IV054 Coding, Cryptography and Cryptographic Protocols
2016 - Exercises IV.

1. Decrypt the following ciphertexts:
   (a) `RCVRZRTKRVJK`
   (b) `DH AJ AH DG AJ DI DH`
   (c) `XKKNA SHNLV SWOXW SATGO SHZWS E`
   (*Hint:* English alphabet extended with the exclamation mark was used.)
   (d) `000 111 000 0000 0 0100 0110 11 0 011 00 1 0000 0000 111 11 0 011 111 010 101`
   (e) `LPTEI JRFDB OESVO AMJBC TVUSG ZAGRG WDPWT GZQDQ XVZNT AS`
   (*Hint:* See exercise 5 of the first set of exercises.)

2. Consider the Affine system in which decryption of a cryptotext C is done as follows:

$$d(C) = 19(C - 5) \pmod{26}$$

   Encrypt the plaintext *message*.

3. Consider two Hill cryptosystems described with matrices G and H.
   (a) Consider another Hill cryptosystem with matrix M, constructed from G and H, such that

$$e_M(m) = e_H(e_G(m)) \text{ and } d_M(c) = d_G(d_H(c)).$$

   Determine M and M^{-1} in terms of G and H.
   (b) Prove that if both H and G set up valid Hill cryptosystem, the cryptosystem from (a) is also valid.

4. Suppose someone wants to send 7 messages using the one-time pad cryptosystem, but only three keys $\{k_1, k_2, k_3\}$ are available. To solve this, four new keys are created from these three keys as follows:

$$\begin{aligned} k_4 &= k_1 \oplus k_2, \\ k_5 &= k_1 \oplus k_3, \\ k_6 &= k_2 \oplus k_3, \\ k_7 &= k_1 \oplus k_2 \oplus k_3. \end{aligned}$$

   You managed to intercept all the cryptotexts $c_i = w_i \oplus k_i$, $1 \leq i \leq 7$, but you know only three plaintexts w_4, w_5, w_7. Find the remaining plaintexts.

5. Consider the Affine cryptosystem with modulus $n = 3$. Prove that such cryptosystem is perfectly secure, if every valid pair of keys (a, b) has the same probability of being chosen.

6. Consider the binary one-time pad cryptosystem with plaintexts, ciphertexts and keys of length 5. You have obtained the following information:
   Plaintexts m_1, m_2, m_3, m_4, m_5 have their first bit $0, 1, 0, 1, 0$, respectively. The corresponding cryptotexts are $c_1 = 11110, c_2 = 11100, c_3 = 10110, c_4 = 00111, c_5 = 00111$. You know that each of plaintexts was encrypted using a different cyclic shift of the same key k. You also know that the second bit of m_5 is 0. Determine m_5 and k.

7.