نام درس: مبانی امنیت اطلاعات | **بسمه تعالی** | زمان : ۷۵ دقیقه

نام و نام خانوادگی: | شماره دانشجویی:

#	سوالات	بارم
۱	از مکانیزم های امنیتی فراگیر، ردپای ممیزی امنیتی Security Audit Trail و از مکانیزم‌های امنیتی مخصوص مبادله اعتبارسنجی را توضیح دهید.	۲
۲	الگوریتم HMAC را توضیح و طراحی روش آن را رسم کنید.	۲
۳	از جمله حملات فعال و غیر فعال Active, Passive را شرح دهید و برای هرکدام دو نمونه تشریح کنید.	۲
۴	یکپارچگی داده را تشریح کرده و سه مورد از سرویس‌های آن را توضیح دهید.	۲
۵	الگوریتم رمزنگاری AES را شرح‌دهید. (اندازه کلید، تعداد دورها، گام‌های هر دور و توضیح آن)	۲
۶	از مودهای علمیاتی رمزهای قالبی مود زنجیره‌ای قالبی Cipher Block Chaining و مود شمارنده COUNTER (CTR) را با رسم شکل توضیح دهید	۲
۷	یک سناریوی حمله مرد میانی موثر برای برای الگوریتم دفی هلمن توضیح دهید.	۲
	سربلند باشید	