Queen Mary
University of London

B. Sc. Examination by course unit 2009

MTH6115 Cryptography

Duration: 2 hours

Date and time: 28 May, 10:00

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 4 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.

Candidates should note that the Examination and Assessment Regulations state that possession of unauthorized 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): Bill Jackson

 TURN OVER

Question 1 Let C be a cipher defined over the alphabet $A = \{a, b, c, \ldots, z\}$.

(a) Explain what it means to say that C is a *substitution cipher* and an *affine substitution cipher.* [4]

(b) Give a brief description of how you might break each of these ciphers, if you know that the plaintext is a piece of English text. [10]

(c) Decrypt the following ciphertext which has been encrypted using an affine substitution cipher. Explain how you obtain your solution.

YGVIV BDYIX TKMVP YYGVK PCR

[11]

Question 2 (a) Explain how a *stream cipher* and a *Vigenère cipher* work. [5]

(b) Describe briefly how a Vigenère cipher can be broken if the period of the keyword is small compared to the length of the ciphertext. [10]

(c) The following ciphertext has been encrypted using a Vigenère cipher.

FHVSOWKZQEADSJKZQDNY

Determine the likely value(s) for the period of the keyword. Can you be certain that the the keyword takes one of these values? Why? [5]

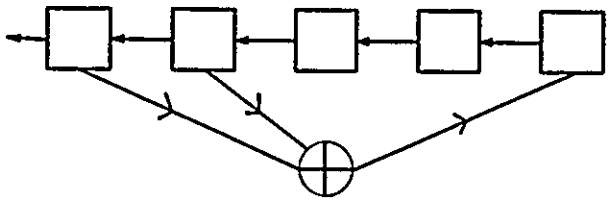
(d) A plaintext message is encrypted using a Vigenère cipher and the resulting ciphertext is then re-encrypted using a substitution cipher. Prove that this combined cipher is a stream cipher by constructing its keyword and substitution table. [5]

Question 3 (a) Define an *n-bit shift register* and explain what it means to say that it is *primitive.* [5]

(b) Describe how a shift register can be used to encrypt a plaintext over the binary alphabet. [4]

(c) State a condition which can be used to deduce that a shift register is not primitive without computing its output sequence, taking care to define each of the terms you use. [4]

(d) Use the condition from (c) to test whether the following shift register could be primitive.



[6]

(e) The ciphertext 1100111010101010 has been encrypted using a 4-bit shift register. Determine the shift register given that the first 10 bits of the plaintext were 00101100. [6]

Question 4 (a) State the conditions that a stream cipher must satisfy in order to be a *one-time pad* cipher. [4]

(b) State and prove Shannon's theorem for one-time pad ciphers, taking care to define the random variables used in the statement of the theorem. Explain the significance of this result for the security of a one-time pad cipher. [10]

(c) Alice uses a one-time pad to send Bob a plaintext which is a piece of English text. Would the security of the cipher be compromised if:

(i) Eve knew the substitution table that Alice and Bob were using but not the keyword?

(ii) Eve knew the keyword that Alice and Bob were using but not the substitution table?

Give brief justifications for your answers. [6]

(d) State Kolmogorov's definition of a random sequence and explain why the output sequence of an m-bit shift register does not satisfy this definition. How would you construct a binary sequence which does satisfy the definition? [5]

Question 5 (a) Define Euler's phi-function $\phi(n)$ and Carmichael's lambda-function $\lambda(n)$. Prove that if $\gcd(x, n) = 1$ then $x^{\phi(n)} \equiv 1 \bmod n$ and deduce that $\lambda(n)$ is a divisor of $\phi(n)$ for every n. [8]

(b) Let p and q be distinct primes. Give, with proof, explicit formulae for $\phi(pq)$ and $\lambda(pq)$. [You may use the Chinese Remainder Theorem and also assume that $\lambda(p) = p - 1$.] [7]

(c) Bob's RSA private key consists of primes p, q and exponents e, d, and his public key consists of pq and e. Explain how Bob should choose e, given p and q. Explain how he calculates d, given p, q and e. Why can Eve not use the same method to calculate d, given pq and e? [5]

(d) Bob has chosen $pq = 1599$ and $e = 1323$. Explain in detail how you would encrypt the plaintext 539 for sending to Bob. [You do not need to perform the encryption.] [5]

Question 6 (a) What is a *primitive root* modulo a prime p? Write down, without proof, an expression for the number of primitive roots modulo p. [4]

(b) Decide, with proof, whether or not 2 is a primitive root modulo 29. [4]

(c) What is the *discrete logarithm problem*? [2]

(d) Explain the operation of the El-Gamal cipher system for encrypting and decrypting messages. Why is it a secure system? [15]

End of Paper