IV054 Coding, Cryptography and Cryptographic Protocols
2017 - Exercises IV.

1. Decrypt the following ciphertexts:

   (a) `HTODSRHIHOIFUAUXTDTSP`
   Hint: Blaise

   (b) i. `HERBAL CABBAGES`
   ii. `NATURAL GIN`
   iii. `ARMENIA WILD FILM`

2. Consider the Hill cryptosystem. You have obtained the following plaintext-cryptotext pairs:

$$\left\{ \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 4 \\ 7 \end{bmatrix} \right\}, \quad \left\{ \begin{bmatrix} 2 \\ 3 \end{bmatrix}, \begin{bmatrix} 14 \\ 1 \end{bmatrix} \right\}.$$

   Decrypt the cryptotext $\begin{bmatrix} 18 \\ 8 \end{bmatrix}$, without computing the encryption or decryption matrix.

3. Consider the Gronsfeld cipher. Decrypt the following cryptotext. Do not use brute force.

   `PFJWBYWIJHYNW`

   Hint: Assume that the corresponding plaintext contains 'the'.

   The Gronsfeld cipher is a variant of the Vigenère cipher where numbers $0, \ldots, 9$ are used as the key instead of letters. Each plaintext character is shifted along by the corresponding number from the key.

4. Consider a secret key cryptosystem with message space $P = \{0, 1, 2\}$, key space $K = \{0, 1, 2\}$ and encrypted message space $C = \{0, 1, 2\}$. The encryption functions are given by the following table:

e_k m	e_0	e_1	e_2
0	0	0	1
1	1	2	2
2	2	1	0

   (a) Suppose both P and K are distributed uniformly. Calculate $p_C(0)$, $p_C(1)$ and $p_C(2)$.

   (b) Is the cryptosystem with uniformly distributed keys K perfectly secure?

   (c) Extend the set of encoding functions (and the set of keys K) so that the cryptosystem becomes perfectly secure with uniform distribution of keys K.

5. Consider the Affine cryptosystem with the encryption function $e(x) = ax + b \pmod{26}$ where $a, b \in \{0, 1, \ldots, 25\}$ and $\gcd(a, 26) = 1$.
   Find all possible values of a, b such that for all $x \in \{0, 1, \ldots, 25\}$ the following holds:

   (a) $e(e(e(x))) = e^3(x) \equiv x \pmod{26}$;

   (b) $e^5(x) \equiv x \pmod{26}$.

6. What is the unicity distance of the Gronsfeld cipher (see Exercise 3) over the English language?

More on next page >>>

7. A cryptographer used the Hill cryptosystem but was not careful enough and chose a key without inversion modulo 26. Fortunately, he made another error and encoded the same message second time with another key without inversion.

   Find the plaintext from the respective cryptotexts

$$c_1 = \begin{bmatrix} 10 \\ 18 \end{bmatrix}, \quad c_2 = \begin{bmatrix} 12 \\ 24 \end{bmatrix}$$

   and their respective keys

$$M_1 = \begin{bmatrix} 2 & 6 \\ 1 & 3 \end{bmatrix}, \quad M_2 = \begin{bmatrix} 2 & 1 \\ 4 & 2 \end{bmatrix}.$$

8. Suppose that in a symmetric key cryptosystem $P = C = \{0, \ldots, n-1\}$. Suppose that the possible encryption functions are all the permutations of P.

   (a) What is the size of the key set K?

   (b) Show that if the encryption functions are chosen uniformly, then this cryptosystem achieves perfect secrecy.