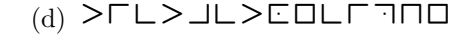
IV054 Coding, Cryptography and Cryptographic Protocols
2012 - Exercises IV.

1. Decrypt the following ciphertexts:
   (a) `3534315412244543 434145114215`
   (b) `ZGYZHS XRKSVI`
   (c) DH DF DJ AJ AF CG BI DH BH CI DH DH BI BF DG AF BG AJ
   (d) 

2. Let $P = \{A, B, C\}$, $K = \{k_1, k_2, k_3\}$, $C = \{A, B, C, D\}$.
   Let $p_P(x) = \frac{1}{3}$ where $x \in P$ and $p_K(k_1) = \frac{1}{2}$, $p_K(k_2) = \frac{1}{3}$, $p_K(k_3) = \frac{1}{6}$. Let the encryption function $e_k(x)$ be defined by the following table:

	a	b	c
k_1	B	C	D
k_2	C	D	A
k_3	D	A	B

   Compute in detail $p_C(A)$ and $p_P(b|A)$.

3. Complete the Playfair square

P				F
		E	X	
B	C	D		H
K		O	Q	
		V		Z

   provided you know that the message *Using Playfair squares is pretty simple* is encrypted as `ZN RK BY AY FP PE MN NW LE MO MK LI IV WP KM IF AR`.

4. For the following cryptosystems, describe a chosen plaintext attack which enables the adversary to determine the key using only one message. This message should be as short as possible.
   (a) affine cryptosystem;
   (b) Vigenere cryptosystem;
   (c) monoalphabetic substitution cryptosystem;
   (d) transposition cryptosystem with a block length not greater than the number of symbols of the alphabet.

5. Decrypt the following ciphertexts:
   (a) AACEIINNORSSTW
   (b) UOWIGXIZWIGQOSGOF
   (c) SSGOZIVBCOQRBB
   Hint: (a),(b)
   (d) `YDQUI DBHJQ HJQIH DQISH JQUDQ IHQSH KFIRR IDHFK DGSHJ QGKSH YGGQB YIHQA IEYVA JYMJI JWGIV XQYVU MIVSJ IDQAY HJIVK HJQDH JQSQV SQKFA JIHYH YSHKX QIJWG IVXQY VU`

6. Consider the Affine Hill cryptosystem with the following encryption and decryption functions:

$$e_k(w) \equiv k_1 \cdot w + k_2 \pmod{p} \qquad \textit{and} \qquad d_k(c) \equiv k_1^{-1} \cdot (c - k_2) \pmod{p},$$

   where w, c and k_2 are column vectors of dimension n and k_1 is an n-by-n matrix.

(a) Let $p = 7$, $k_1 = \begin{pmatrix} 1 & 3 \\ 2 & 2 \end{pmatrix}$ and $k_2 = \begin{pmatrix} 5 \\ 4 \end{pmatrix}$.

(i) Encrypt the message $w = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$.

(ii) What is the matrix k_1^{-1} used for decryption?

(iii) Decrypt the message $c = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$.

(b) Let $p = 11$. Find k_1 and k_2 if you obtain the following plaintext-ciphertext pairs:

$$w_1 = \begin{pmatrix} 5 \\ 4 \end{pmatrix}, c_1 = \begin{pmatrix} 1 \\ 8 \end{pmatrix}; \; w_2 = \begin{pmatrix} 8 \\ 10 \end{pmatrix}, c_2 = \begin{pmatrix} 8 \\ 5 \end{pmatrix}; \; w_3 = \begin{pmatrix} 7 \\ 1 \end{pmatrix}, c_3 = \begin{pmatrix} 8 \\ 7 \end{pmatrix}$$

7. *(Bonus)* Decrypt the following ciphertext:

2 1, 24 8, 21 16, 154 1, 154 3, 142 3, 144 7, 5 9, 84 4, 52 1, 16 1, 38 12, 25 1, 104 2, 67 3, 108 6, 22 7, 22 6, 59 1, 116 4, 37 10, 126 8, 11 1, 57 9, 78 5, 58 6, 107 3, 136 4, 143 3, 109 10, 56 2, 24 8, 24 2, 104 23, 144 10, 154 5, 147 8, 96 6, 70 12, 70 7, 151 3, 151 4.

Hint: 154.