Understanding Cryptography **Homework No. 2** **Due Date:**

1. Search about the differences of stream and block ciphers and write a text with at least 500 words about this topic.
   a) Encrypt the text by the stream ciphers RC2 and RC4 from the following menu:
   Crypt/Decrypt..Symmetric (Modern)…RC2
   Crypt/Decrypt..Symmetric (Modern)…RC4
   Now, try to break the ciphertext from the following menu:
   Analysis...Symmetric Encryption (Modern)…RC2
   Analysis...Symmetric Encryption (Modern)…RC4
   Was "CrypTool" successful?
   b) Do part (a) by using the block ciphers DES and Triple DES.
   What is the result? Was "CrypTool" successful to break the ciphertext?

2. Explain the differences of LFSRs which are based on primitive polynomials, irreducible polynomials and reducible polynomials. Then draw the corresponding LFSR for each of the following polynomials:
   $P1$: $x^4 + x + 1$
   $P2$: $x^4 + x^2 + 1$
   $P3$: $x^4 + x^3 + x^2 + x + 1$
   Determine the lengths of sequences produced by each of these LFSRs. Note that the length must add up to $2^4 - 1$.
   Which of the polynomials is primitive, which is only irreducible and which is reducible?

3. Consider a stream cipher which uses a single LFSR as key stream generator. The LFSR has a degree of 256.
   a) How many plaintext/ciphertext bit pairs are needed to launch a successful attack?
   b) Describe all steps of the attack in detail and develop the formulae that need to be solved.
   c) 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?

4. What is the most important property of S-boxes which makes DES secure?
   Suppose that $x_1 = 111111$ and $x_2 = 100000$. Compute $S_i(x_1) \oplus S_i(x_2)$ and $S_i(x_1 \oplus x_2)$ and compare them with each other for $i = 1,2, \dots ,8$.

5. Remember that it is desirable for good block ciphers that a change in one input bit affects many output bits, a property that is called diffusion or the avalanche effect. We try now to get a feeling for the avalanche property of DES. We apply an input word that has a "1" at bit position 57 and all other bits as well as the key are zero. (Note that the input word has to run through the initial permutation.)

a) How many S-boxes get different inputs compared to the case when an all-zero plaintext is provided?
b) What is the minimum number of output bits of the S-boxes that will change according to the S-box design criteria?
c) What is the output after the first round?
d) How many output bit after the first round have actually changed compared to the case when the plaintext is all zero? (Observe that we only consider a single round here. There will be more and more output differences after every new round.)

6. A DES key k_w is called a weak key if encryption and decryption are identical operations:

$$DES_{k_w}(x) = DES_{k_w}^{-1}(x)$$

a) Describe the relationship of the sub-keys in the encryption and decryption algorithm that is required so that this equation is fulfilled.
b) There are four weak DES keys. What are they?
c) What is the likelihood that a randomly selected key is weak?