دانشگاه صنعتی امیرکبیر
دانشکده مهندسی کامپیوتر

مدرس درس: دکتر حمیدرضا شهریاری

تدریس‌یار: مهدی نیکوقدم

پاییز1402

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
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. 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)
3	برای مبادله کلید از الگوریتم Diffie-Hellman با عدد اول $q = 13$ و ریشه ی اول آن $\alpha = 2$ را در نظر می‌گیریم. اگر کاربر A کلید عمومی $YA = 7$ و کاربر B کلید عمومی $YB = 10$ 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
4	آیا یک الگوریتم رمزنگاری جریانی (Stream cipher) به تنهایی می تواند از یکپارچگی پیام ارسالی (message integrity) محافظت کند؟ توضیح دهید
7	اصطلاحات زیر را تعریف کرده و در قالب یک مثال واقعی تشریح کنید. Vulnerability: Threat : Attack : Asset : Risk :
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
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؟
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.
11	رمز قالبی ۸ بیتی مبتنی بر ساختار **Feistel** با دو **round** را در نظر بگیرید که **K** عضو $\mathbf{Z}_{15}$ و تابع **f** آن به صورت زیر تعریف می شود:

شماره	سوال
	$f_i(x, K) = (2i.K)^x \bmod 15, i = \{1,2\}$ اگر $K = 7$ و متن رمز شده برابر با **00111111** باشد، متن اصلی چه مقداری می‌تواند باشد؟

- **عکسی واضح از برگه پاسخ تهیه و به فرمت pdf در آورید و آپلود کنید.**
- **فرمت نامگذاری پاسخ به صورت HW_StdNO_StdName باشد.**
- **پاسخ تمرینات حتما قبل از موعد تحویل اعلام شده در هر سری، بارگذاری شوند. تمریناتی که بعد از موعد تحویل ارسال شوند به هیچ عنوان تصحیح نخواهند شد.**
- **در صورت مشاهده تمرینات کپی شده برای طرفین نمره صفر در نظر گرفته می‌شود.**

هدف افزایش یادگیری است!

مهدی نیکوقدم