بنام خدا

تکلیف شمارهٔ (۴) درس امنیت اطلاعات

(موضوع رمز نگاری نا متقارن)

۱ -تفاوت بین رمز نگاری متقارن و نا متقارن را نام ببرید.و تفاوت های اساسی آن دو را به اختصار شرح دهید.

۲ -الگوریتمهای متداول در درمز نگاری نامتقارن و امضای دیجیتال را نام ببرید.

۳ -فرق الگوریتم DH و ECDH را بیان نمایید.

۴ -بیان نمایید که در الگوریتم DH چه موادی به صورت رمز انتقال پیدا می کند؟

۵ -بیان نمایید که بدلیل صرفه جویی چه رمزی ارسال می گردد و در طرف مقابل کدام رمز در رمز نگاری DH متقارن و کدام نامتقارن استفاده می گردد.؟

۶ -چرا امضای دیجیتال قوی تر از امضای معمولی می باشد؟

۷ -فرق اساسی بین امضای دیجیتال و رمز نگاری نا متقارن در چیست؟

۸ -پیغام Digest به چه منظور استفاده می شود؟

۹ -از الگوریتم های DSA و RSA کدام برای مقاصد استراق سمع دولت امریکا بکار می رود؟

۱۰ -CA مخفف چیست؟در مورد CA هر چه می دانید بنویسید.

۱۱ - منظور از ریشه های CA چیست نام ببرید.

۱۲ -منظور از PKI چیست؟

*****

***

*