دانشگاه صنعتی امیرکبیر
دانشکده مهندسی کامپیوتر

مدرس درس: دکتر حمیدرضا شهریاری

تدریس‌یار: مهدی نیکوقدم

پاییز1402

نکته1: جواب تمرینات صرفا برای افزایش اطلاعات دانشجویان قرار داده شده است. برای سوالات ممکن است جواب‌های مختلفی درست باشد. در نتیجه در صورتی که مشاهده کردید که جواب تمرینات شما با پاسخی که قرار داده شده است دقیقا مشابه نیست نگران نباشید! همان‌طوری که گفته شد برای سوالات جواب‌های مختلفی جواب صحیح است و این پاسخ‌ها تنها پاسخ‌های صحیح نمی‌باشد. همان‌طوری که از اول ترم در پایین تمامی تمرینات نوشته شده است هدف افزایش یادگیری شماست و همین که دانشجو تلاشی در راستای به دست آوردن جواب کرده باشد ارزشمند است.

نکته2: جواب برخی سوالات به طور کامل نوشته شده است. برخی سوالات نیز با توجه به اینکه حالت تحقیقاتی داشته‌اند آورده نشده است. همچنین با توجه به این موضوع که برخی دانشجویان جواب‌های واقعا جالبی به سوالات داده‌اند. پاسخ آن‌ها به عنوان یک نمونه در این فایل آورده شده است تا نحوه پاسخگویی به سوالات را مشاهده کنید و بتوانید نحوه تفکر و فکر دیگر دوستانتون رو ببینین.

شماره	سوال
1	الف) فرمول زیر کدام الگوریتم رمزنگاری را مشخص می کند؟ با توجه به فرمول آن را توضیح دهید. C = E(K3, D(K2, E(K1, P))) ب) طول کلید موثر در این روش چند بیت است؟ ج) در صورتی برابری سه پارامتر K1, K2, K3 این الگوریتم به چه الگوریتمی تبدیل می شود؟ بر روی فرمول نشان دهید. راهنما : C: Ciphertext P: Plaintext K: Key E: Encrypt function -> E(K, P) = C D: Decrypt function الف) الگوریتم triple des. پیام اولیه سه بار و هر بار توسط یک کلید متمایز رمزنگاری می‌شود. ب) 3*56= 168 bit ج) K=k1=k2=k3 E(k,p)=m D(k,m)=p E(k,p)=m پس در صورت برابر بودن 3 کلید، الگوریتم مانند الگوریتم des عادی و فقط یک بار پیام را رمز می‌کند.
2	می‌خواهیم یک امضای دیجیتال انجام دهیم. پیام مد نظر را پس از هش کردن به الگوریتم RSA می دهیم تا رمز نگاری انجام گیرد. با فرض اینکه پیام مد نظر برابر 234 بوده و دو عدد اول در نظر گرفته شده برابر 71 و 37 باشند: الف) یک توان مناسب برای رمز کردن پیام مد نظر به دست آورید.

شماره	سوال
	ب) پیام رمز شده (C) را بیابید. ج) پارامتر مورد نیاز برای رمزگشایی را به دست آورید. *(نوشتن راه حل و فرمول های استفاده شده ضروری است) در اینجا مقادیر p و q مشخص هستند، در نتیجه ابتدا $\phi(N = pq = 2627) = (p-1)(q-1)$ را محاسبه می‌کنیم که برابر 2520 است. لازم است مقدار توان e و $\phi(N)$ نسبت به هم اول باشند و همچنین e از $\phi(N)$ کمتر باشد. **الف)** مقدار e می‌تواند 127 باشد. **ب)** $$\begin{aligned} C &= M^e \mod N \\ &= 234^{127} \mod 2627 \\ &= 345 \end{aligned}$$ **ج)** حال باید d را محاسبه کنیم: $$\begin{aligned} d \times e &\equiv 1 \mod \phi(N) \\ e^{\phi(N)} &\equiv 1 \mod \phi(N) \\ e^{\phi(N)-1} &\equiv e^{-1} \mod \phi(N) \\ e^{2519} &\equiv 2143 \mod \phi(N) \\ \implies d &= 2143 \end{aligned}$$ $$\begin{aligned} M &= 345^{2143} \mod 2627 \\ &= 234 \end{aligned}$$
3	برای مبادله کلید از الگوریتمDiffie-Helman با عدد اول13 = q و ریشه ی اول آن2 = α را در نظر می‌گیریم. اگر کاربر Aکلید عمومی7 = YA و کاربرB کلید عمومی10 = YB را داشته باشند، کلید های خصوصی هر دو کاربر و کلید مشترک سرّی K را محاسبه کنید. **نوشتن راه حل و فرمول های استفاده شده ضروری است **نمونه اول:**

شماره	سوال
	$$Y_A \equiv \alpha^{X_A} \mod q$$ $$7 \equiv 2^{X_A} \mod 13$$ $$2^{X_A} - 7 \equiv 0 \mod 13$$ $$X_A = 1 \Longrightarrow 2 - 7 \not\equiv 0 \mod 13$$ $$X_A = 2 \Longrightarrow 4 - 7 \not\equiv 0 \mod 13$$ $$X_A = 11 \Longrightarrow 2048 - 7 \equiv 0 \mod 13$$ $$10 \equiv 2^{X_B} \mod 13$$ $$2^{X_B} - 10 \equiv 0 \mod 13$$ $$X_B = 1 \Longrightarrow 2 - 7 \not\equiv 0 \mod 13$$ $$X_B = 2 \Longrightarrow 4 - 7 \not\equiv 0 \mod 13$$ $$X_B = 10 \Longrightarrow 1024 - 10 \equiv 0 \mod 13$$ $$K_{AB} \equiv Y_A^{X_B} \mod 13$$ $$= 7^{10} \mod 13$$ $$= 4$$ $$K_{AB} \equiv Y_B^{X_A} \mod 13$$ $$= 10^{11} \mod 13$$ $$= 4$$ نمونه دوم: q=13 , a=2 , YA=7, YB = 10 XA = 2^7 mod 13 = 11 , XB = 2^10 mod 13 = 10 K = YB^XA mod q = 10^11 mod 13 = 4
4	آیا یک الگوریتم رمزنگاری جریانی (Stream cipher)به تنهایی می تواند از یکپارچگی پیام ارسالی (message integrity)محافظت کند؟ توضیح دهید.

شماره	سوال
	اگر برای یک پیام یکپارچگی کافی وجود نداشته باشد، مهاجم با کمک روشی مانند حمله مرد میانی قسمتی از پیام را کشف کرده و بدون داشتن کلید هم ان را رمزگشایی می‌کند.
7	اصطلاحات زیر را تعریف کرده و در قالب یک مثال واقعی تشریح کنید. Vulnerability: Threat : Attack : Asset : Risk : **نمونه اول** **Vulnerability**: نقطه ضعفی است که می تواند توسط یک عامل تهدید، مانند یک مهاجم، مورد استفاده قرار گیرد تا از مرزهای سیستم عبور کند. **Threat**: یک اقدام یا رویداد منفی بالقوه است که توسط آسیب پذیری تسهیل می شود و منجر به تأثیر ناخواسته بر روی سیستم رایانه ای یا برنامه می شود. **Attack**: به هر تلاشی برای آشکار کردن، تغییر، غیرفعال کردن، تخریب، سرقت یا دستیابی به دسترسی غیرمجاز یا استفاده غیر مجاز از دارایی انجام می شود گویند. **Asset**: به هرگونه داده ، دستگاه یا سایر مولفه های محیط گفته می شود که از فعالیت های مربوط به اطلاعات پشتیبانی می کند. **Risk**: در واقع هر چیزی در رایانه است که ممکن است بدون اطلاع و رضایت کاربر، به داده ها آسیب برساند یا سرقت کند یا به شخص دیگری اجازه دسترسی به رایانه را بدهد. **نمونه دوم** **Vulnerability :**نسبت به حملات و خطرات آسیب‌رسان به جسم یا روح، افراد، جوامع، حیوانات، وسایل و دستگاه‌ها، آب‌وهوا و در کل همه‌چیز می‌تواند بنوعی آسیب‌پذیر باشد. بجز خطرات، افراد می‌توانند نسبت به تمایلات نیز آسیب‌پذیر باشند همچون آسیب‌پذیری جوانان نسبت به اعتیاد و الکل. **Threat :**در امنیت رایانه ، تهدید یک اقدام یا رویداد منفی بالقوه است که توسط آسیب پذیری تسهیل می شود و منجر به تأثیر ناخواسته بر روی سیستم رایانه ای یا برنامه می شود. یک تهدید می تواند یا یک رویداد منفی "عمدی" یا یک رویداد منفی "تصادفی" باشد و یا در غیر این صورت یک شرایط ، قابلیت ، اقدام یا رویداد است. **Attack :** استخراج غیر قانونی اطلاعات از سیستم‌های کامپیوتری، شبکه‌ها و شرکت‌های وابسته به فناوری اطلاعات است. این حمله‌ها با استفاده از کدهای مخرب برای تغییر در کدهای کامپیوتر، داده یا منطق استفاده می‌شود. به عبارت دیگر حمله، یکی از بزرگترین تهدیدات امنیتی در فناوری اطلاعات است و به شکل‌های مختلف، عمل می‌کند. در کامپیوتر و شبکه‌های کامپیوتری دلیل حمله می‌تواند از بین بردن، عمومی‌کردن، تغییر دادن، غیرفعال کردن، سرقت و یا به دست آوردن دسترسی و استفاده غیرمجاز از اطلاعات باشد از این رو در این مقاله به تعریف حمله و انواع حملات فعال در شبکه می پردازیم. **نمونه سوم**

شماره	سوال
	Vulnerability به معنی آسیب‌پذیری است، یک نقطه ضعف سیستم که می‌تواند exploit شود. برای مثال الگوریتم DES یک الگوریتم آسیب‌پذیر محسوب می‌شود چراکه نسبت به حمله bruteforce آسیب‌پذیر است. **Threat** تهدید، به معنی یک خطر بالقوه برای سیستم است. به عنوان مثال می‌توان افشای اطلاعات را یک تهدید تلقی کرد. **Attack** حمله، به معنی تلاش برای نقض امنیت است. تلاش برای یافتن رمز wifi هرچند نافرجام حمله محسوب می‌شود. **Asset** دارایی‌های ارزشمند، که هدف امنیت حفاظت از آنهاست. مثل دیتابیس شامل دیتای مشتریان یک شرکت. **Risk** خطر، احتمال رخداد حمله موفق و از بین رفتن امنیت. مثلا همیشه احتمال پیدا شدن کلید رمزگذاری توسط مهاجم به صورت رندوم وجود دارد، اما به قدری احتمال رخداد آن کم است که عملا خطر یا ریسکی ندارد.
8	چهار روش احراز هویت را نام ببرید و از هرکدام یک مثال بزنید. مزایا و معایب این روش ها را بیان کرده و ازجنبه های مختلف با هم مقایسه کنید(**سوال حذف شد**)
9	الف) درباره الگوریتم های متقارن و نامتقارن، هر از موارد زیر را مقایسه کنید: مدیریت توزیع کلید - عملیات رمز گذاری و رمزگشایی - مقاومت در برابر حملات. ب) با توجه به مزایا و معایب هر کدام از روش های فوق، برای داشتن یک رمزنگاری بهینه چه راه حلی پیشنهاد می‌دهید؟ **نمونه اول**

شماره	سوال
	مدیریت توزیع کلید: متقارن: در الگوریتم‌های متقارن، هر دو طرف برای ارتباط امن نیاز به داشتن یک کلید مشترک دارند. مسئله اصلی در اینجا نحوه امنیت در انتقال و مدیریت این کلیدهاست. اگر کلید به دست یک حمله‌گر بیافتد، امنیت کل مکالمه به خطر می‌افتد. نامتقارن: اصلی‌ترین ویژگی‌های الگوریتم‌های نامتقارن استفاده از یک جفت کلید عمومی و خصوصی است. کلید عمومی برای رمزگشایی و کلید خصوصی برای رمزنگاری استفاده می‌شود. کلیدها بصورت ایمن مبادله می‌شوند و کلید عمومی برای عموم قابل دسترسی است. در الگوریتم‌های نامتقارن، نیاز به مدیریت توزیع کلید کمتر است، زیرا هر فرد یک جفت کلید عمومی و خصوصی دارد. عملیات رمزگذاری و رمزگشایی متقارن: در الگوریتم‌های متقارن، یک کلید واحد برای رمزنگاری و رمزگشایی استفاده می‌شود. نامتقارن: در الگوریتم‌های نامتقارن، دو کلید مختلف برای رمزنگاری و رمزگشایی استفاده می‌شود. الگوریتم رمزنگاری با یک کلید و الگوریتم رمزگشایی با کلید دیگر عمل می‌کند. مقاومت در برابر حملات متقارن: اگر کلید به دست حمله‌گر بیافتد، امنیت کل سامانه به خطر می‌افتد. نامتقارن: گر حمله‌گر کلید عمومی را بداند، نمی‌تواند از آن به کلید خصوصی برسد. ب) سرعت رمزنگاری در الگوریتم‌های متقارن بیشتر است و محدودیت حجم داده هم وجود ندارد. ولی به دلیل اینکه باید یک کلید یکسان در دوطرف وجود داشته باشد و اگر این کلید به دست فرد نامعتبری بیفتد امنیت سیستم به خطر می افتد می توان این روش را پیشنهاد کرد: با استفاده از روش نامتقارن طرف هویت یکدیگر را تایید کنند و سپس با استفاده از همین روش یک کلید مشترک برای رمزنگاری متقارن بین یکدیگر به اشتراک بگذارند. **نمونه دوم** مدیریت توزیع کلید: در رمزنگاري متقارن از یک کلید برای رمزگذاري و رمزگشایی استفاده می شود اما در نامتقارن کلید رمزگذاري و رمزگشایی متفاوت است. رمزگشایی و رمزگذاري: در حالت متقارن با همان کلیدي که رمزگذاري شده است، رمزگشایی هم انجام میگیرد. اما در نامتقارن اگر با کلید عمومی رمزگذاري انجام شود، تنها با کلید خصوصی رمزگشایی می شود و این به صورت بر عکس هم برقرار است. لذا سرعت کار در متقارن بالاتر است ولی مشکل جابجایی کلید در متقارن هست. مقاوم در مقابل حملات: متقارن در مقابل حملات آسیب پذیر است زیرا از یک کلید استفاده می کنند و تمام امنیت آن ها بر پایه مخفی بودن کلید است. در حالی که در نامتقارن کلید عمومی در دست همه هست و امنیت آن بر اساس مخفی بودن کلیدهاي خصوصی است. ب) بسته به میزان اهمیت اطلاعات اگر اطلاعات بسیار برای ما اهمیت دارد، رمز نگاری نامتقارن بهتر است.

شماره	سوال
10	دستگاه فروش خودکار (ATM) را در نظر بگیرید که در آن کاربران یک شماره شناسایی شخصی (PIN) و یک کارت برای دسترسی به حساب ارائه می دهند. در هر یک از موارد confidentiality, integrity, and availability مربوط به سیستم، مثال‌هایی را بیان کنید. **نمونه اول** Confidentiality (محرمانگی) : جلوگیری از دسترسی به اطلاعات توسط افراد غیرمجاز افراد غیرمجاز نتوانند اطلاعات حساب بانکی ما را بخوانند و به آن دسترسی داشته باشند . Integrity (یکپارچگی) : جلوگیری از تغییر و دستکاری اطلاعات توسط افراد غیرمجاز افرادغیر مجاز نتوانند اطلاعات حساب بانکی ما را تغییر بدهند . Availability(دسترسی‌پذیری) : اطلاعات فارغ از حملاتی که ممکن است روی آن انجام شود، در دسترس باشد . اگر بانک دچار حملاتی مانند DDos شود و اگر از دسترس خارج شود این باعث نقص این مورد می شود . **نمونه دوم** سیستم باید شماره های شناسایی شخصی را چه در سیستم میزبان و چه در حین انتقال برای یک تراکنش محرمانه نگه دارد. این باید از یکپارچگی سوابق حساب و معاملات فردی محافظت کند. در دسترس بودن سیستم میزبان برای رفاه اقتصادی بانک مهم است ، اما نه به مسئولیت امانتداری آن. در دسترس بودن ماشین آلات حسابداری کمتر باعث نگرانی می شود. **نمونه سوم** محرمانه بودن: برای دسترسی به کارتهای بدهی یا اعتباری باید یک رمز ورود امنیتی وارد کنید که فقط برای کاربران مجاز در دسترس است و هدف آن افزایش سطح امنیت است. ضمن اطمینان از پین کارت مربوطه ، مسئولیت اطمینان از استفاده از پین محکم به عهده کاربر نهایی است. بانک ها همچنین برای جلوگیری از هک کردن ، هر زمان که ارتباطی بین دستگاه خودپرداز و سرور بانک برقرار است ، باید از حریم شخصی افراد اطمینان حاصل کنند. کل معامله باید به درستی ایمن شود تا از بروز هرگونه آسیب یا هکرهای شکسته شدن پین کارت و دسترسی به آن جلوگیری شود . رمزگذاری صحیح پین اطمینان می دهد که سطح بالایی از محرمانه بودن حفظ می شود در حالی که عدم توجه به همان مورد می تواند منجر به نقض اطلاعات یا اطلاعات مشتریان شود. علاوه بر این ، سیاست مربوط به تغییر پین پس از فواصل منظم به افزایش مشتریان و ایمن نگه داشتن داده ها و اطلاعات کمک می کند. یکپارچگی: استفاده از فناوری پیشرفته ، کارآمد و بهینه سازی و همکاری مناسب دستگاه های خودپرداز برای اطمینان از حفظ یکپارچگی و ایمنی اطلاعات مشتریان ضروری است. هر دو مورد در صورت برداشت و واریز ، سیستم ها باید از نظر زمانی با داده های معتبر به روز شوند و به هیچ وجه بر حساب مشتری تأثیر نمی گذارد. برداشت پول باید به عنوان بدهی در حساب منعکس شود ، واریز وجه منجر به اعتبار حساب می شود. در دسترس بودن : بایستی سیستم های فعال **ATM** تعداد آن متناسب با سرویس گیرندگان آن باشد و اگر تعداد آن کم باشد موجب نارضایتی کاربران میشود
11	رمز قالبی ۸ بیتی مبتنی بر ساختار **Feistel** با دو **round** را در نظر بگیرید که **K** عضو Z_{15} و تابع **f** آن به صورت زیر تعریف می شود: $f_i(x, K) = (2i.K)^x \bmod 15, i = \{1,2\}$ اگر **K = 7** و متن رمز شده برابر با **00111111** باشد، متن اصلی چه مقداری می‌تواند باشد؟

شماره	سوال
	با توجه به ساختار **Feistel** داریم:

DEC:

Ciphertext = (L_{n+1}, R_{n+1})

$R_i = L_{i+1}$

$L_i = R_{i+1} \oplus F(L_{i+1}, K_i)$

Plaintext = (L_0, R_0)

K = 7, $f_i(x, K) = (2 \cdot i \cdot K)^x \bmod 15$,

R2 = 1111, L2 = 0011

$f_2(x, K) = (2 \cdot 2 \cdot K)^x \bmod 15$,

R1 = 0011, L1 = 1111 $\oplus$ $f_2(3, 7)$ = 1111 $\oplus$ 0111 = 1000

$f_2(3, 7) = 28^3 \bmod 15 = (-2)^3 \bmod 15 = 7$

$f_1(x, K) = (2 \cdot 1 \cdot K)^x \bmod 15$,

R0 = 1000, L1 = 0011 $\oplus$ $f_1(8, 7)$ = 0011 $\oplus$ 0001 = 0010

$f_1(8, 7) = 14^8 \bmod 15 = (-1)^8 \bmod 15 = 1$