تمرین عملی اول

۱.با استفاده از کتابخانه‌ی 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 اجرای تابع رمزنگاری DES کنید، در این تمرین دانشجویان محترم میبایست متن و کلید معرفی شده در سوال ۵ تمرین اول را در نظر گرفته و تابع DES را بر روی آن نشان دهند.

M= 0123456789ABCDEF

Key= 133457799BBCDFF1

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.(از 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.

توضیحات: تمرین اول و دوم به صورت حضوری در تاریخ ۱۵ آبان تحویل گرفته میشود، مضافا اینکه دانشجویان موظفند گزارش کتبی از سه تمرین ذکر شده را تا تاریخ ذکر شده بر روی سایت وب آموز برگزاری کنند.