مبانی رایانش امن

تمرین اول

فایل‌های پاسخ خود را با الگوی HW1-9431XXX-StudentName.pdf نامگذاری نمایید.
در صورت مشاهده تقلب برای طرفین نمره صفر درنظر گرفته خواهد شد.
در صورت وجود هرگونه اشکال یا سوالی از طریق ایمیل alireza97hi@gmail.com موارد را بیان کنید.

۱.تفاوت Threat و Attack را بیان کرده و در رابطه با هرکدام یک مثال بیاورید.

۲.در رابطه با موارد زیر نوع بعد امنیتی مربوطه را مشخص کنید.
الف) دسترسی به اطلاعات خصوصی شرکت سونی و افشای آن (۲۰۱۴)
ب) در دسترس نبودن سایت ایران کنسرت برای افراد ثبت‌نام شده در سایت (۱۳۹۷)
ج) تغییر محتوای اخبار و انتشار اخبار جعلی در سایت روزنامه قانون (۱۳۹۷)
د) در دسترس بودن اطلاعات ثبت‌نامی تمامی دانشجویان دانشگاه امیرکبیر

۳.یکی از سیستم‌های زیر را انتخاب کرده و ابعاد امنیتی آن شامل Integrity، confidentiality و availability را بیان کنید.
الف) سامانه فروش آنلاین بلیط سینما
ب) سامانه فروش آنلاین بیمه
ج) سایت سنجش

۴.برای انواع حملات زیر یک نمونه مثال بزنید و یک مکانیزم امنیتی بیان کنید.
الف) masquerade
ب) DOS
ج)Replay

۵.با کمک الگوریتم feistel متنی را رمز کرده‌ایم. تعداد دورها ۴ بوده و کلید و متن رمز شده و round function به صورت زیر است. پیام اصلی را محاسبه کنید.

Cipher text = ۱۱۱۰۰۰۱۰۰۰
Round function(x,k) = x + k
K = 00001

۶.فرض کنید ریک بخواهد پیامی با کمک الگوریتم RC۴ برای مورتی ارسال کند. آن‌ها بین یکدیگر با کلید k به طول L_k به توافق رسیده‌اند و هر دو این کلید را دارند. اگر طول V را با L_v و پیام اصلی را باm نشان دهیم و متن رمز شده به صورت زیر باشد و پیام ارسالی را به صورت (c || v) به مورتی بفرستد آنگاه مورتی چگونه پیام را رمزگشایی می‌کند؟

C = RC4(v || k) + m

۷.الف) پیام اصلی به صورت Plain Text در زیر آمده است. با کمک تابع تعریف شده و مقدار I V مشخص شده متن رمز شده را با هر دو روش ECB و CBC بدست آورید(بلوک‌ها را به صورت ۵ بیتی در نظر بگیرید):

Plain Text = 010000110001001
IV = 10110
E(k,Pi) = k XOR Pi

ب) مزیت‌های روش CTR را بیان کنید.