تکلیف سری اول شبکه‌های انتقال داده

۱- در ارسال داده‌های صوتی چه شرایط باید فراهم باشد تا شبکه بتواند کیفیت مناسبی را ارایه دهد؟

۲- دو شباهت و دو تفاوت مدل OSI و TCP/IP را بیان کنید

۳- در مدل OSI، کدامیک از لایه‌ها وظایف زیر را بر عهده دارند:

الف) تبدیل دنباله‌ها به فریم

ب) تعیین مسیر در شبکه

۴- فرض کنید می خواهیم یک تصویر سیاه و سفید با ابعاد ۳۰۷۲*۱۵۳۶ پیکسل ارسال کنیم(هر پیکسل یک بایت جا می‌گیرد). اگر سرعت ارسال ۵۶ کیلوبایت بر ثانیه باشد این ارسال چقدر طول می‌کشد؟ در صورت سرعت ارسال ۱ مگا بایت بر ثانیه زمان ارسال چقدر است؟

۵- تفاوت سوییچینگ مداری با سوییچینگ بسته چیست؟

۶- تفاوت لایه اتصال‌گرا با لایه بدون اتصال چیست؟

۷- دلیل استفاده از مخابرات ماهواره‌ای در ارسال داده‌ها علی رغم هزینه زیاد چیست؟

۸- فرض کنید بخواهیم دنباله ۰۱۰۰۰۱۰۰۱ را به همراه کد CRC ۴ بیتی آن روی کانال بفرستیم. اگر چند جمله‌ای مربوط به CRC به صورت $x4+x+1$ باشد چه عبارتی روی کانال فرستاده می‌شود؟ فرض کنید در حین ارسال اولین بیت سمت چپ از صفر به یک تبدیل شود(دقت کنید که همراه این کد ۹ بیتی CRC ۴ بیتی آن نیز قرار دارد). این خطا چگونه مشخص می‌شود. آیا می توانید تغییر مثال بزنید که در کد CRC ۴ بیتی مشخص نشود؟

۹- الف) فرض کنید بخواهیم دنباله ۱۰۰۰۱۰۰۱ را به همراه کد CRC ۴ بیتی آن روی کانال بفرستیم. اگر چند جمله‌ای مربوط به CRC به صورت $x3+x2+1$ باشد چه عبارتی روی کانال فرستاده می‌شود؟ب) اگر ۱۰۰۰۰۰۰۱ (یا چند جمله‌ای $x7+1$)روی کانال ارسال شود خروجی چه خواهد بود؟ پ) با توجه به بند ب اگر CRC چند جمله‌ای $f(x)$ برابر A باشد CRC $x7f(x)$ و $(x7+1)f(x)$ چقدر خواهد بود؟ ت) فرض کنید در حین ارسال اولین بیت سمت چپ از صفر به یک تبدیل شود. خطا چگونه مشخص می‌شود؟

۱۰-قابلیت دسترسی در امنیت به چه معنایی است؟ محرمانگی و صحت به چه طریقی به دست می‌آیند؟

۱۱-تفاوت بین حملات فعال و غیر فعال در چیست؟ حمله فعال خطرناکتر است یا غیر فعال؟ توضیح دهید.

۱۲-چرا در رمزهای قالبی طول قالب و کلید ضریبی از ۳۲ است؟ چرا در رمزهای قالبی کلید از یک قالب به قالب بعد تغییر نمی‌کند؟

۱۳-مود CBC به چه دلیل به جای ECB به کار می‌رود؟ در چه محیطی از ECB و در چه محیطی از مود شمارنده (counter) استفاده می‌شود؟

۱۴-فرض کنید f یک تابع یکطرفه باشد. در این صورت به نظر شما چگونه می‌توان از آن یک رمز قالبی در مود شمارنده استفاده نمود؟ شرایط را بیان کنید؟

۱۵-رمزنگاری مود CBC قابل موازی شدن است یا رمزگشایی توضیح دهید.

۱۶-تابع یکطرفه در رمزهای کلید عمومی چگونه به کار می‌آید؟

۱۷-تفاوت روش‌های کلید عمومی و کلید متقارن چیست؟

۱۸-دلیل استفاده از گواهی (certificate) در روش‌های کلید عمومی چیست؟

۱۹-چرا برای امضای یک متن، ابتدا hash ان گرفته می‌شود و سپس امضا می‌شود؟

۲۰-تفاوت امضا با رمز چیست و چرا با کلیدهای متقارن نمی‌توان امضا طراحی کرد؟

۲۱- تفاوت MAC با Hash را بیان کنید.