Queen Mary
University of London

B. Sc. Examination by course unit 2014

MTH6115 Cryptography

Duration: 2 hours

Date and time: 20 May 2014, 14:30–16:30

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 should attempt all questions. Marks awarded are shown next to the questions.

Calculators are NOT permitted in this examination. The unauthorized 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.

Important note: the Academic Regulations state that possession of unauthorized material at any time by a student who is under examination conditions is an assessment offence and can lead to expulsion from QMUL.

Please check now to ensure you do not have any notes, mobile phones or unauthorised electronic devices on your person. If you have any, then please raise your hand and give them to an invigilator immediately. Please be aware that if you are found to have hidden unauthorised material elsewhere, including toilets and cloakrooms, it will be treated as being found in your possession. Unauthorised material found on your mobile phone or other electronic device will be considered the same as being in possession of paper notes. Disruption caused by mobile phones is also an examination offence.

Exam papers must not be removed from the examination room.

Examiner(s): B. Noohi

Question 1 (a) Which method gives ciphers that are harder to break: 1) an affine substitution composed with another affine substitution; 2) a Caesar shift composed with an affine substitution then composed with another Caesar shift. Justify your answer. [4]

(b) The following cipher text has been encrypted using the affine substitution $\theta_{5,4}$:

$$QAMMYL\ JLYEC.$$

Decrypt it. [6]

(c) How many affine substitutions are there on an alphabet of size 60? How many Vigenère keys of length 10 are there on this alphabet? [6]

Question 2 (a) Define what a stream cipher on a given alphabet is, explaining all its ingredients. Explain what the advantages of a one-time pad over a Vigenère cipher are. [8]

(b) Consider the following two substitution tables on the three letter alphabet $\{a,b,c\}$:

	a	b	c
a	a	a	b
b	c	b	a
c	b	c	c

	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Suppose you want to create a secure stream cipher. Which one would you use? Justify your answer. [3]

(c) Suppose you intercepted the ciphertext

$$abbccc$$

and you have reason to believe that it has been encrypted using the left table in part (b). Suppose you also know that the key is

$$cabbac$$

Decrypt the message. [5]

Question 3 (a) Define the Euler function $\phi(n)$ and the Carmichael function $\lambda(n)$. Evaluate $\lambda(55)$. [5]

(b) Let n be an odd number such that $\phi(n) = \lambda(n)$. Prove that there is a prime number p such that $n = p^r$ for some integer $r \geq 1$. [6]

(c) Show how RSA with modulus N can be broken if $\lambda(N)$ is known. Illustrate this by factorizing 589, given that it is a product of two primes and $\lambda(589) = 90$. (The marks are for the method, not the factorisation.) [7]

Question 4 (a) Define what it means for a binary n-bit shift register to be primitive. Give an example of a primitive binary 3-bit shift register. Justify your answer. [5]

(b) The following is the first 10 digits in the output sequence of a binary 5-bit shift register:

$$0011110110.$$

Determine the rest of the sequence and its period. [8]

(c) Is this shift register primitive? Is the periodic part of the sequence you obtain in part (b) pseudo-noise? Justify your answers. [5]

Question 5 (a) Explain how the Diffie–Hellman key exchange is implemented in the RSA cryptosystem. [6]

(b) What is the knapsack problem? What is known about the complexity of the knapsack problem? [4]

(c) Suppose Alice and Bob are using the knapsack cipher and that Bob's key is

$$(22, 2, 46, 5, 100, 1, 702, 10, 351).$$

Alice sends the message 1088 to Bob. Decipher it (write your answer in the form of a binary sequence). [5]

Question 6 (a) Explain the operation of the El-Gamal cipher for encrypting messages. Which hard problem is it based on? [5]

(b) Why is it important that in Bob's El-Gamal public key (p, g, h) the number g is a primitive root mod p? Is $(97, 8, 33)$ a suitable El-Gamal public key? Justify your answer. [5]

(c) Bob's El-Gamal public key is $(83, 5, 52)$ and his secret key is $a = 9$. Bob receives the message $(2, 40)$ from Alice. Decipher it, simplifying your answer as much as possible. [7]

End of Paper