{اجازه ورود در بار چهارم}} + \underbrace{\left(\frac{99.5}{100}\right)^4\times\frac{0.5}{100}}_{\text{تلاش پنجم}}$$

$$\Rightarrow P \simeq 0.02475 \Rightarrow P \simeq 2.475\ \%$$

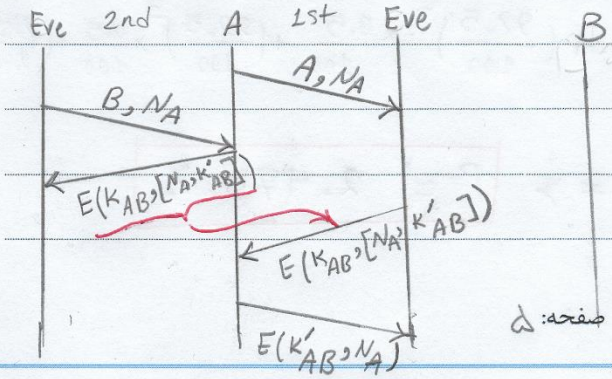
پاسخ سؤال ۴

a.

- A thinks he has shared k'_{AB} with B because B had sent A's Nonce with k'_{AB} encrypted by k_{AB} which is known by A & B
- B thinks he has shared k'_{AB} with A because A has sent A's Nonce encrypted by k'_{AB} which was decrypted only by who knew k_{AB} and cuz just A and B know this key for decryption so B is the only one except A who could decrypted the msg and retrived the key (k'_{AB})
- A thinks k'_{AB} is fresh because it placed in the msg with A's Nonce and the msg should be made after the A's Nonce had sent.
- B thinks k'_{AB} is fresh because → 1st reason is it choosed by himself (B)
  → and 2nd is A could send it back with a A's Nonce encrypted by k'_{AB}

b.

ابتدا حالت عکس را ترسیم می‌کنیم پس به ترتیب می‌پردازیم



ادامه در صفحه بعد

ادامه قسمت b سوال ۴]

چون Eve بدلیل نداشتن کلید مشترک K_{AB} نمی‌تواند پیام را تغییر دهد

در واقع به بیان دیگر می‌توانیم بگوییم:

همانطور که مشاهده می‌فرمایید Eve پس از ارتباط اول

که با A برقرار کرد، یک ارتباط دیگر برقرار کرده و

خود را جای B معرفی می‌کند و $E(K_{AB}, [N_A, K'_{AB}])$ را

از A دریافت کرده و همین را به عنوان پاسخ A

در ارتباط اول (با شکی تک) برمی‌گرداند لذا

با توجه به آنکه پیام $[N_A, K'_{AB}]$ با کلید K_{AB} رمز شده، A مطمئن می‌شود که طرف مقابل B بوده

در صورتیکه اینطور نیست و در واقع Eve replay attack زده است.

$A \rightarrow C : A, N_A$

$Eve \rightarrow A : B, N_A$

$A \rightarrow Eve : E(K_{AB}, [N_A, K'_{AB}])$

$Eve \rightarrow A : E(K_{AB}, [N_A, K'_{AB}])$

$A \rightarrow Eve : E(K'_{AB}, N_A)$

---

c. راه خوبی که به ذهن می‌رسد این است که فرستنده را در پیام رمز شده قرار دهیم بدینسان صورت

پاسخ A در ارتباط دوم به C، $E(K_{AB}, [A, N_A, K'_{AB}])$ خواهد بود و لذا C دیگر

(فرستنده)

امکان جایگذاری این پیام را ندارد چون A تشخیص می‌دهد که این پیام خودش بوده نه

در یک ارتباط دیگر ارسال کرده است.

پاسخ سوال a]

a.

در این پروتکل A نیاز درخواست به سرور (یا کلاینت) B می‌باشد به سرور KDC مراجعه کند.

1. یوزر A، ID خود را به همراه ID کلاینت B که تقصد برقراری یک session با او را دارد و به همراه یک Nonce با علامت N_1 به سرور KDC می‌دهد.

2. KDC در پاسخ، یک کلید session (K_S) نیاز کلید مشترک بین A و B و نیز ID_B و Nonce دریافتی را به همراه یک تیکت که با کلید B رمز شده است (K_b) ترکیب کرده و کل پیام را با کلید A رمز می‌کند تا تنها یوزر A بتواند آن را باز کند و نهایتاً این پیام رمز شده را به A ارسال می‌کند.

3. یوزر A با دریافت این پیام آن را با کلید خود (K_a) باز می‌کند و چون N_1 را مشاهده می‌نماید، متوجه تازه بودن پیام می‌شود. پس کلید session را نیاز خود نگهداشته و تیکت $E(K_b, [K_S \| ID_A])$ را به B ارسال می‌کند. توجه کنید که یوزر A قادر به خواندن یا تغییر محتوای تیکت نیست چون این تیکت با کلید B رمز شده است.

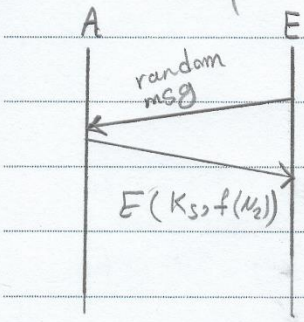
4. B با دریافت تیکت، آن را با کلید خود (K_b) باز می‌کند و کلید session (K_S) و نیز ID_A که قرار است با آن ارتباط برقرار کند را نگه می‌دارد. حال نیاز اطمینان از اینکه یوزر A کلید session را دارد، یک Nonce جدید را با این کلید رمز می‌کند تا یوزر A می‌تواند Nonce را استخراج کند. لذا این پیام را به یوزر A می‌فرستد.

5. یوزر A با دریافت پیام، چون کلید K_S را قبلاً از KDS گرفته بود اقدام به بازگشایی پیام می‌کند و Nonce ارسالی را شناسایی کرده و به جهت آنکه به B بگوید که من K_S را دارم، تابعی از این Nonce را با کلید جلسه (K_S) رمز کرده و به B ارسال می‌کند.

در نهایت B با باز کردن پیام متوجه می‌شود که A، K_S را داشته که توانسته تابعی از Nonce را با این کلید رمز کند و بدرستی

b.5

مشکل این پروتکل این است که B خود را به A authenticate نکرده است و تنها A است که خود را با ارسال $f(N_2)$ به B authenticate یا همان احراز هویت می‌کند.



لذا در مرحله ۴ ام Eve می‌تواند هر چیزی که می‌خواهد را به A بفرستد و در مقابل A پاسخ آن را با $f(N_2)$ بدهد و خود را احراز هویت کند.

c.5 راهکاری که به نظرم می‌تواند پاسخگو باشد این است که در مرحله سوم یک Nonce مثلاً $f(N')$ به B ارسال شود. بدین صورت در مرحله چهارم با ارسال پیامی که $f(N')$ نیز جزئی از آن است، B خود را به A، احراز هویت یا authenticate می‌نماید.

3. $A \rightarrow B: \quad E(K_s, N'), \overbrace{E(K_b, [K_s \| ID_A])}^{\text{تیکت}}$

4. $B \rightarrow A: \quad E(K_s, N_2, N')$

پاسخ سوال ۶

ابتدا اشکال موجود در پروتکل را مطرح می‌کنیم و پس از آن قسمت حل دیگر می‌رویم. مشکل اصلی این است که در مرحله آخر، A از fresh بودن پیام اطلاعی ندارد (اگرچه B می‌داند fresh است ولی A نمی‌داند) لذا Eve می‌تواند هر چند بار همین پیام را بفرستد.

★ ادامه در صفحه‌ی بعد ★

حال به سراغ idealize کردن پروتکل می‌رویم:

$$A \to B : \{N_a\}_{k_{ab}}$$

$$B \to A : \{N_a, N_b\}_{k_{ab}}$$

$$A \to B : \{N_b\}_{k_{ab}}$$

$$B \to A : \{A \overset{k'_{ab}}{\leftrightarrow} B, N'_b\}_{k_{ab}}$$

★ برای هدف $B \mid\equiv (A \overset{k'_{ab}}{\leftrightarrow} B)$ باید بگوییم که هم این هدف جز فرض‌های اولیه است و لذا حکم برقرار است و هم اینکه می‌دانیم کلید k'_{ab} را B کنترل می‌کند لذا وقتی خود B این کلید را کنترل می‌کند پس به $B \mid\equiv (A \overset{k'_{ab}}{\leftrightarrow} B)$ باور هم دارد. هرچند که فرض مسئله این را نگفته بود

★ حال هدف $A \mid\equiv (A \overset{k'_{ab}}{\leftrightarrow} B)$ را بررسی می‌کنیم.

$$\frac{A \mid\equiv (A \overset{k_{ab}}{\leftrightarrow} B) \quad , \quad A \lhd \{A \overset{k'_{ab}}{\leftrightarrow} B, N'_b\}_{k_{ab}}}{A \mid\equiv B \mid\sim (A \overset{k'_{ab}}{\leftrightarrow} B, N'_b)}$$

(آخرین مرحله)

توجه نمایید که N'_b عملاً هیچ نقشی را ایفا نمی‌کند لذا می‌توانیم بگوییم:

$$A \mid\equiv B \mid\sim (A \overset{k'_{ab}}{\leftrightarrow} B) \quad *$$

اما آیا پیام دیده‌شده دقیقاً این است که A به آن باور کند؟ خیر

ادامه در صفحه بعد

ادامه سوال ۶)

همانطور که فرض کردیم مشکل اصلی این است که A در مرحله آخر از نزد بدون پیام اطلاعی ندارد و لذا هدف $A \mid\equiv (A \overset{k'_{ab}}{\longleftrightarrow} B)$ به همین دلیل است که برآورده نمی‌شود.

* نتیجتاً بدلیل همین مشکل است که Eve می‌تواند هر چند بار این پیام را ارسال کند.

★ حال فرض کنید که در مرحله سوم A یک Nonce (N'_a) نیز ارسال کند. می‌خواهیم ببینیم با این فرض اضافه آیا می‌توانیم هدف فعلی را اثبات کنیم.

3. $A \longrightarrow B : \{N_b, N'_a\}_{k_{ab}}$

4. $B \longrightarrow A : \{A \overset{k'_{ab}}{\longleftrightarrow} B, N'_b, N'_a\}_{k_{ab}}$

توجه شود که N'_b اصلاً بکار نمی‌آید

حال ادامه اثبات را با این فرض بررسی می‌کنیم:

فرض $A \mid\equiv \#(N'_a)$

طبق تراکنش *

$$\frac{A \mid\equiv \#(A \overset{k'_{ab}}{\longleftrightarrow} B, N'_b, N'_a),\quad A \mid\equiv B \mid\sim (A \overset{k'_{ab}}{\longleftrightarrow} B), N'_a, N'_b}{A \mid\equiv \#(A \overset{k'_{ab}}{\longleftrightarrow} B, N'_a),\quad A \mid\equiv B \mid\sim (A \overset{k'_{ab}}{\longleftrightarrow} B, N'_a)}$$

$$\frac{A \mid\equiv B \mid\equiv ((A \overset{k'_{ab}}{\longleftrightarrow} B), N'_a)}{A \mid\equiv B \mid\equiv (A \overset{k'_{ab}}{\longleftrightarrow} B),\quad A \mid\equiv B \Rightarrow (A \overset{k'_{ab}}{\longleftrightarrow} B)}$$

B طلبی را می‌سازد (کنترل می‌کند)

$$A \mid\equiv A \overset{k'_{ab}}{\longleftrightarrow} B$$

لذا با در نظر گرفتن N'_a و رفع مشکل مسأله می‌توانیم به هدف دوم نیز برسیم.