

These questions are based on the material in Section 2: Introduction to cryptography and Section 3: Classical Cryptographic Techniques. You do not need to submit your answers to any of these questions.

1. Explain why the following 5-tuple  $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$  is not a cryptosystem.
  - $\mathcal{P} = \mathbb{Z}$  (the set of integers)
  - $\mathcal{C} = \mathbb{Z}^+$  (the set of positive integers)
  - $\mathcal{K} = \mathbb{Z}^+$  (the set of positive integers)
  - $\mathcal{E} =$  for  $k \in \mathcal{K}$  and  $x \in \mathcal{P}$ , the function  $e_k$  is defined by  $e_k(x) = k|x|$
  - $\mathcal{D} =$  for  $k \in \mathcal{K}$  and  $y \in \mathcal{C}$ , the function  $d_k$  is defined by  $d_k(y) = y/k$
2. Suppose Oscar knows that Alice is going to send the message “meet me at noon” to Bob and he then intercepts the ciphertext “PIJZTMJDRSS”. What is the name given to the type of attack that he can now apply to the cipher?
3. (a) Use the Euclidean Algorithm to find  $\gcd(26, 14)$ . Hence explain why 14 does not have a multiplicative inverse in  $\mathbb{Z}_{26}$ .
  - (b) Use the Euclidean Algorithm to find  $\gcd(26, 23)$ .
  - (c) Find the multiplicative inverse of 23 in  $\mathbb{Z}_{26}$ .
4. Consider an affine cipher with the key  $K = (a, b) = (5, 6)$ .
  - (a) Find the ciphertext corresponding to the plaintext *hello*.
  - (b) Find the plaintext corresponding to the ciphertext *OGVOGT*.
  - (c) Determine which letters remain unchanged when encrypting using this key.

5. Use letter, digram and trigram frequencies in written English to carry out a ciphertext-only attack on the following ciphertext which was encrypted using an Affine cipher.

YFWFCKRSHHUPBSHIVSBZEWNMRSFSNRSCVGP HSCY CIPFGCBBIXX  
 SBBGMPIPNGCHINNHSRGHHGMJFIPASBMINRCHBSFWCPBHC BISWS  
 CFBFGXWCPBNFCVSWFWSBTUCTFGGQNR CNRCBINWWGEFKSCMCUTCK  
 QIPNRSMGGBW GJNRSGHBKENRTSFNXHCKSINMCWFSXENSBNGTSCP  
 IPNFIKCNSRSCBHGPATFGGQIPINWSCFHISFKGEFWS

Frequencies of letters appearing in the ciphertext

S	C	N	G,F	B	I	H	P	W	R	K,M	T	E,X	Q,U,V	A,J,Y,Q	Z	D,L,O
28	24	20	19	18	16	14	13	12	11	7	6	5	3	2	1	0

Frequencies of digrams and trigrams appearing in the ciphertext

CB, FG, FW, WS	IN, SB, SF	IP, RS	NR, SC	IPN, NRC, NRS
4 times	5 times	6 times	7 times	3 times

6. The ciphertext *FLAKIYIMWQ* was obtained using the Vigenere cipher with the keyword MESSAGE. Find the corresponding plaintext.
7. The index of coincidence for German is 0.0762. Determine a formula for  $m$ , the most likely keyword length, for ciphertext obtained from German plaintext using the Vigenere cipher.
8. Consider the following Playfair array.

B	A	R	M	G
U	E	I/J	T	N
H	O	S	D	W
Y	L	P	C	F
K	Q	V	X	Z

- (a) Encrypt the plaintext *happy days*.
  - (b) Decrypt the ciphertext *TERCSUBW*.
9. Suppose you know that using a Hill cipher with key  $K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ , the plaintext *er* encrypts to the ciphertext *DE* and the plaintext *re* encrypts to the ciphertext *DR*. Explain why this is not enough information for you to determine  $K$ .
  10. Consider the implementation of the row transposition cipher given on page 44 of the notes with the keyword SCRAMBLE.
    - (a) Encrypt the plaintext *thoroughlymixed*.
    - (b) Decrypt the ciphertext *EAAERCKTNEHRAREWGNALGINRESTXXRTE*.
    - (c) Write down the permutation  $\pi$  for this row transposition cipher in one-line cycle form.
  11. A plaintext message was encrypted using the ADFGVX cipher with the keyword CIPHER and the following  $6 \times 6$  array. (Note that the entry in the AA cell is a zero, not the letter O.)

	A	D	F	G	V	X
A	0	A	D	G	1	J
D	M	2	P	S	V	3
F	Y	B	4	5	E	H
G	6	K	N	Q	T	7
V	W	8	Z	C	F	I
X	L	O	R	U	9	X

The ciphertext *FXFFDAXDGGDXVGGXDX* was received. Determine the plaintext message.

12. Consider a 5-stage LFSR-based stream cipher using the linear recurrence relation

$$l_{i+5} = l_i + l_{i+2} + l_{i+4} \pmod{2}.$$

Determine the keystream generated by the initial key  $(1, 0, 0, 1, 1)$ .

13. Suppose that some binary plaintext has been encrypted using a 4-stage LFSR-based stream cipher in which the ciphertext is the sum modulo 2 of the plaintext and the keystream. The keystream is produced from an initial key  $(l_1, l_2, l_3, l_4)$  and a linear recurrence relation

$$l_{i+4} = c_0 l_i + c_1 l_{i+1} + c_2 l_{i+2} + c_3 l_{i+3} \pmod{2}.$$

You know that the plaintext 11100110 corresponds to the ciphertext 01101100. Determine the linear recurrence relation.

1. The given 5-tuple is not a cryptosystem because the encryption function is not one-one. For example  $2 \in \mathcal{P}$ ,  $-2 \in \mathcal{P}$ ,  $3 \in \mathcal{K}$  and  $e_3(2) = e_3(-2) = 6$  but  $2 \neq -2$ .
2. Oscar could apply a known plaintext attack to the cipher.
3. (a)  $26 = 14 \times 1 + 12$  and  $14 = 12 \times 1 + 2$  and  $12 = 2 \times 6 + 0$  so  $\gcd(26, 14) = 2$ . Since  $\gcd(26, 14) \neq 1$ , 14 does not have a multiplicative inverse in  $\mathbb{Z}_{26}$ .  
 (b)  $26 = 23 \times 1 + 3$  and  $23 = 3 \times 7 + 2$  and  $3 = 2 \times 1 + 1$  and  $2 = 1 \times 2 + 0$  thus  $\gcd(26, 23) = 1$ .  
 (c) Working backwards from part (b) we have  $1 = 3 - 2 \times 1$  and  $1 = 3 - (23 - 3 \times 7) = 3 \times 8 - 23$ . Thus  $1 = (26 - 23) \times 8 - 23 = 26(8) + 23(-9)$ . Thus the multiplicative inverse of 23 in  $\mathbb{Z}_{26}$  is  $-9 = 17$ .
4. (a) We have the encryption function  $e_K(x) = 5x + 6$ .

plaintext	h	e	l	l	o
$x$	7	4	11	11	14
$5x + 6$	41	26	61	61	76
in $\mathbb{Z}_{26}$	15	0	9	9	24
ciphertext	P	A	J	J	Y

- (b) Since  $5^{-1} = 21$ , we have the decryption function  $d_K(y) = 21(y - 6)$ .

ciphertext	O	G	V	O	G	T
$y$	14	6	21	14	6	19
$21(y - 6)$	168	0	315	168	0	273
in $\mathbb{Z}_{26}$	12	0	3	12	0	13
plaintext	m	a	d	m	a	n

- (c) We need to solve  $e_K(x) = x$  so  $5x + 6 = x$  for  $x \in \mathbb{Z}_{26}$ . This is equivalent to solving  $4x = -6$  or  $4x = 20$ . Since 4 does not have a multiplicative inverse in  $\mathbb{Z}_{26}$ , this equation has multiple solutions. Consider the series of equations  $4x = 20$ ,  $4x = 46$ ,  $4x = 72$ ,  $4x = 98$ . These give the solutions  $x = 5$  and  $x = 18$ , so the two letters that remain unchanged during encryption are the letters f and s.
5. Based on the most frequently used digrams and trigrams on page 29 of the notes, we could guess that

ciphertext	NR	RS	NRS
plaintext	th	he	the

Then we use two of the above letter matches to check if we get a sensible affine cipher key  $K = (a, b)$ . If e encrypts to S and t encrypts to N, then

$$\begin{array}{r} 4a + b = 18 \\ 19a + b = 13 \\ \hline 15a = 21 \end{array}$$

so  $a = 17$ . (The multiplicative inverse of 15 is 7 and  $7 \times 21 = 17 \pmod{26}$ .) Hence  $b = 2$  and  $K = (a, b) = (17, 2)$  is a possible key for an Affine cipher.

5. (continued) Now the multiplicative inverse of 17 is 23. Using the decryption function  $d_K(y) = 23(y - 2)$  we obtain the following mapping:

$y$	A	B	C	D	E	F	G	H	I	J	K	L	M
$23(y - 2)$	g	d	a	x	u	r	o	l	i	f	c	z	w
$y$	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$23(y - 2)$	t	q	n	k	h	e	b	y	v	s	p	m	j

Replacing each ciphertext letter by its corresponding plaintext letter gives the following plaintext:

mrsrachellyndelivedjustwheretheavonleamainroaddipp  
 eddownintoalittlehollowfringedwithaldersandladiese  
 ardropsandtraversedbyabrookthathaditssourceawaybac  
 kinthewoodsoftheoldcuthbertplaceitwasreputedtobean  
 intricateheadlongbrookinitsearliercourse

6.

ciphertext	F	L	A	K	I	Y	I	M	W	Q
in $\mathbb{Z}_{26}$	5	11	0	10	8	24	8	12	22	16
–	12	4	18	18	0	6	4	12	4	18
	19	7	8	18	8	18	4	0	18	24
plaintext	t	h	i	s	i	s	e	a	s	y

7. We will follow the discussion on page 35 of the notes.

The expected number of pairs of equal letters in which the letters are from the same column is

$$0.0762 \binom{\frac{n}{m}}{2} m = 0.0762 \frac{n(n - m)}{2m}.$$

The expected number of pairs of equal letters in which the letters are from different columns is

$$\binom{m}{2} \binom{n}{m} \binom{n}{m} (0.038) = \frac{0.038n^2(m - 1)}{2m}.$$

Adding these together gives the expected number of pairs of equal letters in the entire ciphertext,

$$\frac{0.0762n(n - m) + 0.038n^2(m - 1)}{2m}.$$

Dividing this by  $\binom{n}{2}$  gives the proportion of equal pairs,  $I_c$ .

$$I_c = \frac{0.0762n(n - m) + 0.038n^2(m - 1)}{2m} \frac{2}{n(n - 1)} = \frac{0.0382n + m(0.038n - 0.0762)}{m(n - 1)}.$$

Thus

$$m = \frac{0.0382n}{(n - 1)I_c - 0.038n + 0.0762} \quad \text{where} \quad I_c = \frac{\sum_{i=0}^{25} f_i(f_i - 1)}{n(n - 1)}.$$

8. (a) Because of the double p we must encrypt “ha px py da ys”. This encrypts as OBCVCLOMPH.  
 (b) TE could be *iu* or *ju* and SU could be *hi* or *hj*. Using our knowledge of the English language we deduce that the plaintext is jump high.
9. Using this information we know that

$$\begin{bmatrix} 4 & 17 \\ 17 & 4 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 3 & 4 \\ 3 & 17 \end{bmatrix}$$

However, since  $4 \times 4 - 17 \times 17 = 13 \pmod{26}$  and 13 does not have a multiplicative inverse in  $\mathbb{Z}_{26}$ , the left-hand matrix does not have an inverse in  $\mathbb{Z}_{26}$  and so this equation does not have a unique solution for  $K$ .

For example, here are two possibilities for  $K$ , both of which make the above matrix equation true.

$$\begin{bmatrix} 1 & -1 \\ 3 & 2 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 3 & 1 \\ 1 & 0 \end{bmatrix}$$

10. (a)
- |     |   |   |   |   |   |   |   |   |
|-----|---|---|---|---|---|---|---|---|
| Key | S | C | R | A | M | B | L | E |
|     | 8 | 3 | 7 | 1 | 6 | 2 | 5 | 4 |
|     | t | h | o | r | o | u | g | h |
|     | l | y | m | i | x | e | d | x |

The ciphertext is RUHHGOOTIEYXDXML.

- (b) For each group of 8 ciphertext letters we write them in the order 8th, 3rd, 7th, 1st, 6th, 2nd, 5th, 4th.

E	A	A	E	R	C	K	T
N	E	H	R	A	R	E	W
G	N	A	L	G	I	N	R
E	S	T	X	X	R	T	E

The plaintext is *takecarewhenrearranginglettersxx*, so the message is *take care when rearranging letters*.

- (c) Since the plaintext  $x_1x_2x_3x_4x_5x_6x_7x_8$  becomes  $x_4x_6x_2x_8x_7x_5x_3x_1$ , the permutation is (1,4,8) (2,6,5,7,3).

11. Since the keyword was CIPHER, to undo the permutation of the letters, for each group of 6 ciphertext letters, we write them in the order 1st, 4th, 5th, 3rd, 2nd, 6th.

Thus the ciphertext FXFFDA XDGGDX VGGXDX is rearranged as FFDFXA XGDGDX VXDGGX. Then we consider pairs as row-column labels and decrypt them using the  $6 \times 6$  array. This gives the plaintext message *4 plus 3 is 7*.

12. The keystream is  $1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, \dots$ . It has period 15.
13. To obtain the keystream we add modulo 2 the ciphertext and the plaintext (in mod 2, addition is the same as subtraction). Thus the keystream is

$$1, 0, 0, 0, 1, 0, 1, 0 = l_1, l_2, l_3, l_4, l_5, l_6, l_7, l_8.$$

We obtain 4 equations in the 4 unknowns  $c_0, c_1, c_2, c_3$

$$\begin{aligned}l_5 &= c_0l_1 + c_1l_2 + c_2l_3 + c_3l_4 \quad \text{so } 1 = c_0 \\l_6 &= c_0l_2 + c_1l_3 + c_2l_4 + c_3l_5 \quad \text{so } 0 = c_3 \\l_7 &= c_0l_3 + c_1l_4 + c_2l_5 + c_3l_6 \quad \text{so } 1 = c_2 \\l_8 &= c_0l_4 + c_1l_5 + c_2l_6 + c_3l_7 \quad \text{so } 0 = c_1 + c_3\end{aligned}$$

Thus  $c_0 = c_2 = 1$  and  $c_1 = c_3 = 0$  so the linear recurrence relation is  $l_{i+4} = l_i + l_{i+2}$ .