دانشکده مهندسی برق و کامپیوتر

میان‌ترم درس امنیت شبکه

زمان: ۷۵ دقیقه

۱۱ اردیبهشت ۱۴۰۱

نام و نام خانوادگی:

شماره دانشجویی:

۱- ارکان امنیت را نام ببرید و برای هر کدام مواردی را مثال بزنید که **فقط** آن رکن نقض می شود؟

۲- سیستم تشخیص نفوذ چیست و چه انواعی دارد؟

۳- روش رمزنگاری AES از چند Round استفاده می‌کند. توضیح دهید که در هر Round چه اعمالی انجام می شود؟

۴- توضیح دهید چرا سبک کاری ECB ناامن است؟

۵- چگونه می توان با استفاده از سبک‌های کاری یک رمز قالبی را به رمز جریانی تبدیل کنیم. در صورت نیاز مثال زنید.

۶- معکوس ضربی ۱۷ به پیمانه ۴۰۷ را پیدا کنید.

موفق باشید

اصغریان