به نام خدا

پاسخ تکلیف دوم مبانی رایانش امن

سوالات 1-5

سوال اول:

i) MicrosoftExchangeserver

ii) FakeNetflixapponPlayStorecaughthijackingWhatsAppsessions

iii)flag{cAesaR_CiPhErS_juST_aREnT_sEcUrE:)}

iv)flag{FakeNetflixapponPlayStorecaughthijackingWhatsAppsessions}

v) flag{this_homework_is_about_cryptography_and_key_management.}

- سه رشته کاراکتری آخر دارای حروف اسکی است و با توجه به الگوریتم سزار و وجود یک چرخش، پس باید از جدول اسکی استفاده شود و یک بازه مناسب را نیز انتخاب کرد تا به نتیجه درست رسید که با توجه به کاراکترهای استفاده شده که کاراکترهای چاپی هستند بازه [33,127) مناسب است.

- خیر همیشه بیشترین احتمال پاسخ مسئله نیست.

سوال دوم:

1. در کتاب و کلاس درس توضیح داده شده است.

2. ابتدا باید دنبال الگوهای تکراری باشیم و بررسی الگوهای طولانی، شانس موفقیت را افزایش میدهد چون احتمال تصادفی بودن کمتر میشود. بیشترین اشتراکی که بین این فاکتور ها وجود دارد می تواند طول کلید را دهد. با توجه به دو الگوی طولانی مشخص شده و نیز فاکتورهای مشترک، طول کلید 2، 3 و یا 6 حرفی است. چون بزرگترین عامل مشترک در این دو الگو 6 است پس احتمال 6 حرفی بودن کلید بیشتر است (در متن های

طولانی محاسبه IC تقریب خوبی را از طول کلید نشان میدهد). پس با همین فرض و با استفاده از ابزار آنلاین متن اصلی را بدست می آوریم که چون متن بدست آمده با معناست پس کلید 6 حرفی درست و عبارت نمایش داده شده می باشد.

(معمولا احتمال دو حرفی بودن کلید بسیار کم است.)

"Llglv eji ouec jicmfrk xq vv hawcjgsarvyu efh ouec jicmfrk xq vv lgtgzlp.oi clv xzi qhvw olq xvgahg qyillgl ks ti jigixyn ii hawcjgsarvyu"

Letters	Start	End	Gap length	Factors of gap length
ouec jicmfrk xq vv	8	38	30	2,3,5
hawcjgsarvyu	23	101	78	2, 3, 13

Plaintext: There are many reasons to be disappointed and many reasons to be hopeful. we are the ones who decide whether to be hopeful or disappointed.

Key = sucure

سوال سوم:

1. در رمزهای نامتقارن کاربر فقط باید کلید خصوصی خود را حفظ کند و کلیدی که به افراد دیگر داده میشود کلید عمومی است که خود آشکار است. نوع متقارن کاربردهای وسیعی دارند. میتوان به استفاده از آن ها در احراز هویت یا تصدیق اصالت، اطمینان از صحت و عدم تغییر پیام ,integrity (authentication) و انتقال کلید رمزنگاری اشاره کرد.

2. در Certificate و با توجه به امضای شخص سوم مورد اعتماد، این اطمینان را میدهد که کلید عمومی حتما متعلق به identity مورد نظر است(bind) و اطلاعات صحت دارد.

3. Eavesdropping, Modification, Denial of Service, Replay, Man in the Middle, Certificate Manipulation,…

4. طول کلید در این الگوریتم باید حداقل برابر با طول پیام و کاملا تصادفی باشد. با توجه به آنکه تولید، انتقال و ذخیره کلید خود یک امر چالش انگیر است پس اگر پیام ها هم طولانی باشند ایجاد یک کلید کاملا رندوم در هر مرحله کار آسانی نیست و هم چنین محافظت از کلید و انتقال امن آن دشوار است واگر قرار بر انتقال کلید با همان طول متن به روش مطمئنی است خود متن را انتقال میدادیم.

سوال چهارم:

با توجه به روابط ریاضی در الگوریتم RSA، برای رسیدن به کلید خصوصی نیاز به تابع فی اویلر است و یکی از راه های بدست آوردن این تابع تجزیه n به عوامل اول یعنی p و q می باشد.

چون (n,e) کلید عمومی است و آشکار است پس n باید به گونه ای انتخاب شود که امکان شکست آن به عوامل اولش وجود نداشته باشد و عمل تجزیه برای آن سخت باشد. در این سوال طول کلید کوتاه است و براحتی با تجزیه آن به p و q میتوان تابع فی اویلر را بدست آورد و به کلید خصوصی و متن اصلی رسید (الگوریتم RSA با پیمانه 1024 بیتی، امنیتی در حد الگوریتم های متقارن با کلیدهای 87 بیتی دارد).

برای بدست آوردن عامل های اول n راه های مختلفی وجود دارد که یکی از آن ها استفاده از سایت factordb است.

- کد ضمیمه شده است.

Plaintext: flag{Isfahan_University_of_Technology}

سوال پنجم:

1. تازگی کلید (کلید جلسه در اجرای کنونی پروتکل تولید شده باشد و قدیمی نباشد)،

تصدیق هویت کلید (اطمینان ایجاد شود که هیچ کس جز طرف مقابل و سایر معتمدین به کلید جلسه نمیتواند دسترسی داشته باشد)،

تصدیق هویت دو طرفه (هر دو طرف ارتباط هویت خود را اثبات میکنند)،

تایید کلید (مطمئن باشند که طرف مقابل واقعا کلید جلسه را در اختیار گرفت)،

محرمانگی پیشرو (اگر مهاجم کلید اصلی را یافت، همچنان کلیدهای جلسه قبلی امن بمانند)،

استحکام در برابر کلید فاش شده (اگر مهاجم کلید جلسه را یافت، نتواند به کلید اصلی یا کلید جلسات دیگر دسترسی پیدا کند).

.2

پروتکل اول:

با توجه به آنکه پروتکل ساده ای است به بخشی از معایب آن اشاره میشود؛ تصدیق هویت طرفین بررسی نمیشود. بنابراین یک Eve میتواند مانع از رسیدن پیام سوم بهB شود یعنی به جای A خودش را جایگزین نماید.

$\text{Eve} \rightarrow \text{B: } (K_S)\ K_{BT}\ , E\text{ve}$

تازگی پیام را بررسی نمیکند. بنابراین یک مهاجم میتواند پیام 2 یا 3 را از اجراهای قبلی دوباره بفرستد.، تایید کلید بررسی نمیشود بنابراین A مطمئن نیست که B کلید جلسه را در اختیار گرفته است.

پروتکل دوم:

تازگی کلید بررسی نمیشود. تصدیق هویت طرفین بررسی نمیشود.

محرمانگی پیشرو وجود ندارد چون با آشکار شدن کلید اصلی کلید جلسه نیز آشکار میشود.

تایید کلید وجود ندارد.

3. بله. در پروتکل اول Eve میتواند مانع از رسیدن پیام سوم به B شود. امکان حمله replay هم وجود دارد. هم چنین در برابر حمله MITM آسیب پذیر است که eve میان A و B قرار گرفته و A به جای آنکه با B کلید جلسه مبادله کند با Eve ارتباط برقرار میکند و چون هیچ تصدیق اصالتی وجود ندارد متوجه این جریان نمیشود. سناریو بدین شکل خواهد شد:

$A \rightarrow Eve : A, B$

$Eve \rightarrow T: Eve, A$

$T \rightarrow Eve: (K_S)K_{EveT}, (K_S)\ K_{AT}$

$Eve \rightarrow A: (K_S)\ K_{AT}\ , (K_S)\ K_{EveT}$

$A \rightarrow Eve : (K_S)\ K_{EveT}, A$

پروتکل دوم:

امکان تغییر پیام هم چون تغییر n_B ، حمله replay مانند تکرار پیام سوم وجود دارد و هم چنین Eve میتواند خود را به عنوان A معرفی کند و B را فریب دهد که سناریو آن بدین صورت است:

ایتدا Eve خود را به عنوان A پیام n_A, A را برای قربانی B ارسال کرده و B با فرستادن MAC(A, n_A) به عنوان پاسخ به چالش Eve و پیام $\text{MAC}(n_B)\ K_{AB} \oplus K_S$ او را به چالش می کشد و انتظار دارد مهاجم برای او A, MAC (A, n_B) K_{AB} را ارسال کند. چون مهاجم کلید K_{AB} را ندارد پس نمیتواند چنین پاسخی را برای B بفرستد پس یک ارتباط دیگر با B ایجاد میکند و به عنوان چالش برای او A و n_B را میفرستد و B در جواب این چالش MAC (A, n_B) K_{AB} را ارسال میکند یعنی همان جوابی که در ارتباط اول باید برای B می فرستاد را اکنون از B در ارتباطی دیگر گرفته است و به این صورت B فریب میخورد.

سناریو بدین شکل خواهد شد:

$Eve \rightarrow B: A, n_A$

$B \rightarrow Eve: n_B, B, K_S \oplus \text{MAC}\ (n_B)\ K_{AB}, \text{MAC}\ (A, n_A)\ K_{AB}$

B is waiting for response of A(Eve) include [A, $\underline{\text{MAC (A, } n_B) \, K_{AB}}$]

Eve $\rightarrow$ B: A, n_B

B$\rightarrow$ Eve: n_B, B, $K_S \oplus$ MAC (n_B) K_{AB}, $\underline{\text{MAC (A, } n_B) \, K_{AB}}$

Now Eve continue the session:

Eve $\rightarrow$ B: A, MAC (A, n_B) K_{AB}

(سناریوی فوق reflection attack نام دارد)

4. در پروتکل اول شناسه‌ها را رمزشده بفرستیم یعنی شناسه مخاطب ارتباط و کلید جلسه با کلید اصلی رمز و تصدیق هویت شوند.

A $\rightarrow$ T: A, B

T $\rightarrow$ A: (K_S, B) K_{AT} , (K_S, A) K_{BT}

A $\rightarrow$ B: $(K_{S,}\, A)$ K_{BT}

در پروتکل دوم در خط دوم برای مثال عبارت MAC (A, n_B, n_A) K_{AB} جایگزین شود که تفاوت بیشتری در پیام سوم و پیام دوم باشد.

ایجاد تصدیق هویت طرفین برای جلوگیری از MITM، استفاده از sequence number،

استفاده از nonce و یا timestamp برای بررسی تازگی کلید،

استفاده از challenge response برای جلوگیری از حمله تکرار و... .

توجه: در کلیه سوالات، پاسخ هایی که میتوانند صحیح باشند ولی مانند پاسخ نامه نباشند نیز صحیح گرفته می‌شود.