Queen Mary
University of London

B. Sc. Examination by course unit 2012

MTH6115 Cryptography

Duration: 2 hours

Date and time: 8th May 2012, 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 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 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) What is the difference between a transposition cipher and a substitution cipher? Which one would you use to confuse digram frequency analysis? [3]

(b) Find an affine substitution that encrypts b to K. Find another one. [4]

(c) Encrypt the message 'did you write your name' with a Vigenère cipher, with the key 'test'. [6]

(d) Which method gives ciphers that are harder to break: 1) a substitution cipher given by a certain permutation on the alphabet; 2) an affine cipher, composed with the substitution cipher given by a permutation on the alphabet, and then composed by another affine cipher. Justify your answer. [5]

(e) You have intercepted a ciphertext which you know has been encrypted by a Vigenère followed by an affine substitution (but you don't know the keys). How would you go about decrypting it? [7]

Question 2 (a) The following message has been encrypted using a Caesar shift. Decrypt it. [6]

```
MUUJ RAIQ COZN EUAX LOTG RKDG SY
```

(b) Two affine substitutions θ and θ' on the English alphabet have the property that $\theta(c) = \theta'(c)$ and $\theta(f) = \theta'(f)$. (That is, they both encrypt the letter c to the same letter, and also the letter f to the same letter). Prove that $\theta = \theta'$. [6]

(c) What is wrong with using a Vigenère-based crypto-system for public-key cryptography? [3]

(d) Describe in detail how you add a 'signature' to your ciphertext in public-key cryptography. Why is it that the recipient can be fairly sure that it was you, and not someone else, who added the signature to the message? [5]

(e) Define a 'trapdoor one-way' function and explain its relevance to public-key cryptography. [5]

Question 3 (a) Define an n-bit shift register and describe the associated polynomial. [6]

(b) Prove that the 5-bit shift register associated to an irreducible degree 5 binary polynomial is primitive. Is the same thing true for degree 4 polynomials? [6]

(c) Consider the shift register associated to $x^6 + x^3 + 1$. Take 000001 as input and let the shift register run indefinitely. Describe the resulting output sequence (this is an infinite sequence). Is this a primitive shift register? [6]

(d) The first six bits of the output sequence of a 3-bit shift register are 011100. Determine the next three bits of the output sequence. [7]

Question 4 (a) What is a Latin square over an alphabet $\mathscr{A} = \{a_0, \ldots, a_{q-1}\}$ of size q? [3]

(b) Write down a self-transpose Latin square on an alphabet of size 4. [3]

(c) Consider the following Latin square on the alphabet $\mathscr{A} = \{a, b, c, d\}$.

b	c	a	d
c	d	b	a
d	a	c	b
a	b	d	c

Let $\oplus$ be the binary operation on $\mathscr{A}$ obtained from the above Latin square. (We have indexed the rows, from top to bottom, and columns, from left to right, by a, b, c, and d.) Find $a \oplus b$, $(a \oplus d) \oplus c$, and $a \ominus c$. [3]

(d) Find the adjugate of the above Latin square. [6]

(e) State and prove Shannon's Theorem about one-time pads. [10]

Question 5 (a) Explain the Diffie-Hellman key exchange protocol. [7]

(b) What would go wrong if we used one-time pads to implement the Diffie-Hellman key exchange? [4]

(c) Suppose you know that 2829 is the product of two distinct prime numbers, and that $\lambda(2829) = 680$. Use this information to factorise 2829. (The marks are for the method rather than the factorisation.) [7]

(d) You are given that $T_7 : x \mapsto x^7 \pmod{299}$ is the inverse to $T_{19} : x \mapsto x^{19} \pmod{299}$. Use this information to factorise 299. (The marks are for the method rather than the factorisation.) [7]

Question 6 (a) Explain the 'discrete logarithm problem.' Is it NP-complete? Name a crypto-system which is based on the 'discrete logarithm problem.' [6]

(b) What is the order of 2 modulo 43? [5]

(c) What is a primitive root modulo p? [3]

(d) Let p be a prime number. Prove that there are exactly $\phi(p-1)$ primitive roots modulo p. (You may assume the existence of at least one primitive root.) [7]

(e) Write down all primitive roots modulo 11. [4]

End of Paper