بنام خدا

تکلیف شمارهٔ (۳) درس امنیت اطلاعات

۱ -تفاوت بین یک **block cipher** و یک **stream cipher** در چیست و از هریک در چه کاربردهائی استفاده می-شود؟

۲ -اثر **avalanche** چیست ؟

۳ -مودهای **ECB**،**CBC** ، **CFB** ، **OFB** و **COUNTER** که در رابطه با رمزهای قالبی از آنها استفاده میشود هریک دارای چه محاسن و چه معایبی هستند و در چه کاربردهائی از آنان استفاده میشود؟

۴ -کدام مودهای رمزهای قالبی میتوانند برای رمزنگاری اطلاعات بصورت **real-time** استفاده شوند؟

۵ -اگر بخواهیم یک نگاشت برگشت پذیر از **n** بیت به **n** بیت دیگر داشته باشیم، چند حالت ممکن وجود دارد؟

۶ -اگربا استفاده از رمزنگاری قالبی **S-DES** و با استفاده از کلید رمز **1100110111** ، یک بایت اطلاعات بصورت **AA** (هگزادسیمال نوشته شده است) باشد، بایت رمزشده چه خواهد بود؟

۷ -تعداد کلیدهای ممکن رمز **PLAYFAIR** چند کلید است ؟

۸ -**AES** به دنبال چه نیازهائی بوجود آمد ؟

۹ -در **AES** کلید معمولاً چند بیتی است و چند زیرکلید ازاین کلید تولید میشود. هریک از زیرکلیدها چند بیتی هستند ؟

۱۰ -حملهٔ**meet-in-the middle** به **Double DES** چیست ؟

۱۱ -چرا مرحلهٔ میانی **Triple DES** بجای رمزنگاری یک رمزگشائی است ؟

۱۲ -با جستجو در اینترنت ، الگوریتم های رمزنگاری **IDEA** ، **CAST-128** ، و **RC-2** را از نظر قالبی بودن و یا دنباله ای بودن، طول کلید ، طول بلوک های ورودی و خروجی و همچنین کاربرد مقایسه نمائید.

۱۳- نقاط قوت و ضعف رمزنگاری لینک و رمزنگاری سر- به- سر را بیان کنید

۱۴- تفاوت بین **Master Key** و **Session Key** در چیست؟

۱۵- **Nonce** چیست؟ چگونه تولید میشود و برای چه منظورهائی مورد استفاده قرار میگیرد؟

*****

***

*