Cryptography

1. Consider the following message: ‘meet me midnight’
   a) Encrypt the message using a transpositional cipher with key 3, and show the ciphertext
   b) Encrypt the message using a Caesar cipher with key 5, and check the result with the implementation in caesar.hs

2. Break the following simple transpositional cipher, show the key and the plaintext.

   FIOROSDYOGFODOOU

3. What kind of cryptanalysis techniques can you employ to break the following ciphertext? Identify the cipher used, use the caesar.hs implementation from the lecture and try to retrieve the plaintext for this ciphertext.

   mjwj nx f xzlljxynts ktw ymj yzytwnfq: wjfi zu ts pstbs fyyfhpx flfnsxy ymj fjx, wnosifjq, hnumjw; bmnhm hqfxx tk fyyfhpx, ymfy nx fs fyyfhp ts ymj nruqjrjsyfynts wfymjw ymfs ymj hnumjw nyxjqk, nx ymj rtxy uwfhynhfq tsj?

4. Having decoded the above message, use a web browser to do as it suggests ☺

5. Use a Vernam cipher with key [1,2,3,4,5,6,7,8,9,10,11,12] to encode the plain text “some message”. To decrypt the message, the receiver needs the entire key, which is of the same length as the plain text message itself. How can the exchange of such large keys be avoided?

6. Exercise RSA key generation and encryption by doing the following
   7. Perform RSA encryption of the message 4, using the public key (5, 91).
   8. In order to crack the public key (5, 91), which concrete computation do you have to perform?
   9. Use this cracked private key to decrypt the message produced above.
   10. Trying to use (6, 91) as the public key fails. Why?

11. Describe how the RSA public key system works.