به نام خدا

محمدمهدی آقاجانی

۹۳۳۱۰۵۶

تمرین سوم

استاد : دکتر شهریاری

سوال اول

الف)

۱- ابتدا طرف اول اعداد a , g , p را به دلخواه انتخاب میکند که p یک عدد اول بزرگ است

۲- سپس $A = g^a \bmod p$ را محاسبه میکند و g,p,A را برای طرف مقابل میفرستد.

۳- طرف دوم عدد b را به طور دلخواه انتخاب میکند.

۴- مقدار $B = g^b \bmod p$ را محاسبه میکند

۵- طرف دوم مقدار $K = A^b \bmod p$ را محاسبه کرده و B را به طرف اول ارسال میکند

۶- طرف اول مقدار $K = B^a \bmod p$ را محاسبه میکند

مقدار K به عنوان کلید دو طرف استفاده میگردد. در این الگوریتم از این موضوع که حل مساله لگاریتم گسسته سخت می باشد استفاده شده است

ب) بله. ابتدا همه باید روی q و a توافق کنند .حال باید هر شخص کلید خود را برای تمامی طرفین ارسال نماید:

Yn=a^Xn mod q

برای به دست آوردن کلید مشترک دیگر اعضا،n-1 مقدار Yرا از سایرین دریافت و کلید عمومی را به صورت زیر می سازد

K=(YaYb..Yn)^Xn mod q:

و کلید مشترک: a ^ (XaXb…Xn) mod q

ج) چون در نمونه اولیه این پروتکل شناسایی دو طرف وجود ندارد فرد مهاجم میتواند رد میان قرار گیرد و با هر طرف به طور جداگانه کلید مبادله کند و برای ارتباط پیام را با کلید طرف اول رمزگشایی کرده و با کلید طرف دوم رمزگذاری نماید.

سوال دوم

۱. این گزینه مقاوم می باشد زیرا مثلا اگر g مقاوم نباشد میتوان a و b را با خروجی یکسان پیدا کرد اما برای f که مقاوم است این کار سخت است درنتیجه حاصلی که از concat این دو تابع بدست می اید نیز برای دو مقدار a و b متقاوت است

۲. این گزینه میتواند مقاوم نباشد فرض کنید که g مقاوم نباشد در این صورت اگر a , b برای این تابع خروجی y بدهند آنگاه f(y) حاصل خروجی کلی a , b خواهد بود که یعنی خروجی کلی این دو مقدار با هم برابر است و این تابع مقاوم نمی باشد.

۳. این گزینه نیز مقاوم است زیرا اگر یکی از دو تابع مقاوم باشد آنگاه تنها یکی از جملات این تابع ترکیبی مقاوم نخواهد بود و دیگری مقاوم است و به دلیل آنچه در قسمت اول گفته شد این تابع نیز مقاوم است

سوال سوم

الف) بعد از اینکه تمام کلمات متن را به هم چسبانده و ۸ تا ۸ تا جدا میکنیم باید بر اساس کلید داده شده از هر کلمه i امین حرف را انتخاب کنیم که به متن زیر میرسیم :

He sitteth between the cherubims. The isles may be glad thereof. As the rivers in the south.

ب) چون کلید را نمیدانیم د رواقع مشخص نخواهد شد که باید چه حروفی را انتخاب نماییم مگر اینکه هر ۸ حرف را جدا کنیم و تمام حالات را بررسی نماییم و ببینیم که کدام جمله معنی میدهد که اگر تعداد حروف زیاد باشد کار سخت است همچنین اینکه بفهمیم آیا جمله معنی میدهد یا نه هم کار دشواری ست پس از امنیت خوبی برخوردار است

ج) در این حالت نمیتوان گفت که روش ، امن میباشد . زیرا با بررسی کلید ممکن است فرد مقابل حدس بزند که این اعداد ، اعدادی بین ۱ تا ۸ هستند و بفهمد که باید متن را به قسمت های ۸ تایی تبدیل کند.

سوال چهارم

الف) ماتریس m3 به صورت زیر خواهد بود :

۵	۲	۴	۱	۵
۱	۴	۲	۳	۲
۳	۱	۵	۲	۳
۴	۳	۱	۴	۴
۲	۵	۵	۵	۱

ج) دو شرط مهم برای این که این روش امن باشد این است که اعداد داخل ماتریس های اولیه باید کاملا تصاوفی انتخاب شده باشند و دوم ، باید ماتریس ها دارای اندازه برزرگ باشند

سوال پنجم

۴,۷)

a) این بدان معناست که a خود را به روی b میخواهد authenticate کند و برای این کار id خود را به b میفرستد و b هم یک مقدار رندم r2 را با کلید عمومی a رمز میکند و برای او میفرستد سپس a آن را با کلید خصوصی خود باز کرده و r2 را خوانده و آن را به b میفرستد.

b) اگر فردی مانند c بین راه بنشیند میتواند خود یک پیام r2 تولید کرده و نقش b را بازی کند در این صورت دیگر a پیام های خود را به c میفرستد

۴,۸)

شامل آیدی alice و اسم bob و timestamp میباشد که توسط KDC-Bob secret key رمزگذاری شده است

۴,۹) شامل نام Alice میباشد که با KDC-Bob secret key رمزگذاری شده است

۴,۱۰) با استفاده از nonce مانند timestamp که با session key رمزگذاری شده است

۴,۱۱) شامل session key می شود که با KDC-Bob secret key رمزگذاری شده است.

سوال ششم

$$d.e \ mod \ \varphi(n) = 1$$
$$132111 * d \ mod \ (838)(982) = 1$$
$$132111 * d \ mod \ 822916 = 1$$
$$132111 * d = 822916 * k + 1$$
$$d = 26959$$

برای امضا کردن هم به صورت زیر عمل میکنیم :

$$23547^{26959} \ mod \ 824737 = 331823$$