# به نام خدا

# محمدمهدی آقاجانی

# 9331056

# تمرین سوم

# استاد : دکتر شهریاری

سوال اول

الف)

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

2- سپس A = ga mod p را محاسبه میکند و g,p,A را برای طرف مقابل میفرستد.

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

4- مقدار B = gbmod p را محاسبه میکند

5- طرف دوم مقدار K = Ab mod p را محاسبه کرده و B را به طرف اول ارسال میکند

6- طرف اول مقدار K = Ba mod 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) از آنجایی که وقتی B یا A به طرف مقابل میرسد تنها میتواند این مقادیر را به توان عددی که خودتولید کرده برساند لذا باید همیشه این مقادیر توسط بقیه به تان رسیده باشند تا این طرف با به توان رساندن به مقدار خود کلید را تولید نماید اما چنین چیزی ممکن نیست در نتیجه نمیتوان آن را به بیش از دو طرف تعمیم داد

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