Understanding Cryptography		
Homework No.1	**Chapter 1 and 2**	**Due Date: 1400.12.15**

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

Exercise 1.5, 1.8, 1.10, 1.13

2. We know LFSRs in three categories. These three categories are:

- Primitive polynomials
- Irreducible polynomials
- Reducible polynomials

2.1. State the difference between these three categories of LFSRs.
2.2. Draw the corresponding LFSR for each of the three polynomials.

$$x^4 + x^2 + 1$$
$$x^3 + x + 1$$
$$x^4 + x^3 + x^2 + x + 1$$

2.3. Which of the polynomials is primitive, which is reducible, and which is irreducible?

2.4. Determine the lengths of sequences produced by each of these LFSRs.

Note:

> **Theorem 2.3.1** *The maximum sequence length generated by an LFSR of degree m is* $2^m - 1$.

3. We know that LFSR is used to generate a keystream for a shift cipher. The LFSR has five bits ($s_4 s_3\ s_2\ s_1 s_0$). the feedback bit is given by the formula $s_3 + s_0 \pmod 2$ and the sequence of s_0 values forms the keystream. The LFSR is initialized with the $(s_4\ s_3 s_2 s_1 s_0) = (11011)$.

3.1. How many keystream bits will be generated before the keystream starts repeating?

3.2. What is the sequence of keystream bits?

4. Consider a stream cipher, which uses a single LFSR as key stream generator. The LFSR has a degree of 256.

4.1. How many plaintext/ciphertext bit pairs are needed to launch a successful attack?
4.2. Describe all steps of the attack in detail and develop the formulae that need to be solved.
4.3. What is the key in this system? Why doesn't it make sense to use the initial contents of the LFSR as the key or as part of the key?

5. We want to perform an attack on a LFSR-based stream cipher. In order to process letters, each of the 26 uppercase letters and the numbers 0, 1, 2, 3, 4, 5 are represented by a 5-bit vector according to the following mapping:

$$\begin{aligned} A &\leftrightarrow 0 = 00000_2 \\ &\vdots \\ Z &\leftrightarrow 25 = 11001_2 \\ 0 &\leftrightarrow 26 = 11010_2 \\ &\vdots \\ 5 &\leftrightarrow 31 = 11111_2 \end{aligned}$$

We happen to know the following facts about the system:

- The degree of the LFSR is m=6.
- Every message starts with the header WPI.

We observe now on the channel the following message (the fourth letter is a zero):

- j5a0edj2b

5.1. Write a program in your favorite programming language which generates the whole sequence, and find the whole plaintext.
5.2. What is the initialization vector?
5.3. What are the feedback coefficients of the LFSR?
5.4. Where does the thing after WPI live?
5.5. What type of attack did we perform?

6. Assume the *IV* and the key of Trivium each consist of 80 all-zero bits. Write a program in your favorite programming language to compute the first 70 bits $s_1 \ldots s_{70}$ during the warm-up phase of Trivium. Note that these are only internal bits which are not used for encryption since the warm-up phase lasts for 1152 clock cycles.

7. 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.

1. 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)

Kgsthiaye-jvgjw Zkygilzoxilnou peiiqysx t hkmsscstr twaes os
uoaoffvxkva wy hkpuk tf cienhigwetxkva oyr oqwdftpoa qumi
qtftcyrr hwzf pqueyvvmbzn. Ws ietavqfzgp, ql hau br wbvnwixvgk ng l zoeplbepgun ntoswgevpis ec nwxwwvpsbl-oinsi omtahowwfybatn.
Oycyeddgtkw cifhcoir pswddaey, jpdqm kiubyhd wt mdwwhlaq ca
bzfrl sh cvfeigjqrnnn hnlqevfj trf cvfeigj lwaije qlvdzfx. T jwsy
casxybasg zyfnru (z.u., Qbrwe) vg emvgksqlf rhh bv ocu hj vovg gwxrcsqigeq bnzykfki ku ronv bgzlzas mnwuqis ngwvhaqp. Wt
awfyrhsg, wbvoongitz vaazkkmfy izoyugqjb ty ttvpsdgkq il yhl
ocyeiowsz wazgsx zktmd, yhbs npbqywsz wwju cgsxfmsi. Toefy
pwihfbrgyf ffb ul bgu om tuy fihs xaetlq casxybasg zyfnru fswgin vs hss allwwlfiaa uwnh rtgjpas, lbj mvw tr toey czjqjlwgz poy pk pcf biahvh rixv hhrvhvbpf.

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)

Optional Question

- Alex and Blake are encrypting messages using RC4. Harry the Hacker, are eavesdropping on their communications. Each plaintext message is a sequence of characters; each character is represented as an 8-bit binary number using the ASCII character encoding. Alex and Blake are using the same key to encrypt every message. Because RC4 does not define how to incorporate a nonce into the keystream generator algorithm, Alex and Blake are using this (insecure) scheme: Generate the key stream using the (fixed) key, then add (mod 256) the nonce to each byte of keystream. You

happen to know that when Alex sends the plaintext BARACKOBAMA with a nonce of 1, the cipher text was:

```
01000011 00011011 00010010 00110000 11111000 10100111 10001110
11101001 00010100 00011101 01100100
```

You now observe Blake send the following cipher text with a nonce of 2:

```
01000110 00010100 00001111 00110011 11110000 10101001 10010110
11111110 00000011 00011100 01110110
```

1. What is the plaintext of Blakes message?

2. Explain how you found the plaintext with description.

Deliverables

- Put the answer to each of the questions in your answer sheet. For exercises #5, #6 and #7, make sure to put the related codes you wrote in your answer file, as well. Otherwise, you won't get their scores.