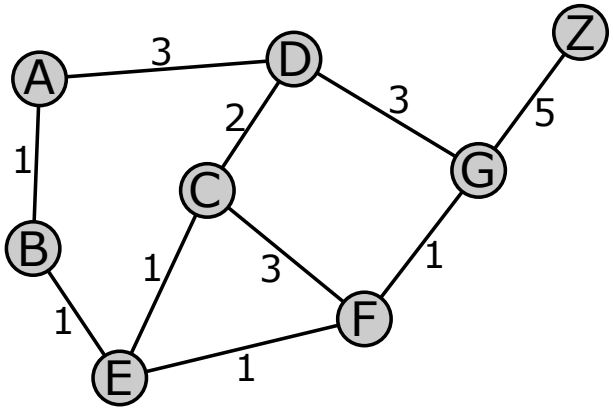
به نام زیبایی

پایان ترم شبکه‌های مخابراتی

زمان: ۱۲۰ دقیقه

پرسش ۱)

توپولوژی زیر داده شده است:

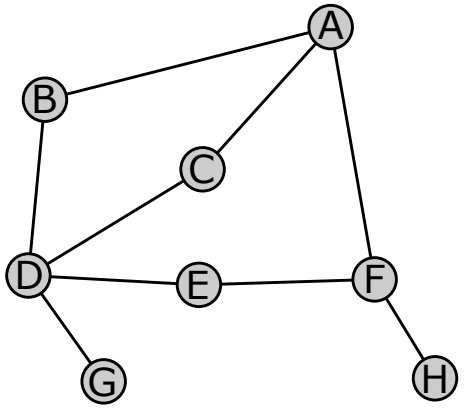


الف) با استفاده از الگوریتم دایکسترا، کوتاه ترین مسیر از A تا Z را بیابید.

ب) فرض کنید الگوریتم Bellman-Ford برای محاسبه‌ی کوتاه ترین مسیر بین نودهای شبکه‌ی فوق استفاده شده باشد. اگر هزینه‌ی لینک EF به ۱۰۰ افزایش یابد، الگوریتم Bellman-Ford برای تعیین مسیر بین C و Z به چه مشکلی بر می‌خورد؟ برای رفع این مشکل، راه حلی را پیشنهاد کنید و توضیح دهید این راه‌حل، چگونه مشکل بوجود آمده را رفع می‌کند.

پرسش ۲)

در شبکه‌ی زیر، فرض کنید نود A بسته‌ای به حجم 1Mbytes را به سایر نودها Broadcast کند. (احتمال آن که این بسته بر روی هر یک از لینکهای شبکه از یک نود به نود دیگر برسد، برابر ۰/۸ است.)



مجموع حجم بسته‌هایی که در شبکه مبادله می‌شوند (تا زمان دریافت موفق آمیز بسته توسط تمام نودها) چقدر است؟ اگر

الف) هر نود به محض دریافت یک نسخه از این بسته، آن را روی تمام لینک‌های خود به سایر نودها ارسال کند؟

ب) یک بسته در هر نود زمانی پذیرفته شود که از لینکی که روی کوتاهترین مسیر بین این نود و نود A قرار دارد دریافت شود؟ در صورت پذیرش، این بسته بر روی سایر لینکهای خروجی نود کپی می‌شود.

پ) از Minimum Spanning Tree استفاده شده باشد؟ فرض کنید این درخت پیشتر محاسبه شده است (Minimum Spanning Tree، خروجی الگوریتم دایکسترا از نود A به سایر نودهاست).

(هزینه‌ی تمام لینک ها برابر ۱ است.)

پرسش ۳)

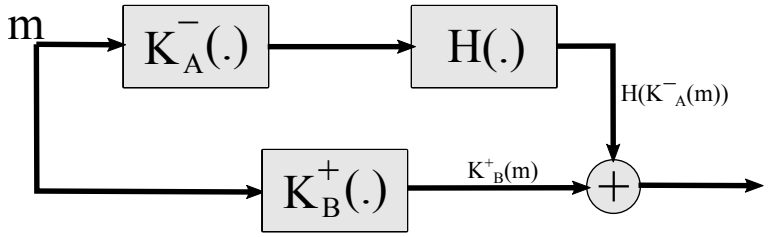
دو کاربر جهت ارسال بسته های خود، از یک لینک مشترک و پروتکل Slotted Aloha استفاده می‌کنند. مقادیر تایم اسلات، نرخ لینک و حجم بسته‌ها به ترتیب برابر 1msec ، 100Mbps و 12.5Kbytes است. احتمال ارسال بسته (تکراری یا غیرتکراری) در هر تایم اسلات، برای کاربر ۱ برابر p_1 و برای کاربر ۲ برابر p_2 است. اگر هر دو کاربر در یک تایم اسلات مشخص، بسته‌های خود را ارسال کنند، هر دو بسته در لینک از بین می‌روند.

الف) نرخ مؤثر ارسال برای هر یک از کاربران چقدر است؟

ب) به ازای چه مقدار از p_1 و p_2، مجموع نرخ مؤثر ارسالی کاربران بیشینه می‌شود؟ اگر $p_1 = 3p_2$ باشد چطور؟

پرسش ۴)

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. در مراحل رمزنگاری زیر در سمت آلیس،



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

ب) برای رفع مشکلهای مطرح شده در الف، چه راه حلی پیشنهاد می‌کنید؟

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

ت) باب برای تأیید اصالت کلید عمومی آلیس، چه سازوکاری را اتخاذ می‌کند؟ (جزئیات کامل)

ث) چنانچه آلیس بخواهد فایل ۲۰۰ مگابایتی را به باب ارسال کند، چه ساختار بهتری برای رمزنگاری آلیس پیشنهاد می‌کنید؟ دلیل برتری ساختار پیشنهادی خود را بیان کنید.