بسمه تعالی

تکلیف سری اول درس امنیت شبکه

1. در این سوال قصد داریم با نحوه استفاده از نرم افزار Cryp Tool آشنا شویم. ابتدا نرم افزار را از لینک زیر دانلود کرده و سپس به قسمت­های مربوطه پاسخ دهید:

<http://www.cryptool.org/ct1download/SetupCrypTool_1_4_31_Beta6b_r3670_VS2008_en.exe>

الف) متن زیر را با استفاده از نرم افزار فوق با استفاده از روش سزار رمزنگاری کنید.

Cryptography is the practice and study of hiding information. Modern cryptography

intersects the disciplines of mathematics, computer science, and engineering

ب) متن زیر با استفاده از شیفت دادن حروف رمز شده است.با استفاده از نرم افزار فوق، عدد شیفت شدن حروف را بیابید و متن اصلی را نیز پیدا کنید.

Ocz adzgy ja izorjmf viy Diozmizo nzxpmdot xjindnon ja hzvnpmzn oj yzozm, kmzqzio,

yzozxo, viy xjmmzxo nzxpmdot qdjgvodjin ocvo diqjgqz ocz omvinhdnndji ja diajmhvodji.

1. در مورد مدهای کاری رمزهای متقارن به سوالات زیر پاسخ دهید:

الف) اگر IV استفاده شده در مد CBC همواره صفر باشد چه مشکلی بوجود می­آید؟

ب) تفاوت اصلی عملیاتی میان مد کاری CBC و CTR در حالت رمزگشایی و رمزنگاری چیست؟ در چه حالاتی مد CTR را به CBC ترجیح می­دهید؟

 3) نشان دهید الگوریتم DES خاصیت متمم گیری را داراست؟ برای این کار باید نشان دهید اگر C=E(K,P) آنگاه C’=E(K’,P’) .

 4) فرض کنید که مکان دقیق فیلد نمره در دیتابیس کارنامه دانشجویان دانشکده­ای برای ترودی معلوم باشد( مثلا بایت دهم از هر رکورد 100 بایتی) و از یک رمز قطعه­ای امن برای رمزنگاری دیتابیس استفاده شده باشد. اگر ترودی از نمره واقعی خود مطلع باشد، به سوالات زیر در دوحالت مدهای CBC و CTR پاسخ دهید:

 الف) آیا ترودی قادر است با دستکاری دیتابیس نمره خود را به 20 تغییر دهد؟ چگونه؟

 ب) اگر از CRC برای تشخیص تغییرات احتمالی محتوای دیتابیس استفاده شده باشد چطور؟

 ج)اگر از MAC برای تشخیص تغییرات احتمالی محتوای دیتابیس استفاده شده باشد چطور؟

 5) سه رمز زیر با استفاده از فرمول C=xP+y mod n برای زبان انگلیسی طراحی شده­اند. ابتدا رمزها را بررسی کرده و به سوالات مربوطه پاسخ دهید(سری به مسئله 23 از فصل دوم بزنید):

 رمز اول) با توجه به حروف زبان انگلیسی از پیمانه n=26 برای عملیات رمزنگاری استفاده شده است.

 رمز دوم) با توجه به کنار گذاشتن 7 حرف نادر از زبان انگلیسی، از n=19 برای عملیات رمزنگاری استفاده شده است.

 رمز سوم) به منظور خوانایی بهتر متون رمزگشایی شده، علایم " . ، : ؟ ! " به الفبای زبان انگلیسی افزوده شده است و از پیمانه n=31 برای عملیات رمزنگاری استفاده شده است.

 الف) برای هریک از سه رمز فوق محاسبه کنید دشمن به منظور دستیابی به مقادیر کلید x و y از طریق جست و جوی کامل فضای کلید، به طور متوسط( با در اختیار داشتن فقط متن رمز شده) باید چند عمل رمزگشایی انجام دهد؟

 ب) کدام یک از رمزهای فوق را از نظر امنیتی قابل توصیه می­دانید؟ چرا؟

 ج) آیا می­توانید رمز چهارمی را در همین چهارچوب پیشنهاد دهید که برتر از سه رمز فوق باشد؟ توضیح دهید؟