دانشگاه صنعتی امیرکبیر
دانشکده مهندسی کامپیوتر

دکتر حمیدرضا شهریاری

مهدی نیکوقدم

پاییز 1402

1. سه روش که می‌تواند امنیت اعتبارسنجی کاربر در یک محیط توزیع شده را بهبود دهد بیان کنید؟

2. چهار نیازی که برای **Kerberos** تعریف شده است کدامند؟

3. تفاوت‌های بین ورژن 4 و **Kerberos 5** در چیست؟

4. هدف از استفاده کلید جلسه در **Kerberos** چیست؟

5. تفاوت بین توافق کلید و تبادل کلید در چیست؟ کدام سربار کمتری دارند؟ در چه زمانی از توافق کلید و در چه زمانی از تبادل کلید استفاده می‌کنیم؟

6. پارامترهایی که حالت **Session** را تعریف می‌کنند را بیان کرده و مختصرا توضیح دهید. تفاوت بین کلید عمومی خصوصی و کلید جلسه را بیان کنید.

7. تعریف شما از مرکز توزیع کلید چیست و راه‌های ممکن برای توزیع یک کلید سری بین دو واحد را نام ببرید.

8. به لینک https://sslcheck.cert.ir/fa/ و یا https://sslcheck.certcc.ir مراجعه کنید و بعد از مطالعه و فهم مسئله‌ای که هدف سایت است، 3 سایت را به دلخواه از نظر امنیتی بررسی کنید و نتایج را به صورت اسکرین در **PDF** قرار دهید.

9. چگونه می‌توان از رمزنگاری کلید عمومی برای توزیع یک کلید مخفی استفاده کرد؟

10. الگوریتم دیفی هلمن را با عدد اول **q=11** و ریشه ابتدایی **a=2** در نظر بگیرید.
الف. اگر کاربر کلید عمومی **A** و **Ya=9** را داشته باشد کلید اختصاصی **Xa** کدام است؟
ب. اگر کاربر **B** کلید عمومی برابر ۳ داشته باشد، کلید سری مشترک **k**چیست؟

- 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