به نام او

امتحان پایان ترم درس شبکه های مخابراتی

مدت امتحان:

سوال ۱) درستی یا نادرستی هر یک از گزاره های زیر را با بیان دلایل کافی تعیین کنید.

الف) در پروتکل های دسترسی چندگانه Random Access و Taking-Turns ، هنگامی که M نود به طور همزمان از کانالی با نرخ R استفاده می کنند، نرخ ارسال هر یک از نودها مقدار $\frac{R}{M}$ را خواهد داشت.

ب) در رهیافت Slotted Aloha با دو کاربر، اگر احتمال ارسال کاربر ،A دو برابر احتمال ارسال کاربر B باشد، نرخ موثر ارسال کاربر A نیز دوبرابر نرخ موثر ارسال کاربر B خواهد بود.

پ) PGP بر مبنای کلیدهای خصوصی و عمومی کار می کند و به کاربر هر دو امکان رمزگذاری (Encryption) و امضای دیجیتال (Digital Signature) را می دهد.

ت) به کمک nonce در SSL، می توان از ارسال بسته های تکراری یک کانکشن بسته شده و غیرفعال در یک کانکشن جاری، توسط شخص مزاحم (Intruder) جلوگیری کرد.

(ث) در Agent Solicitation، هنگامی که کاربر بیسیمی به شبکه‌ای می پیوندد، Foreign Agent آن شبکه سرویس خود را در قالب پیام ICMP شامل آی پی Agent و COA به کاربر می‌فرستد.

(ج) IPsec، برای کدگذاری دیتاگرام (datagram) های لایه‌ی شبکه استفاده می‌شود.

(چ) یکی از موانع پیاده سازی Collision Detection در مخابرات بیسیم، مسئله‌ی Hidden Terminal است.

سوال ۲) (امتیازی) در پروتکل Mobile IP، فرض کنید کاربری دارای مشخصات زیر است:

$$\text{Permenant Address} = 192.168.1.20$$
$$\text{Home Agent Address} = 192.168.1.10$$

این کاربر وارد شبکه‌ی جدیدی (Foreign Network) با مشخصات زیر می شود:

$$\text{Foreign Network Subnet Mask} = 34.56.112.128/25$$

الف) در مرحله Agent Discovery با رویکرد Agent Advertisement، چگونه آدرس آی پی جدید توسط Foreign Agent به این کاربر اختصاص داده می‌شود؟

ب) اگر آدرس آی پی جدید اختصاص داده شده به کاربر ،(COA) برابر 34.56.112.153 باشد، چگونه Home Agent از این آی پی جدید مطلع می‌شود؟ (مراحل را توضیح دهید.)

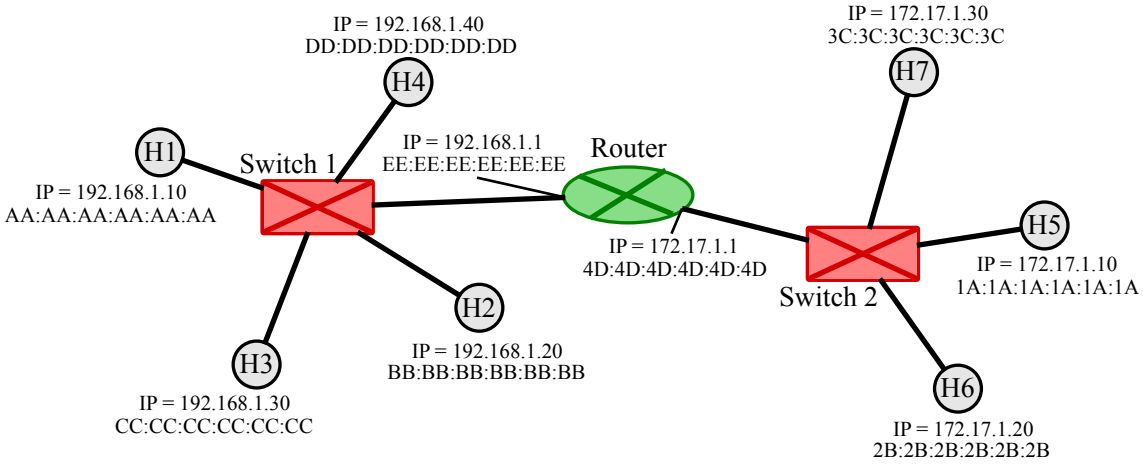
پ) هنگامی که کاربر از Foreign Network خارج می‌شود، آیا لازم است Foreign Agent مربوطه، آدرس آی پی اختصاص داده شده به کاربر (COA) را به طور دستی آزاد کند؟ چرا؟

سوال ۳) در تکنیک CSMA/CD، دو کاربر A و B از یک کانال به طور مشترک استفاده می‌کنند. هر کاربر پس از آشکارسازی n تصادم برای هر بسته خود، به اندازه K تا ارسال بعدی بسته صبر می‌کند که K به تصادف از بازه‌ی $\{۰, ۱, ۲, \cdots, ۲^n - ۱\}$ (بر حسب میلی ثانیه) انتخاب شده است. فرض کنید ارسال هر بسته، دقیقا ۱ میلی ثانیه طول می‌کشد و هر دو کاربر با شروع از تایم ابتدای تایم اسلات اول، بسته های خود را به طور پشت سر هم می‌فرستند.

الف) با چه احتمالی، کاربر A بسته‌ی اول خود را در تایم اسلات سوم با موفقیت ارسال می‌کند؟

ب) اگر در یک تایم اسلات خاص، کاربر های A و B، به ترتیب m و n تصادم را برای بسته خود تجربه کنند، با چه احتمالی در دو تایم اسلات بعدی تصادمی رخ نمی‌دهد؟

سوال ۴) در شبکه‌ی زیر که دو زیرشبکه (subnet) توسط یک روتر به هم متصل شده اند:

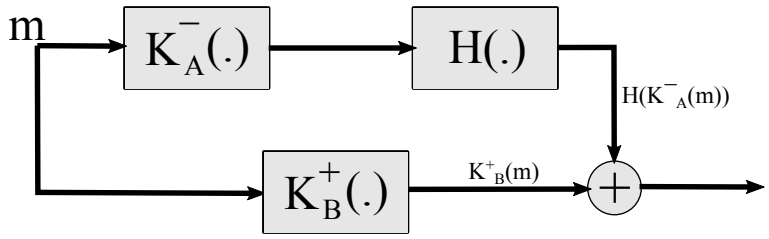


الف) اگر H1 بخواهد پیامی را به H2 بفرستد و Lookup Table سوئیچ ها خالی باشد، این پیام به کدام یک از نودهای H2 تا H7 فوروارد می‌شود؟ چرا؟

ب) اگر H1 بخواهد پیامی را به H5 بفرستد، با فرض آن که ARP table در تمام نودها و همچنین Lookup Table سوئیچ کامل باشد، مک آدرس و آی پی آدرس مبدا و مقصد را در frame هایی که از سوئیچ ۱ به پورت P1 روتر و از پورت P2 روتر به سوئیچ ۲ می روند را بنویسید.

پ) فرض کنید بخواهیم دو subnet مستقل ایجاد کنیم که subnet اول شامل نودهای H1 و H2 و subnet دیگر شامل نودهای H3 و H4 باشد. بدین منظور، برای دستکاری تنظیمات سوئیچ ۱ چه تکنیکی را پیشنهاد می‌کنید؟ توضیح دهید چگونه این تکنیک، نیاز شما را برآورده می‌کند.

سوال ۵) در مراحل رمزگذاری زیر، فرض کنید بلوک دایره الحاق دو رشته به هم را نشان می‌دهد. آلیس میخواهد پیام m را رمزگذاری کرده و به باب منتقل کند. فرض کنید کلید های خصوصی و عمومی آلیس به ترتیب K_A^- و K_A^+ و کلیدهای خصوصی و عمومی باب به ترتیب K_B^- و K_B^+ باشند.



الف) آیا تمام موارد محرمانگی پیام ،(Confidentiality) اصالت پیام (Authentication) و تمامیت پیام (Message Integrity) حفظ شده اند؟ هر مورد را توضیح دهید.

ب) باب در هنگام رمز گشایی پیام و تایید هویت فرستنده (Authentication) به چه مشکلی بر می‌خورد؟ راه حل این مشکل چیست؟

پ) پس از رفع مشکل قسمت ب، بلوک دیاگرام لازم را برای رمزگشایی پیام رسم کنید.

سوال ۶) برای firewall یک شبکه داخلی، جدولی زیر را به گونه ای تکمیل کنید که

- به کاربران داخلی شبکه، اجازه‌ی ارسال پکت به کاربران خارج شبکه را روی تمام پورت ها بدهد.
- به کاربران داخلی شبکه، اجازه‌ی ارتباط با سروری با آی پی 172.17.15.234 خارج از شبکه را روی پورت های ۰ تا ۱۰۲۳ بدهد.
- جلوی ارسال بسته از شبکه ای با $\text{subnet mask} = 10.33.12.16/28$ را بگیرد.

شماره پورت	آدرس آی پی مقصد	آدرس آی پی مبدا	عملکرد (مسدود/اجازه)