1. تگ‌های RFID دستگاه­های کوچکی هستند که قابلیت پخش کردن عددی را در هوای اطراف دارند که این اعداد توسط سنسورهای مربوطه که در نزدیکی محل عبور تگ­ها نصب شده­اند، دریافت و شناسایی می­شوند. یکی از کاربردهای سیستم­های RFID در شناسایی اقلام مختلف کالا در انبارها و گمرک­ها می­باشد. می­توان تگ­های RFID را در پول­های کاغذی نیز به کار برد تا بتوان از جعل کردن پول جلوگیری به عمل آورد.

الف) درباره مشکلاتی که پیرامون حریم شخصی (Privacy) در سیستم­های RFID وجود دارد، توضیح دهید.

ب) به نظر شما چه مشکلاتی علاوه بر حریم شخصی سیستم­های RFID را تهدید می­کند؟

2) راهی برای شکستن رمز Double Transpostion ارائه دهید.( سعی کنید متنی با حداقل 9 حرف که در ماتریسی به ابعاد 3\*3 قادر به جایگذاری می­باشد، رمز کرده و سپس راه خود را روی آن پیاده کنید)

3) در این سؤال قصد داریم تا با رمز Vigenere آشنا شویم. در رمز ویگنر، دنباله­ای از جابه­جایی حروف رخ می­دهد تا متن رمز شده بدست آید. در این رمز از کلید نیز استفاده می­شود. درباره رمز ویگنر تحقیق کرده و سعی کنید متن زیر را با کلید IUT رمز کنید.(فاصله­ها را درنظر نگیرید)

*The solution is by no means so difficult as you might be led to imagine from the first hasty inspection of the characters.*

4) فرض کنید کلیدهای عمومی آلیس و باب در فایلی بر روی سرور ذخیره شده است. آلیس و باب با استفاده از Authenticate با یکدیگر ارتباط برقرار کرده و قصد دارند پیامی خصوصی را رد و بدل نمایند. ترودی قصد دارد تا پیام محرمانه آلیس و باب را بخواند ولی نمی­تواند کلیدهای خصوصی آلیس و باب را پیدا کند و تنها می­تواند به سرور نفوذ کرده و فایل حاوی کلیدهای عمومی آلیس و باب را تغییر بدهد.

الف) ترودی چگونه می­تواند فایل را تغییر دهد تا بتواند پیام خصوصی آلیس و باب را بخواند؟

ب) آیا آلیس یا باب می­توانند از دستکاری فایل توسط ترودی مطلع شوند؟ توضیح دهید.

5) سیستم OTP(One Time Pad) ای را در نظر بگیرید که از کلیدی 128 بیتی برای رمزنگاری استفاده می­کند و برای پیام­هایی با طول بیشتر از 128 بیت، از همان کلید به صورت پی­در­پی استفاده می­شود. توضیح دهید که چرا این سیستم می­تواند مورد حمله قرار گیرد و بشکند؟

6) فرض کنید پیامی با 1024 بیت طول دراختیار دارید. روشی پیشنهاد دهید که بتوان کلیدی 64 بیتی را به کلیدی 1024 بیتی گسترش داد و سپس کلید بدست آمده را با پیام XOR کرد( مانند روش OTP ). آیا متن رمز شده بدست آمده به اندازه متنی که در روش OTP بدست می­آید امن است؟ آیا هیچ متن رمزشده­ای می­تواند مانند متن OTP امن باشد؟ جواب­های خود را توضیح دهید.

7) در کلاس حل تمرین مختصری درباره Forward search attack صحبت شد:

الف) درباره این حمله و چگونگی انجام آن توضیح داده و مثالی بزنید.

ب) چگونه می­توان از این حمله در سیستم­های کلید عمومی خصوصی جلوگیری کرد؟

ج) چرا نمی­توان این حمله را برروی سیستم­های متقارن انجام داد؟

8) در رمز قطعه­ای DES و در مرحله آخر، یک جا­به­جایی میان بیت­های سمت چپ و راست رخ می­دهد زیرا متن رمز شده به جای آنکه C=(L16,R16) باشد، به صورت C=(R16,L16) است. چرا این جا­به­جایی در مرحله آخر لازم است؟ توضیح دهید.

9) فرمول روش CTR به صورت زیر است:

Ci= Pi xor E(IV+i,K)

اگر فرمول بالا را به صورت Ci= Pi xor E(K,IV+i) تغییر دهیم مشکلی ایجاد خواهد شد یا خیر؟ درهر صورت جواب خود را اثبات کنید.

10)در این سوال قصد داریم روش CBC و معایب و مزایای آن را بررسی کنیم. در همه قسمت­های این سوال فرض برآن است که 4 بلاک متن به صورت P1,P2,P3,P4 در اختیار داریم. آلیس برای رمز این 4 بلاک از روش CBC استفاده کرده و با استفاده از IV و K ، 4 بلاک رمز شده به صورت C1,C2,C3,C4 بدست آورده است. به سوالات زیر پاسخ دهید:

الف) فرض کنید باب ابتدا بلاک­های رمز شده را با استفاده از کلید از رمز درمی­آورد و سپس آنها را دوباره با روش CBC و IV ، رمز می­کند. اگر در این حالت بلاک آخر رمز شده توسط باب با بلاک آخر ارسال شده توسط آلیس برابر بودند، باب بر integrity پیام مطمئن می­شود. اگر ترودی مقدار C1 را به X تغییر دهد، آیا باب متوجه دستکاری ترودی می­شود؟ اگر ترودی مقدار C3 را به Y تغییر دهد، در این حالت باب می­تواند متوجه دستکاری شود؟ جواب­های خود را توضیح دهید.

ب) فرض کنید ترودی قادر است هریک از بلاک­های رمز شده را قبل از آنکه به باب برسد، تغییردهد. نشان دهید اگر ترودی P1 را بداند، می­تواند این قطعه­ را با X طوری جایگذاری و سپس رمز کند، که باب متوجه نشود و به جای P1 قطعه X به دست باب برسد.

ج) فرض کنید آلیس تصمیم می­گیرد تا MAC پیام را به شکل KxorX محاسبه کند که X مقداری ثابت است و MAC و قطعات رمز شده را به باب می­فرستد. نشان دهید باب می­تواند متوجه حمله cut-and-paste شود.

د) فرض کنید آلیس MAC پیام را با کلید K’ حساب کرده و سپس پیام را با کلید K رمز می­کند و قطعات رمز شده را بدست آورده و آنها را همراه با MAC و IV به باب ارسال می­کند. ترودی پیام ارسال شده را دستکاری کرده و C1 را با X عوض می­کند و سپس محتوا را به باب ارسال می

­کند. باب برای آنکه integrity پیام را بررسی کند، ابتدا محتوا را با کلید K از رمز درآورده و سپس با کلید K’ ، MAC را محاسبه می­کند. نشان دهید که باب می­تواند از دستکاری ترودی مطلع شود.