بسمه تعالی

دانشگاه شهیدبهشتی
دانشکده مهندسی و علوم کامپیوتر
امنیت شبکه‌های کامپیوتری پیشرفته
تمرین دوم

۱. دسته بندی خدمات امنیتی را فهرست کرده و به طور مختصر تعریف کنید.
۲. بر اساس آنچه مهاجم شناخته شده است انواع حملات رمزنگاری را فهرست کرده و به طور خلاصه تعریف کنید.
۳. دو مشکل one-time pad چیست؟
۴. تفاوت بین رمز بلوکی و رمز جریان چیست؟
۵. تفاوت بین message authentication code و تابع one-way hash چیست؟
۶. امضای دیجیتال چه ویژگی هایی باید داشته باشد؟
۷. یک طرح امضای دیجیتال باید چه الزاماتی را برآورده کند؟
۸. سه رویکرد کلی برای مقابله با replay attacks را فهرست کنید.
۹. چه خدماتی توسط IPSec ارائه می شود؟
۱۰. تفاوت بین حالت transport و حالت tunnel چیست؟
۱۱. تفاوت بین SSL connection و SSL session چیست؟
۱۲. پارامترهایی را که یک SSL session state را تعریف می کنند فهرست کرده و به طور خلاصه تعریف کنید.
۱۳. پارامترهایی را که یک SSL session connection را تعریف می کنند فهرست کرده و به طور خلاصه تعریف کنید.
۱۴. چه خدماتی توسط پروتکل SSL Record ارائه می شود؟