به نام خدا

امنیت شبکه | تمرین سری اول | زمان انتشار: ۳۰ مهر ۹۵

دستورالعمل تحویل تمرین‌ها:

لازم است به غیر از تمرین شماره‌ی ۱؛ سایر تمرین‌ها را از طریق پست الکترونیک net.sec.iauk@gmail.com با موضوع

NS-EX-1-8888888

که 8888888 برابر با شماره‌ی دانشجویی شما است؛ ارسال فرمایید. همچنین می‌توانید سوالات نوشتاری را به صورت نسخه‌ی دستی؛ در کلاس تحویل دهید.

۱- متن زیر با استفاده از رمز سزار یا Shift به ازای K محرمانه‌ای رمز شده است.

amvl iv muiqt EqBp Bpm ACjrmkB Va-XMf-1-888888 Bw vmB.Amk.qiCs .iB. ouiqt.kwu Epmzm 888888 qA GwCz ABClmvB vCujmz

دستورالعمل تحویل این تمرین؛ شامل ارسال یک ایمیل با موضوع مشخص به یک آدرس پست الکترونیک است. برای رمزگشایی این متن با استفاده از جستجوی کلید فراگیر یا تحلیل فرکانس؛ می‌توانید از ابزارهای آنلاین مانند CryptoTool در آدرس http://www.cryptool-online.org استفاده نمایید.

الگوریتم رمز سزار

http://www.cryptool-online.org/index.php?option=com_content&view=article&id=48&Itemid=95&lang=en

تحلیل آماری

http://www.cryptool-online.org/index.php?option=com_content&view=article&id=96&Itemid=117&lang=en

۲- متن رمز شده‌ی زیر با استفاده از الگوریتم رمزنگاری جایگذاری (Substitution) و با کلیدی محرمانه رمز شده است. متن واضح معادل با آن را با استفاده از تکنیک تحلیل آماری به دست آورید.

lrvmnir bpr sumvbwvr jx bpr lmiwv yjeryrkbi jx qmbm wi bpr xjvni mkd ymibrut jx irhx wi bpr riirkvr jx ymbinlmtmipw utn qmumbr dj w ipmhh but bj rhnvwdmbr bpr yjeryrkbi jx bpr qmbm mvvjudwko bj yt wkbrusurbmbwjk lmird jk xjubt trmui jx ibndt

wb wi kjb mk rmit bmiq bj rashmwk rmvp yjeryrkb mkd wbi iwokwxwvmkvr mkd ijyr ynib urymwk nkrashmwkrd bj ower m vjyshrbr rashmkmbwjk jkr cjnhd pmer bj lr fnmhwxwrd mkd wkiswurd bj invp mk rabrkb bpmb pr vjnhd urmvp bpr ibmbr jx rkhwopbrkrd ywkd vmsmlhr jx urvjokwgwko ijnkdhrii ijnkd mkd ipmsrhrii ipmsr w dj kjb drry ytirhx bpr xwkmh mnbpjuwbt lnb yt rasruwrkvr cwbp qmbm pmi hrxb kj djnlb bpmb bpr xjhhjcwko wi bpr sujsru msshwvmbwjk mkd wkbrusurbmbwjk w

jxxru yt bprjuwri wk bpr pjsr bpmb bpr riirkvr jx jqwkmcmk qmumbr cwhh urymwk wkbmvb

برای انجام تحلیل آماری می‌توانید از ابزارهای سوال قبل نیز استفاده نمایید. همچنین جدول فراوانی حروف الفبای انگلیسی در ۱,۱ کتاب آمده است.

۳- تمرین 1.9 کتاب Understanding Cryptography

۴- تمرین 1.13 کتاب Understanding Cryptography