Queen Mary
University of London

B. Sc. Examination by course unit 2010

MTH6115 Cryptography

Duration: 2 hours

Date and time: 9th June 2010, 10:00–12:00

Apart from this page, you are not permitted to read the contents of this question paper until instructed to do so by an invigilator.

You may attempt as many questions as you wish and all questions carry equal marks. Except for the award of a bare pass, only the best FOUR questions answered will be counted.

Calculators are NOT permitted in this examination. The unauthorised use of a calculator constitutes an examination offence.

Complete all rough workings in the answer book and cross through any work which is not to be assessed.

Candidates should note that the Examination and Assessment Regulations state that possession of unauthorised materials by any candidate who is under examination conditions is an assessment offence. Please check your pockets now for any notes that you may have forgotten that are in your possession. If you have any, then please raise your hand and give them to an invigilator now.

Exam papers must not be removed from the examination room.

Examiner(s): J. N. Bray

Question 1 (a) Explain the terms *plaintext*, *key* and *ciphertext*, as used in symmetric cryptosystems. Illustrate these terms by means of an example. [5]

(b) The following English text has been encrypted with a Caesar shift.

`LEWSHPU AOL ALYT ZALNHUVNYHWOF.`

Decrypt it, and answer the question. [5]

(c) Define the Vigenère cryptosystem for an alphabet $\mathscr{A} = \{a_0, \dots, a_{n-1}\}$, or equivalently on $\mathbb{Z}_n = \mathbb{Z}/(n)$. [5]

(d) Decipher `VVLW KGUE VVHV GOVC`, which has been encrypted using a Vigenère cipher on the English alphabet with keyword `CODE`. [4]

(e) Explain briefly how to break a Vigenère cipher, including a method to try to guess the length of the keyword of the cipher. [6]

Question 2 Let $\mathscr{A}$ be the alphabet $\{a_0, \dots, a_{n-1}\}$, where we may identify a_i with $i \in \mathbb{Z}_n$, and let C be a cipher defined over $\mathscr{A}$.

(a) Explain what it means for C to be a *substitution cipher* and an *affine substitution cipher*. [4]

(b) Decrypt the following:

`RNMZ MWIC SYGC PYAR RNMZ MUCX XMDM JM,`

which is English text that has been encrypted using an affine substitution cipher. Briefly justify your answer. [7]

(c) Why is it important that a cipher has a large number of potential keys? [2]

(d) How many essentially distinct keys are there in the following cases:

(i) A substitution cipher over an alphabet with 47 letters.

(ii) An affine substitution cipher over an alphabet of size n.

(iii) A Vigenère cipher with a key of length 50 over an alphabet of size 31.

(iv) An affine substitution cipher followed by a Caesar shift, both over the same alphabet of size 33.

[You should simplify your answer as far as possible, but it may still contain expressions like $23^6 \times 41!$. Numerical answers less than 10^8 should be evaluated explicitly.] [12]

Question 3 (a) Define an *n-bit shift register*, and explain what it means to say it is *primitive*, and give the $\mathbb{Z}_2$-polynomial corresponding to such a shift register. [7]

(b) You intercept the following bit string:

10111 11001 01001 10001 10101 01010 11100 11010 01010.

You have reason to believe that the message was converted into a bit string using the International Teleprinter Code, and then encrypted using a keystring derived from a 5-bit shift register. You have reason to believe that the message commences MI. Decrypt the message.

[*The International Teleprinter Code is given at the end of the paper*.] [11]

(c) Is the shift register of the previous part primitive? Justify your answer. [2]

(d) Let f be the polynomial corresponding to that shift register. Is f irreducible? Justify your answer. [3]

(e) Is the above keystring suitable for use as a one-time-pad? Very briefly explain your answer. [2]

Question 4 (a) Define *Euler's function* $\phi(n)$ and *Carmichael's function* $\lambda(n)$, and calculate $\lambda(12)$ from first principles. [5]

(b) Let $M \in \mathbb{Z}$ be such that $x^M \equiv 1 \pmod{n}$ whenever $\gcd(x,n) = 1$ (for example $M = \phi(n)$). Prove that $\lambda(n) \mid M$. [3]

(c) Let p and q be distinct primes. Write down the values of $\phi(pq)$ and $\lambda(pq)$. Prove that $\lambda(mn) = \mathrm{lcm}(\lambda(m), \lambda(n))$ whenever m and n are coprime. [5]

(d) Let $n = pq$, where p and q are primes with $2 < p < q$. Explain how to use knowledge of $\lambda(n)$ to obtain p and q. Illustrate your method when $n = 1961$, given that $\lambda(n) = 468$ (and n is the product of two distinct odd primes).
[You will gain no marks if you factor 1961 by trial division.] [6]

(e) Bob's RSA private key consists of primes p and q and exponents d and e, and his public key consists pq and e. What is the encryption y of the plaintext x for sending to Bob, and how does Bob recover x from y? Explain how Bob chooses e given p and q, and how he calculates d given p, q and e. [6]

Question 5 (a) What is a Latin square? Complete the following to a 5×5 Latin square, for which most of the first two rows has been given.

$$\begin{array}{ccccc} C & E & B & A & D \\ A & B & E & & \end{array}$$

[There several solutions; any solution will do.] [5]

(b) What is a one-time-pad? [4]

(c) State Shannon's Theorem. [4]

(d) A message in the 4-letter alphabet $\{0,1,2,3\}$ has been encrypted using a random keystring, with the keys uniformly distributed, and substitution table:

	0	1	2	3
0	0	2	1	3
1	2	3	2	2
2	3	0	0	0
3	1	1	3	1

The message has length 3. Before intercepting the ciphertext your estimates of the probabilities of the plaintext strings are

$$\mathrm{P}(p = 023) = \tfrac{1}{3}, \quad \mathrm{P}(p = 200) = \tfrac{2}{3},$$

with the other probabilities being 0. Calculate the probability $\mathrm{P}(z = 301)$ given the above. You intercept the ciphertext $z = 301$. Calculate the conditional probability $\mathrm{P}(p = 023 \mid z = 301)$ given this information. Does your answer contradict Shannon's Theorem? [12]

Question 6 (a) Let p be a prime, and let x be an integer such that $p \nmid x$. Define the *(multiplicative) order* of x modulo p. [3]

(b) What is a *primitive root* modulo p? (This is the same as a primitive element of $\mathbb{Z}_p$.) [3]

(c) What are the orders of 2 and 3 modulo 41? Justify your answers. [5]

(d) Are either of these primitive? If not, find a primitive element modulo 41. [4]

(e) Explain carefully the operation of the *El-Gamal cipher*. On what hard problem does its security depend? [10]

A	11000
B	10011
C	01110
D	10010
E	10000
F	10110
G	01011
H	00101
I	01100
J	11010
K	11110
L	01001
M	00111
N	00110
O	00011
P	01101
Q	11101
R	01010
S	10100
T	00001
U	11100
V	01111
W	11001
X	10111
Y	10101
Z	10001
Letters	11111
Figures	11011
Line feed	01000
Carriage return	00010
Word space	00100
All space	00000

Table 1: International Teleprinter Code

End of Paper