تکلیف سری اول مبانی رمزنگاری

۱- تمرین زیر از کتاب درسی را حل کنید.

تمرین فصل یک:

1.7, 1.8, 1.9, 1.10, 1.13

تمرین کریپتول

1- CrypTool" is an open-source widespread e-learning software which illustrates cryptographic and cryptanalytic concepts. Download it and do the following exercises using this helpful cryptology tool. For each part, put the output of the software in your answer file.

a. Encrypt your full name using the Caesar cipher with key = 'M' (to do so select Crypt/Decrypt > Symmetric (classic) > Caesar). how many letters is the alphabet shifted by?

2- Encipher the following quote using the substitution cipher, use the given cipher alphabet as the key and the remainder of your student number divided by 26 as the offset. (to do this exercise select Crypt/Decrypt > Symmetric (classic) > Substitution/Atbash).
Plain text: Success usually comes to those who are too busy to be looking for it.

Cipher alphabet: fharjolyinectzspdbkwxgumvq

3- Vigenere" Cipher is a method of encrypting alphabetic text. by using a series of interwoven Caesar ciphers, based on the letters of a keyword. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution. The encryption of the original text is done using the Vigenère square or Vigenère table. First described by Giovan Battista Bellaso in 1553, the scheme was misattributed to Blaise de Vigenère (1523–1596) in the 19th century, and so acquired its present name. (To encipher your text using this method select Crypt/Decrypt > Symmetric (classic) > Vigenère)

a. Derive a biliteral key by concatenating the first letters of your first name and family name and encrypt the plain text used in the previous question using the Vigenere Cipher with this key.
b. Encrypt the same text using the same algorithm, but this time, generate the key by concatenating your full first name with your last name.
c. Compare the results of previous parts by analyzing their entropy. What do you think the entropy is? According to this measure, how does the key length affect the cipher text? Explain your reasons. (to do this exercise you can use Analysis > Tools for Analysis > Entropy)

4- Decipher the following cipher text, enciphered with Vigenere cipher, using CrypTool analytical tools, what do you guess the drawn diagram is? (To break the cipher select Analysis > symmetric Encryption (classic) > Ciphertext-only > Vigenere)

Cipher text: udgaxgat tw nqzj jdqftfdq iyh wmaj xg gap qswqyk af qoisx nzv lqinlazo aigbtp etace gjkxesydialq ub lpka kzrlmqyw kqdpvsx lpqgzaevsfqzr wjixtdqa elsf ici vqatkfql es tq dpvq qidc la nzpdae lrv nzpec pwhr ltm xeltmxelukd mffw dqsxt xefmopetxm dxwba.

5- In cryptography, the one-time pad is an encryption technique that cannot be cracked, but requires the use of a one-time pre-shared key the same size as, or longer than, the message being sent. In this technique, a plaintext is paired with a random secret key. Answer the following questions regarding this encryption technique.

a. With the help of Cryptool, encrypt the following plaintext using the given key as one time pad. (to do this exercise select Crypt/Decrypt > Symmetric (classic) > OTP)

Plaintext: Today, Internet service providers (ISPs) try to deliver more and more value-added services integrated with their residential Internet access offer, such as triple-play (voice, Internet, and video). This situation generates the need for more powerful and expensive home devices to cover these needs. This device receives different names, from customer premise equipment (CPE) to residential router and to home gateway (HGW), but all have a common ground: the trade-off between low-cost and rich functionalities, with a potentially negative effect on the device security. As a result, vHGW was one of the first scenarios that were adopted within the NFV paradigm, to demonstrate its potential in terms of efficiency and security. In this chapter, we are going to describe the NFV architecture that Telefonica designed and implemented in a commercial trial, to evaluate its potentiality.

OTP Key: Thksp, Afuqfgwj abnqkku xdhsqlbfo (TYTd) jom th kifbxdy sevo kxr atlj wedxe-utpxk yehxmtsb gfuqyzfbjo smpx trwul vmnqlbjqcsp Nfuqfgwl qxarge otlru, evsf ed teqjoi-fswi (zhwte, Kuqqeyeb, fbb lqlbm). Iwsh yoxbwdpif lstjhrcqq npd cgoh dpq sevq thouvnzg oes igmgfzmxz tcva vnxmtqq ne hqxdy xkiui vgohc. Ykqw fadxms dgdqmxzi vjfwedryj seofc, vuyc towrfagz zsqqzqg bugijwknz (NES) nv vmnqlbjqcog osodqr lzd fa tbcr sshdgtc (ZEX), fbq imw vbmq v quhgif lpipzd: fvx urhga-kjd cqlupmm ecp-yeej oes hwfd oufliysvspnrcfy, zeto w tbsuecccfpp iebsvlei mnjgbd xo xki hfmwte wtokvnvi. Xw k tepqbv, vZEX azk ghf ee whl eypbh cvoxxtkpc ykkp funx uvdnckd exbguv rzg SMF ksrhggfq, th kirqnnmhrcy sru xrlzsngth ne pveeb az dklapguzsf wle cwnmlfeu. Ar bgua ejsyimv, zs gjs nikhd th kmhotxcy uag SMV jkydtnklxxiy uaus Wejpztesxs riduetwz bbo ygcaybmfuqb hc a dgehoxmpqe ufyzh, ca slznihte dhp iwlnjqcspnhj.U

b. Use your full name as the OTP key and encrypt the same plaintext with the same algorithm. (don't forget to write the key in your answer file)
c. Try to find the OTP key of each of the two cipher texts in the previous parts using the Cryptool analytical tools and put the results, especially the predicted length of the key, in

your answer file; Compare the security of the keys based on the results of analysis. (To do this part select Analysis > Symmetric Encryption > cipher text only > XOR)

6-

In classical cryptography, the *Hill* cipher is a polygraphic substitution cipher based on linear algebra. This cipher is vulnerable to a known-plaintext attack because it is completely linear. Suppose we have somehow obtained a plaintext-ciphertext pair that we know is enciphered using the Hill cipher. Knowing this, make use of CrypTool analytical tools to decipher the given secret message which is encrypted using the same key and algorithm.

Plain text: One characteristic of processes that do not leak information comes from the observation that a process must store data for later retrieval. A process that does not store information cannot leak it. However, in the extreme, such processes also cannot perform any computations, because an analyst could observe the flow of control or state of the process and from that flow deduce information about the inputs. This leads to the observation that a process that cannot be observed and cannot communicate with other processes cannot leak information. Lampson calls this total isolation.

Cipher text: Ojg idgrihcyczqcje pm htakrxanf nbej nu tch zocg fodslqhsqdw gfxop gvyy dzo qmfycmyansa glsj a ikolrev lirk omlry tset dsl pelie cmoscbokc. A mhqmopt nbej nuul aay trifa nydslqhsqdw itytch zoce pq. Hchvzqr, mi qla kftvyfb, uxph dholryzrq doit tgakog smkyyeb yof gfxhmryanoux, xwconhk zm gaxhomh imiqs qmfycmy ggm miqp ht ssvpdum xf ipicd cm udo fhqmopt ssy xpig ekmi mdou dizudh icuyebyanuq rlykn zha nyhmrs. Turk qnggb zu xzi whacnnytmih hrse t htakrxm waaq lgakka wq xqwhwvkv ssy itytch gfxgtusvrro wcsi ikyas khqmoptcx fgakyi iyhl icuyebyanuq. Lrqyzcc juecm wawh egunb moqgbtmin.pt

Secret message: ipp tebw blcblcfaommm bciozxvex dzk jxgybn ycibhqt.k

از طریق ایمیل زیر برای هر گونه ابهام و سوال در مورد تمرینات با من ارتباط برقرار کنید .

Gelare71oudi@gmail.com