سوال 1) برای آنکه در سیستم RSA سرعت بالا رود، می‌توان برای تمامی کاربران از e=3 استفاده کرد. حمله­ای به نام cube root برای سیستم بالا وجود دارد. درباره این حمله توضیح داده و در حالتی که (N,e)=(33,3) ، حمله فوق را برروی سیستم گفته شده انجام دهید.

سوال 2) در الگوریتم تبادل کلید دفی-هلمن، امکان حمله man in the middle وجود دارد. دیاگرامی برای تبادل کلید میان آلیس و باب رسم کرده و سعی کنید نقص الگوریتم فوق را به راه حل خود برطرف سازید.

سوال 3) پروتکل زیر را در نظر گرفته و به سوالات داده شده پاسخ دهید:

الف) آلیس مقدار S=[M]Alice  را محاسبه می­کند.

ب) آلیس (M,S) را به سمت باب می­فرستد.

ج) باب V={S}Alice  را محاسبه می­کند.

د) اگر باب به رابطه V=M برسد، متوجه می­شود که آلیس در سمت دیگر است و مکالمه را قبول می­کند.

1. نشان دهید ترودی می­تواند به راحتی خود را به جای آلیس جا بزند.
2. پروتکل بالا را به نحوی تغییر دهید که مشکل قسمت قبل حل شود.

سوال 4) روش­های MAC و HMAC را توضیح داده و کاربردها، مزایای و معایب هرکدام را بیان کنید.

سوالات 22 و 27 از فصل Hash Functions ++ را نیز حل کنید.

مهلت ارسال تکالیف تا ساعت 23:59 روز چهارشنبه می­باشد.

باتشکر