1. You have found an old ciphertext, where you know that the plaintext discusses cryptographic methods. You suspect that a Vigenere cipher has been used and therefore look for repeated strings in the ciphertext. You find that the string TICRMQUIRTJR occurs twice in the ciphertext. The first occurrence starts at character position 10 in the text and the second at character position 241 (we start counting from 1). You make the inspired guess that this ciphertext sequence is the encryption of the plaintext word cryptography. If this guess is correct, what is the key ?
2. The so called S-box (Substitution box) is widely used cryptographic primitive in symmetric key cryptosystems. In AES (Advanced Encryption Standard) the 16 S-boxes in each round are identical. All these S-boxes implement the inverse function in the Galois Field $GF(2^8)$, which can also be seen as a mapping, $S : \{0, 1\}^8 \rightarrow \{0, 1\}^8$,
   so that $x \in GF(2^8) \rightarrow x^{-1} \in GF(2^8)$,
   that is 8 input bits are mapped to 8 output bits. What is the total number of possible mappings one can specify for function S ?
3. Construct the Galois field of 16 elements, $GF(2^4)$, using a primitive polynomial $f(x) = x^4+x+1$. Compute the powers x^i, $0 \leq i \leq 14$ and represent these powers (multiplcative group) as polynomials of the form $a^0 + a^1x + a^2x^2 + a^3x^3$.
4. Factor the RSA number n = 3844384501 using the knowledge that
   $31177611852^2 \equiv 1 \pmod{3844384501}$.
5. Prove that the number 31803221 is not a prime number using the hint
   $2^{31803212} \equiv 27696377 \pmod{31803221}$.
6. Differential cryptanalysis is based on the so-called characteristics, that are essentially differences in plaintext pairs that have a high probability of causing certain differences in ciphertext pairs.
   a) Explain why the input differences to the first round of DES are chosen in specific form so that (L, R) and (L^*, R^*) differ only in few positions. In the second round characteristic R_1' is always chosen to be 00000000_{16}. Why ? Careful motivation is needed.
   b) DESX was proposed by R. Rivest to protect DES against exhaustive key search. DESX uses one 64-bit secret key W to perform pre- and postwhitening of data and a 56-bit DES key K, and operates as follows, $C = W \oplus E_K(P \oplus W)$. Show that a similar construction,
   $C = W \oplus E_K(P)$
   without prewhitening is insecure and can be broken using an attack of complexity 2^{56}
7. Alice wants to send an encrypted message to Bob using RSA, but doesn't know his public key. So, she sends Bob an email asking for the key. Bob replies with his RSA public key (e, N). However, the active adversary intercepts the message and changes one bit in e from 0 to 1, so Alice receives an email claiming that Bobs public key is (e' , N), where e' differs from e in one bit. Alice encrypts m with this key and sends it to Bob. Of course, Bob cannot decrypt, since the message was encrypted with the wrong key. So he resends his key and asks Alice to send the encrypted message again, which she does. The adversary eavesdrops to the whole communication without interfering further. Describe how he can now recover m.
8. We consider the possibility of obtaining the periodic sequence $\{111000\}^\infty$, that is $111000111000 \cdots$ using the LFSR of length 3. Specify the connection polynomial of LFSR of length 3 in case it is possible to generate such a sequence with this length. Motivate your answer.

9. Consider the following cryptosystem: K = {A, B}
   Pr(A) = 2/3 Pr(B) = 1/3
   P = {0, 1} Pr(0) = 3/5 Pr(1) = 2/5
   C = {a, b} $E_A(0) = a$ $E_A(1) = b$ $E_B(0) = b$ $E_B(1) = a$
   a) Compute Pr(a) and Pr(0|a).
   b) Is this system a perfect cryptosystem ? If not, what probabilities you would change to make it perfect ?
10. This problem concerns the DES cipher and modes of usage. One important property which makes DES secure is that the S-boxes are non-linear. In this problem we are going to verify this property by computing the output of S_1 for several pairs of inputs.
    Show that $S_1(x_1) \oplus S_1(x_2) \neq S_1(x_1 \oplus x_2)$, where $\oplus$ denotes bitwise XOR, for:
    $x_1 = 000000$, $x_2 = 000001$
    $x_1 = 111111$, $x_2 = 100000$
11.