دانشگاه صنعتی امیرکبیر
دانشکده مهندسی کامپیوتر

مدرس درس: دکتر حمیدرضا شهریاری

تدریس‌یار: مهدی نیکوقدم

پاییز1402

1. عبارت Computer Security به چه معناست ؟

2. تفاوت حمله، تهدید، و آسیب‌پذیری را توضیح دهید.

3. منظور از حملات فعال و غیرفعال را توضیح دهید. تشخیص کدام حمله سخت‌تر است؟ توضیح دهید.

4. حملات زیر را توضیح دهید و بیان کنید که در کدام دسته از حملات قرار می‌گیرند.

- حمله جعل هویت
- حمله تکرار
- حمله دستکاری
- حمله شنود
- حمله منع سرویس

5. در مورد سوال موارد زیر **تحقیق** کنید و توضیح دهید که هر کدام زیر مجموعه کدام مورد دیگر است.

- data leakage
- privacy
- anonymity
- untraceability
- confidentiality

6. فرض کنید که DES(a,k) رمزنگاری متن ساده a را با کلید k با استفاده از سیستم رمزنگاری DES را نشان دهد. همچنین فرض کنید c = DES(a,k) و cc= DES(a', k') که در آن منظور از (') مکمل بیتی میباشد. ثابت کنید $cc = 'c$

- **عکسی واضح از برگه پاسخ تهیه و به فرمت pdf در آورید و آپلود کنید.**
- **فرمت نامگذاری پاسخ به صورت HW4_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