Queen Mary
University of London

B. Sc. Examination by course unit 2015

MTH6115: Cryptography

Duration: 2 hours

Date and time: 21 May 2015, 2:30–4:30

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 unauthorised use of a calculator constitutes an examination offence.

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

Possession of unauthorised material at any time when under examination conditions is an assessment offence and can lead to expulsion from QMUL. Check now to ensure you do not have any notes, mobile phones, smartwatches or unauthorised electronic devices on your person. If you do, raise your hand and give them to an invigilator immediately. It is also an offence to have any writing of any kind on your person, including on your body. If you are found to have hidden unauthorised material elsewhere, including toilets and cloakrooms it shall 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. A mobile phone that causes a disruption in the exam is also an assessment offence.

Exam papers must not be removed from the examination room.

Examiner(s): B. Noohi

Question 1.

(a) In an encryption competition called Cipher Challenge you are permitted to use one of the following two methods to encrypt your message: A) a combination of at most 3 Vigenères with each key length at most 6, B) a combination of at most 2 Vigenères with each key length at most 9. Which method will you use? Justify your answer. **[4]**

(b) The following text has been encrypted using a Vigenère key of length 3.

```
ZHYW IQBO SUPJ DNXX
```

You have reason to believe that the plaintext starts with `What`. Decrypt it. **[6]**

(c) The Rotokas alphabet has 12 letters. How many affine ciphers are there in this alphabet? **[4]**

Question 2. Let n be a positive integer.

(a) Define the *Carmichael function* $\lambda(n)$ and the *Euler function* $\phi(n)$. **[4]**

(b) Prove that if the positive integer l is coprime to $\lambda(n)$, then the function $T_l : \mathbb{Z}_n^* \to \mathbb{Z}_n^*, x \mapsto x^l \pmod{n}$, is a bijection. Here $\mathbb{Z}_n^*$ denote the set of congruence classes modulo n coprime to n. **[6]**

(c) You are given that $T_5 : x \mapsto x^5 \pmod{221}$ is the inverse to $T_{29} : x \mapsto x^{29} \pmod{221}$. Use this information to factorise 221. (The marks are for the method not the factorisation.) **[7]**

Question 3.

(a) Define the complexity classes NP and NP-*complete*. Give an example of an NP-complete problem and explain why it is in NP. [**6**]

(b) State *Shannon's Theorem* for one-time pads. Explain, using an example, how a stream cipher produced using a substitution table that is not a Latin square can give away information about the plaintext. [**5**]

(c) The following ciphertext has been encyrpted by a stream cipher which uses a keystring generated by a 6-bit shift register:

$$Z = 10001111000010.$$

Your spies have informed you that the polynomial of this shift register is of the form $1 + ax + bx^2 + cx^3 + x^6$, but they do not know the values of a, b, c. They have also told you that the plaintext starts with

$$P = 001111101....$$

Determine the rest of the plaintext. Is this shift register primitive? [**8**]

Question 4.

(a) Explain the *Diffie-Hellman key establishment*. Why is it a fairly secure way of sharing a key? [**6**]

(b) Bob's ElGamal public key is $(p, g, h) = (71, 5, 57)$. However, this is a poorly chosen key. Explain why it is so, and exploit the weakness of the key to find Bob's secret key. (Hint: there is something wrong with $g = 5$.) [**5**]

(c) Let n be an odd positive integer. We say that a is a primitive root modulo n if a has order $\phi(n)$ modulo n. Prove that if such an a exists, then n must be of the form $n = p^r$ for some prime number p and positive integer r. [**6**]

Question 5.

(a) Let N be a positive integer. Suppose that m is a positive integer such that for every a coprime to N we have $a^m \equiv 1 \pmod{N}$. Prove that $\lambda(N)|m$. **[5]**

(b) Show that for every a coprime to 440, we have $a^{20} \equiv 1 \pmod{440}$. **[5]**

(c) Show that there exists an integer a coprime to 440 such that $a^{50} \not\equiv 1 \pmod{440}$. **[4]**

Question 6.

(a) Explain how one can use orthogonal arrays to implement a secret sharing scheme. **[6]**

(b) The following is an orthogonal array on the alphabet $\{a, b, c\}$. Determine the degree k and the strength t of this orthogonal array. **[3]**

1	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c	a	b	c
2	a	b	c	b	c	a	c	a	b	b	c	a	c	a	b	a	b	c	c	a	b	a	b	c	b	c	a
3	a	b	c	c	a	b	b	c	a	b	c	a	a	b	c	c	a	b	c	a	b	b	c	a	a	b	c
4	a	a	a	a	a	a	a	a	a	b	b	b	b	b	b	b	b	b	c	c	c	c	c	c	c	c	c

(c) Use this orthogonal array to share the password *acacba* between your three vice-presidents VP1, VP2 and VP3 so that three of them together can recover the password but no two of them can. **[6]**

(d) In your method explain in detail why if only VP1 and VP2 are present they cannot get any clue about the password. **[4]**

End of Paper.