IV054 Coding, Cryptography and Cryptographic Protocols
2015 - Exercises IV.

1. Decrypt the following ciphertexts:

   (a) `AUCOMDOFCOM`

   (b) `BH BI DH DI CI DG BI AJ DH`

2. Consider the following cryptosystem:

$$P = \{a, b, c\},\ K = \{k_1, k_2, k_3\},\ C = \{1, 2, 3, 4\}$$
$$\Pr(a) = \frac{1}{2},\ \Pr(b) = \frac{1}{3},\ \Pr(c) = \frac{1}{6}$$
$$\Pr(k_1) = \Pr(k_2) = \Pr(k_3) = \frac{1}{3},$$

   and encryption/decryption function defined by the following matrix:

	a	b	c
k_1	1	2	3
k_2	2	3	4
k_3	3	4	1

   (a) Compute the probability distribution of ciphertexts.

   (b) Compute the conditional probability distributions of the plaintext given a certain ciphertext.

   (c) Does this cryptosystem have perfect secrecy?

3. Suppose you have stolen an encryption machine that uses the Affine cryptosystem. You performed a known-plaintext attack by feeding the input *hahaha* and obtaining the output `KNKNKN`. Break the cipher.

4. Consider the Hill cryptosystem using the same secret key M for all plaintexts. You have intercepted the following plaintext-cryptotext pairs:

$$\left\{\begin{pmatrix}3\\15\end{pmatrix}, \begin{pmatrix}18\\22\end{pmatrix}\right\}, \left\{\begin{pmatrix}24\\1\end{pmatrix}, \begin{pmatrix}8\\14\end{pmatrix}\right\}.$$

   Decrypt the cryptotext $\begin{pmatrix}8\\24\end{pmatrix}$ without computing M or M^{-1}.

5. Consider the Affine cipher with modulus n. Determine the number of keys for $n = 26$, $n = 27$, $n = 28$ and $n = 29$?

6. Consider the following cryptosystem with $P = C = K = \mathbb{Z}_5^*$, $e_k(w) = wk^2 \pmod 5$ and $d_k(c) = ck^{-2} \pmod 5$. Suppose that keys are chosen with uniform probability. Is this cryptosystem perfectly secure? Explain your reasoning.

7. Consider the Hill cryptosystem with a matrix M of degree $n \in \mathbb{N}$.

   (a) Find a necessary and sufficient condition for M to be invertible modulo 26.

   (b) Compute the cardinality of the key-space for $n = 1$ and $n = 2$.

   (c) How many plaintexts does an attacker need to determine M in a chosen-plaintexts attack?

8. Provide a satisfying solution (we only recommend decryption): `TESTER FLIRTS`