Understanding Cryptography

Homework No.1 **Due Date: 98.11.12**

1. Solve the following exercises in your textbook " Understanding Cryptography":

Exercise 1.5, 1.7, 1.8, 1.9, 1.10, 1.13

2.

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.

- **Encryption/Decryption**

    1. Encrypt your full name using the Caesar cipher with key = 'G' (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 first digit of your student number as the offset (to do so select *Crypt/Decrypt > Symmetric (classic) > Substitution/Atbash*)**.**
       Plain text: If you cannot explain it to a six year old you do not understand it yourself.
       Cipher alphabet: qhpgiuwaeylnofdxjkrzvstcmb

    3. *Vigenere* Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the *Vigenère square or Vigenère table*.
       (To encipher your text using this method select *Crypt/Decrypt > Symmetric (classic) > Vigenère*)
       i Encrypt the plain text used in the previous question using the Vigenere Cipher with key = 'iut'.
       ii Encrypt the same text using the same algorithm with the key = 'isfahanuniversityoftechnology'.
       iii Compare the results of previous parts. How does the key length affect the cipher text? Explain your reasons.

4. The *Playfair* cipher was the first practical digraph substitution cipher. In this cipher, unlike traditional ciphers we encrypt a pair of alphabets (digraphs) instead of a single alphabet.
   (To encipher your text using this method select *Crypt/Decrypt* > *Symmetric (classic)* > *Playfair*)

   i Encrypt the plain text in used in the question 2 using the Playfair Cipher, select the 6x6 key Matrix and use your full name, without space, concatenated with your student number as your key phrase.

   ii Decrypt the resulting cipher text using the same method and key.

- **Analysis**

1. The two following cipher texts are enciphered using substitution cipher, which one of them is better deciphered, using Cryptool analytical tools, in terms of simililarity to the written language? What is the reason for that?
   (To break the cipher select *Analysis* > *symmetric Encryption (classic)* > *Ciphertext-only* > *Substitution*)

   i tk whmdvjrhqdum, q gbpgvtvbvtjk wtdueh tg q sevujo ji ekwhmdvtkr pm nutwu bktvg ji dlqtkvezv qhe hedlqweo ntvu wtduehvezv, qwwjhotkr vj q itzeo gmgves; vue "bktvg" sqm pe gtkrle levvehg (vue sjgv wjssjk), dqthg ji levvehg, vhtdlevg ji levvehg, stzvbheg ji vue qpjce, qko gj ijhvu. vue hewetceh oewtduehg vue vezv pm dehijhstkr vue tkcehge gbpgvtvbvtjk. gbpgvtvbvtjk wtduehg wqk pe wjsdqheo ntvu vhqkgdjgtvtjk wtduehg. tk q vhqkgdjgtvtjk wtdueh, vue bktvg ji vue dlqtkvezv qhe heqhhqkreo tk q otiiehekv qko bgbqllm fbtve wjsdlez jhoeh, pbv vue bktvg vuesgelceg qhe leiv bkwuqkreo. pm wjkvhqgv, tk q gbpgvtvbvtjk wtdueh, vue bktvg ji vue dlqtkvezv qhe hevqtkeo tk vue gqse gefbekwe tk vue wtduehvezv, pbv vue bktvg vuesgelceg qhe qlveheo. vuehe qhe q kbspeh ji otiiehekv vmdeg ji gbpgvtvbvtjk wtdueh. ti vue wtdueh jdehqveg jk gtkrle levvehg, tv tg vehseo q gtsdle gbpgvtvbvtjk wtdueh; q wtdueh vuqv jdehqveg jk lqhreh rhjbdg ji levvehg tg vehseo djlmrhqdutw. q sjkjqlduqpevtw wtdueh bgeg itzeo gbpgvtvbvtjk jceh vue ekvthe seggqre, nueheqg q djlmqlduqpevtw wtdueh bgeg q kbspeh ji gbpgvtvbvtjkg qv otiiehekv djgtvtjkg tk vue seggqre, nuehe q bktv ihjs vue dlqtkvezv tg sqddeo vj jke ji gecehql djggtptltvteg tk vue wtduehvezv qko ctwe cehgq.

   ii ycegklng egu eqytjejkfyc iuzskqt muegkt vkq bquyejfn y mjdut wlhwejelejkf ycpgyhue jw wjmpcu, y wuqjklw tjwytayfeynu jw egye egu cywe cueeuqw kv egu ycpgyhue (sgjbg yqu mkwecz cks vquolufbz) euft ek weyz ye egu uft. y weqkfnuq syz kv bkfweqlbejfn y mjdut ycpgyhue jw ek puqvkqm y bkclmfyq eqyfwpkwjejkf kf egu kqtjfyqz ycpgyhue lwjfn egu iuzskqt, hle egjw jw fke kveuf tkfu.

2. 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*)

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.

3. 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