مبانی رایانش امن، تمرین دوم،

فصل زمستان سال یک‌هزاروسیصدوچهارصد

دانشکده علم رایانه و فناوری اطلاعات،دانشگاه تحصیلات تکمیلی علوم پایه زنجان

۱- جعبه سین و جعبه دال بررسی شود.

۲- ضعف‌های ارد مطرح شده در درس را بررسی کنید.

۳- ارد را پیاده کنید.

۴- یک مورد از سه مورد زیر را انجام دهید

a. یک مورد از روش‌های بلوک‌بندی را پیاده کنید و نتایج را گزارش و تحلیل کنید.

b. RC۴ را پیاده کنید.

c. انسی X۹.۱۷ را پیاده کنید. از ارد به جای س‌ارد استفاده کنید.

۵- تحقیق کنید. که امروزه چه روش‌های رمز دنباله‌ای به جای RC۴ استفاده می‌شود. چند نمونه از پروتکل‌ها و محل‌های استفاده از هر یک را توضیح دهید.

کپی و سرقت از دیگران موجب رد شدن دانشجو خواهد شد

پیاده‌سازی نیاز به گزارش مستندسازی جداگانه و افزودن توضیحات در خود کد دارد.

انجام تمرین در قالب گروه‌های تک یا دونفره است.

در صورت پاسخ دو نفری، میزان مشارکت هریک و چه بخش‌هایی را پاسخ داده است مشخص شود.

مهلت ارسال: تا آخر بهمن ۱۴۰۰

نحوه ارسال

ا-نامه: amniat.iasbs@gmail.com

عنوان: امنیت- تمرین دو

فایل متنی: قالب پی‌دی‌اف: MRA-T-2-namKhanevadeghi-Nam.pdf

MRA-T-2-namKhanevadeghi-Nam.zip