Exercise 2

۱. با استفاده از کتابخانه ای hashlib در زبان برنامه نویسی پایتون، اقدام به اجرای تابع درهم ساز SHA256 و MD5 بر روی متن زیر کنید.

"If you want to keep a secret, you must also hide it from yourself"

هربار خروجی تابع درهمساز را ثبت کنید، در ادامه اقدام به حذف یکی از حروف متن فوق کنید و مجددا تابع درهمساز را بر روی متن جدید اعمال کنید، بررسی کنید به ازای تغییر یک حرف، چند بیت از خروجی تابع درهمساز تغییر کرده است.

۲. با استفاده از کتابخانه های موجود در زبان برنامه نویسی پایتون اقدام به رمزنگاری و سپس رمزگشایی شماره دانشجویی خود کنید.

۳. متن زیر توسط الگوریتم سزار رمز شده است.به کمک نرم افزار cryptool مشخص کنید که برای رمز کردن این متن از چه کلیدی استفاده شده است و پس از یافتن کلید، متن واضح را بدست آورید(ز قسمت آنالیز این ابزار استفاده کنید)

Jxu Squiqh Syfxuh jusxdygku yi edu ev jxu uqhbyuij qdt iycfbuij cujxet ev udshofjyed jusxdygku. Yj'i iycfbo q jofu ev ikrijyjkjyed syfxuh, y.u., uqsx bujjuh ev q wylud junj yi hufbqsut ro q bujjuh iecu vynut dkcruh ev feiyjyedi temd jxu qbfxqruj. Veh unqcfbu myjx q ixyvj ev 1, Q mekbt ru hufbqsut ro R, R mekbt rusecu S, qdt ie ed. Jxu cujxet yi qffqhudjbo dqcut qvjuh Zkbyki Squiqh, mxe qffqhudjbo kiut yj je secckdysqju myjx xyi evvysyqbi. Jxki je syfxuh q wylud junj mu duut qd ydjuwuh lqbku, ademd qi ixyvj mxysx ydtysqjui jxu dkcruh ev feiyjyed uqsx bujjuh ev jxu junj xqi ruud celut temd.

توضیح دهید این ابزار چگونه بدون داشتن کلید به متن اصلی دست میابد.

۴. یک محیط آزمایشگاهی برای خود بسازید که شامل یک سیستم به همراه ابزار NMAP و دو سیستم عامل دیگر باشد، این سه سیستم را به نحوی آماده کنید که یکدیگر را PING کنند. مراحل زیر و اسکن های گفته شده را انجام دهید(پیش از شروع اسکن شبکه، ابزار وایرشارک را باز کنید تا بسته های اسکن را در شبکه رصد کنید):

- با دستور nmap –h با این ابزار بیشتر آشنا شوید.
- Tcp full scan
- Stealth scan
- Udp scan
- fingerprint scan
- idle scan

گزارش کاملی از نحوه‌ی انجام تمرین فوق تهیه کنید. از هر مرحله عکس گرفته و توضیحات تکمیلی را در ادامه بنویسید. در نامگذاری فایل حتما شماره دانشجویی خود را ذکر کنید.