بنام خدا

تکلیف شمارهٔ (۲) درس امنیت اطلاعات

۱- تفاوت بین الگوریتمی که دارای امنیت نامشروط است با الگوریتمی که دارای امنیت محاسباتی است در چیست؟

۲- فرق یک cryptograph با یک cryptoanalyst چیست؟

۳- فرق یک رمز قالبی (block cipher) با یک رمز دنباله ای (stream cipher) چیست؟ موارد استفاده هرکدام کدام است؟

۴- امحاء اسناد چه نقشی را در امنیت اطلاعات بازی میکند؟

۵- حملات آماری به رمزها چه هستند و برای کم کردن آسیب پذیریهای آنها چه باید کرد؟

۶- پنهان نگاری (steganography) چیست؟ یک مثال بزنید.

۷ – یک ضرب المثل انگلیسی با استفاده از رمز playfair بصورت زیر درآمده است. کلید رمزنگاری trouble بوده است. ضرب المثل چه بوده است؟

WGWLOROUBTEADOUBOVROUBTDLRFCFLOUBTEAROUBTDDNXUAZ

۸- پیام WE ARE DISCOVERED SAVE YOURSELF را با استفاده از رمز HILL و کلید $\begin{bmatrix} 9 & 5 \\ 8 & 3 \end{bmatrix}$ **به رمز درآورید. محاسبات خود را نشان دهید.**

۹- عبارت " مزاحم نشوید" را به رمز درآورید:

الف- با استفاده از رمز Vigenere و کلید (چرا) .

ب - با استفاده از رمز Autokey و کلید (چرا) .

۱۰- مصرع اول بیت

" بیا به خلوت بی ماهتاب من بگذر به شام تار من ای آفتاب بگذر"

را با استفاده از رمز Railfence به رمز درآورید.

*****

***

*