به نام خدا

محمدمهدی آقاجانی

۹۳۳۱۰۵۶

تمرین دوم

استاد : دکتر شهریاری

سوال ۱ :

الف) هر نفر باید n-1 کلید داشته باشد تا بتواند یک ارتباط بین اعضای دیگر برقرار نماید زیرا هر فرد باید با n-1 فرد دیگر ارتباط جداگانه داشته باشد. در نتیجه تعداد کل کلید ها برابر با n*(n-1)/2 می باشد.

ب) در فضای اینترنت از پروتکل SSL (Secure Socket Layer) استفاده میشود که مستقل از لایه application است بنابراین تمامی پروتکل ها میتوانند از آن استفاده کنند اما برای برخی پروتگل ها از جمله HTTP , FTP بهینه سازی شده است. در SSL از دو کلید عمومی و خصوصی استفاده میشود همچنین حالت متقارن در ای پروتکل از امنیت خوبی برخوردار نخواهد بود در نتیجه از حالت نامتقارن استفاده میگردد.

همچنین در این پروتکل عملیاتی ابتدایی به نام دست دادن وجود دارد که به صورت زیر است :

مرحله اول : برقراری ویژگی های امنیتی

این مرحله برای آغاز اتصال به کار میرود

مرحله دوم : احراز اصالت مبدا و تبادل کلید سرور

در این مرحله چندین پیام از سرور به کلاینت ارسال میگردد که پیام اول مربوط به گواهی سرور است در پیام بعدی کلید سرور تبادل میشود و پیام بعدی در صورت مخفی بودن سرور ارسال میگردد و همچنین یام نهایی هم به معنای اتمام این مرحله ارسال میگردد.

مرحله سوم : احراز اصالت و ارسال کلید کلاینت

در این مرحله نیز پیامی از کلاینت به سرور ارسال میگردد تا کلید مبادله گردد

مرحله ۴ : مرحله پایانی

طرفین با ارسال پیامی وضعیت رمز خود را اطلاع میدهند و سپس مرحله دست دادن به اتمام میرسد.

سوال ۲ :

الف) چون تعداد حروف انگلیسی ۲۶ تاست کلا ۲۶ حالت انتقال داریم در نتیجه فضای حالت برابر ۲۶ است

ب) امنیت این سیستم در برابر جست و جو ی کل فضای حالت بسیار پایین است در حالتی که فرد حمله کننده بداند در رمزنگاری از رمز سزار استفاده شده با امتحان کردن ۲۶ حالت میتواند رمز را بشکند.

پ) روش های حمله به رمز سزار مبتنی بر تحلیل های آماری زبان شناختی زبان انگلیسی ست که در واقع میزان تکرار حروف یا عبارت های پرتکرار در زبان انگلیسی را مشخص میکند. مثلا میدانیم که حرف e در انگلیسی پرتکرار ترین حرف است . کافی ست در متن رمز سزار به دنبال پرتکرار ترین حرف بگردیم و آن را معادل e فرض کنیم.

روش دیگر استفاده از ترکیب پرتکرار th است که میتوانیم به دنبال دو حرفی پرتکرار بگردیم و آن را معادل بگیریم و میزان شیفت را بدست آوریم.

ت) !26

سوال ۴ :

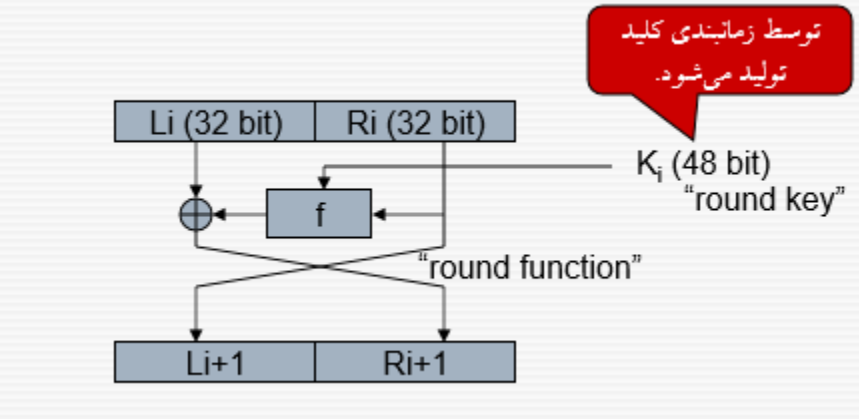
الف) برای اینکار کافی است v را بدست آوریم و اگر ۸۰ بیت اول v or c را داشته باشیم میتوانیم v را بدست آوریم در نتیجه چون v , c , k را داریم میتوان پیام m را بازیابی کرد :

$$m = RC4(v||k) \oplus c$$

ب) اگر مهاجم بفهمد که مقادیر v برای متون مختلف یکسان می باشند آنگاه میفهمد که کلیدها نیز یکسان هستند. وقتی کلید ها یکسان باشند آنگاه الگوریتم دیگر امن نخواهد بود.

سوال ۵ :

هر دور در رمز نگاری DES به صورت زیر است که در اسلاید ها نیز آن را داشتیم :



Plain text=01111111 L1=0111 , R1=1111

R2 : f(15,7) = $(2 * 1 * 7)^{15}$ mod 15 =$14^{15}\ mod\ 15 = (-1)^{15} mod\ 15 = 14$

f(15,7) = 1110

R2=1110 $\oplus$ 0111 = 1001

نتیجه مرحله اول: 11111001 : L2=1111 , R2=1001

R3: f(9,15)= $(2 * 2 * 7)^{9} mod\ 15 = (28)^{9} mod\ 15 = (-2)^{9} mod\ 15 = -512\ mod\ 15 = 13$

$f(9,7) = 1101$

R3= 1101 $\oplus 1111 = 0010$, $L3 = 1001$

نتیجه نهایی: 10010010