Queen Mary
University of London

B.Sc. EXAMINATION BY COURSE UNITS

MAS335 Cryptography

30 May 2008, 10:00–12:00

The duration of this examination is two *hours.*

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 five *questions answered will be counted. Show your calculations.*

Calculators are not *permitted in this examination.*

YOU ARE NOT PERMITTED TO START READING THIS QUESTION PAPER UNTIL INSTRUCTED TO DO SO BY AN INVIGILATOR

1. (a) [3 marks] Explain the terms *plaintext*, *key* and *ciphertext*, as used in symmetric cryptosystems.

   (b) [7 marks] Explain how the Vigenère cipher works, and illustrate by decrypting the ciphertext

   `GOYBXLGDEMHKMPFGR`

   which has been encrypted with the key `EXAM`.

   (c) [4 marks] Explain briefly how a Vigenère cipher can be broken.

   (d) [3 marks] What is the likely key-length in the following ciphertext, which has been encrypted with a Vigenère cipher? Why?

   `VYCRTHYRTAFVYCBTF`

   (e) [3 marks] What effective measures can be taken to improve the security of a Vigenère cipher?

2. (a) [6 marks] Explain how a simple substitution cipher works, and describe briefly how it can be broken.

   (b) [3 marks] What methods could you employ to make a substitution cipher harder to break?

   (c) [1 mark] Alice and Bob decide to use a simple substitution cipher with an alphabet of 75 symbols, consisting of 52 upper and lower case letters, 10 digits, 12 punctuation marks, and space. How many possible keys are there for this cipher?

   (d) [5 marks] What differences would you expect to see in the frequency analysis for this cipher as opposed to the usual 26-letter alphabet?

   (e) [5 marks] Would this cipher be harder or easier to break than the standard substitution cipher? Give reasons.

3. (a) [4 marks] What is a Latin square? Complete the following to a Latin square:

   R P Q T S
   P R S Q T

   (b) [3 marks] What is a one-time-pad?

   (c) [10 marks] State and prove Shannon's Theorem.

   (d) [3 mrks] What are the two main problems which may arise with a stream cipher if the substitution table is not a Latin square?

[Next question overleaf]

4. (a) [8 marks] Define Euler's function $\phi(n)$ and Carmichael's function $\lambda(n)$, and prove that $\lambda(n)$ is a divisor of $\phi(n)$. Calculate $\lambda(8)$ from first principles.

   (b) [4 marks] Prove that if m and n are coprime positive integers, then $\lambda(mn) = \mathrm{lcm}(\lambda(m), \lambda(n))$. Give an example to show that this is not true if we drop the condition that m and n are coprime.

   (c) [2 marks] Hence write down a formula for $\lambda(pq)$ where p and q are primes, and calculate $\lambda(31.53)$.

   (d) [6 marks] Suppose you are told that n is a product of two distinct primes, and you are told the value of $\lambda(n)$. Explain how to factorise n, and carry out your procedure when $n = 851$ and $\lambda(n) = 396$.

5. (a) [5 marks] What is a primitive root mod p, where p is a prime? Show that 2 is a primitive root mod 13, and find a primitive root mod 19.

   (b) [5 marks] Explain how to calculate $x^a \bmod p$ efficiently. If a lies between 2^m and 2^{m+1}, approximately how many arithmetical operations are required for this calulation?

   (c) [10 marks] Explain the El-Gamal public-key cryptosystem. On what hard problem does its security depend? Why is it important for Alice to choose her encryption exponent randomly?

6. (a) [10 marks] What is the knapsack problem? Explain the Merkle–Hellman public-key cryptosystem based on this problem.

   (b) [10 marks] Explain how a Latin square can be used to construct a secret-sharing scheme. How many people share the secret, and what is the minimum number who can together reconstruct the secret?

[End of examination paper]