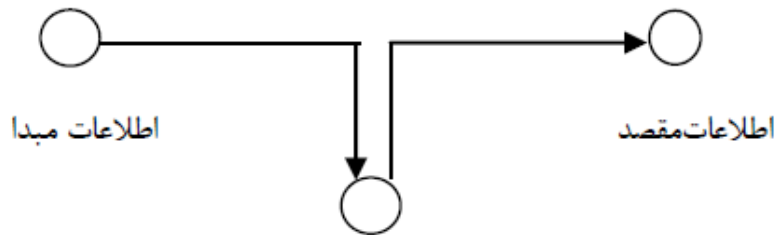


به نام خدا

آزمون میان ترم امنیت شبکه های کامپیوتری

۱- امنیت اطلاعات را تعریف کنید، کنترل هایی که برای تامین امنیت اطلاعات انجام می شود را نام برده و هرکدام را توضیح دهید؟

۲- حملات فعال و غیر فعال را توضیح داده و برای شکل زیر شرح دهید که چه حمله ای صورت گرفته است؟



۳- الف- چرا با وجود رمزنگاری متقارن از رمزنگاری نامتقارن نیز استفاده می گردد؟ تفاوت رمزنگاری متقارن با رمزنگاری نامتقارن در چیست؟ سرعت کدامیک بیشتر است؟

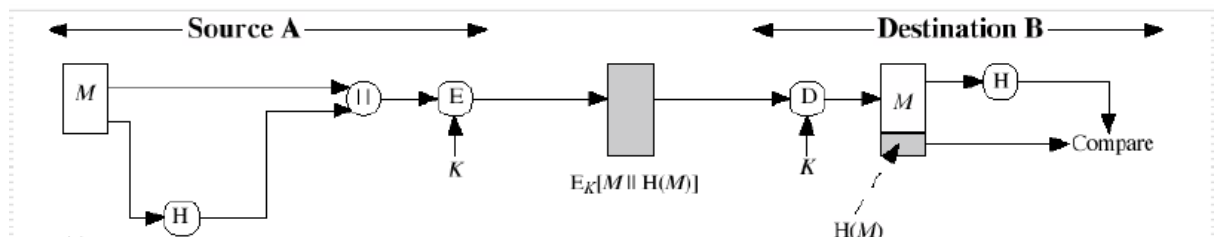
مشخصات ساختاری الگوریتم AES را بیان کنید؟ (طول قالب، طول کلید)

۴- خصوصیات و کاربرد های عمده رمزنگاری کلید عمومی (نامتقارن) را نام ببرید ؟

۵- رمزنگاری و کدگذاری چه تفاوتی با هم دارند و دلیل بوجود آمدن هرکدام را شرح دهید؟

۶- مد رمزنگاری چیست دلیل استفاده از آن را ذکر کرده و مد های معروف رمزنگاری را نام ببرید؟

۷- کاربرد توابع درهمساز را نام ببرید و برای شکل زیر توضیح دهید که چه کاربردی مد نظر است؟



۸- عبارت زیر را با روش ۲۱۳ رمزنگاری کنید؟

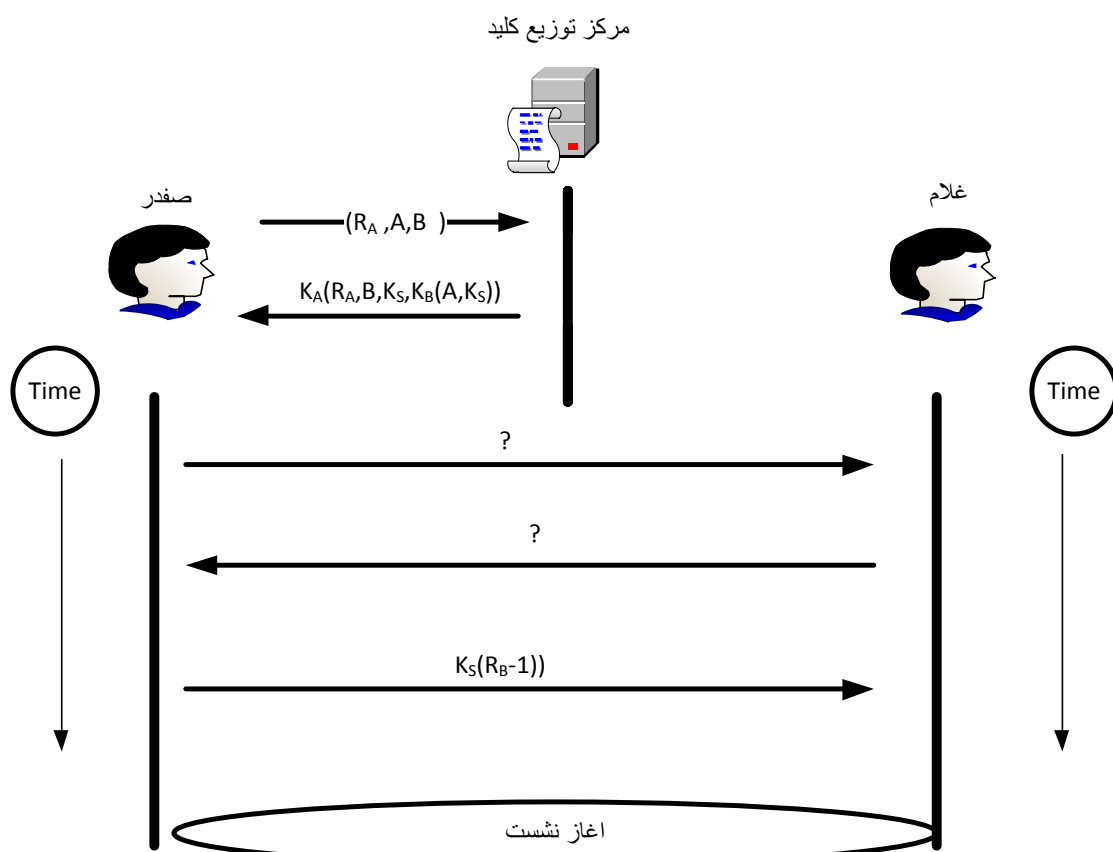
I KHOW HOW YOU FEEL.

۹- مفهوم AAA در دنیای امنیت اطلاعات چیست (ضمن تعریف مفهوم با ذکر مثال ارش که از خدمات یک بانک میخواهد استفاده کند توضیح دهید).

۱۰- مفاهیم نشست، نشست رمزنگاری شده و کلید نشست را توضیح دهید؟

۱۱- با توجه به شکل ابتدا قسمت های ناقص را با عبارات صحیح تکمیل کنید و سپس ضمن شرح مرحله ای این

پروتکل، به سوالات زیر پاسخ دهید؟



الف- نقش مرکز توزیع کلید کی به پایان میرسد؟

ب- در این پروتکل به چه صورت از حمله تکرار جلوگیری می شود؟

موفق باشید

بهار ۹۴