Queen Mary
University of London

B. Sc. Examination 2007

MAS 335 Cryptography

Duration: 2 hours

Date and time: 29 May 2007, 14:30–16:30

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 5 questions answered will be counted.

Calculators are NOT permitted in this examination. The unauthorised use of a calculator constitutes an examination offence.

© Queen Mary, University of London 2007

Question 1 (20 marks)

(a) Explain the terms *plaintext*, *ciphertext* and *key*. Illustrate by means of an example. [4]

(b) Decrypt the following question, and then answer it:

```
ADIY ORJ ZIBGDNC RJMYN RCDXC VMZ HVKKZY
JIZ JIOJ OCZ JOCZM WT V XVZNVM NCDAO
```

[6]

(c) Explain how a substitution cipher works, and explain briefly how a simple substitution cipher can be broken. What improvements can you suggest which would make a substitution cipher more difficult to break? [10]

Question 2 (20 marks)

(a) Why is it important for the number of possible keys to a cipher to be large? [3]

(b) Why is it important for the key to a cipher to be chosen *randomly* from this large number of possibilities? [3]

(c) How many possible keys are there in the following cases:

(i) A Vigenère cipher with key of length 100 over an alphabet of 26 letters.

(ii) A substitution cipher over an alphabet of 100 letters.

(iii) A stream cipher based on a primitive binary shift register with 100 bits.

[9]

(d) Alice and Bob have decided to use a combination of a Vigenère cipher and a substitution cipher to encrypt their messages. Should they do the substitution first, followed by the Vigenère, or should they do the Vigenère first and then the substitution? Or does it make no difference? Why? [5]

Question 3 (20 marks)

(a) Define the term *Latin square* over an alphabet A. Prove that $n \times n$ Latin squares exist for all natural numbers n. [4]

(b) Explain how a Latin square can be used in conjunction with a random string over A to create a stream cipher. [4]

(c) State and prove Shannon's Theorem for such a stream cipher. [8]

(d) Give an example to show that Shannon's Theorem does not necessarily hold if the substitution table is not a Latin square. [2]

(e) What other problems might arise if the substitution table is not a Latin square? [2]

Question 4 (20 marks)

(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. [6]

(b) Let p and q be distinct primes. Give, with proof, explicit formulae for $\phi(pq)$ and $\lambda(pq)$. [You may assume that $\lambda(p) = p-1$.] [6]

(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 calculate d, given pq and e? [4]

(d) Bob has chosen $pq = 1147$ and $e = 257$. Explain in detail how you would encrypt the plaintext 233 for sending to Bob. [You do not need to perform the encryption.] [4]

© Queen Mary, University of London 2007

Question 5 (20 marks)

(a) What is a *primitive root* modulo a prime p? Prove that the number of primitive roots modulo p is $\phi(p-1)$.

[You may assume that every non-zero element of $\mathbb{Z}/(p)$ has order dividing $p-1$, and that every polynomial of degree k over $\mathbb{Z}/(p)$ has at most k roots. You may also assume that $\sum_{d|n} \phi(d) = n$ for any $n > 1$.] [8]

(b) Decide, with proof, whether or not 2 is a primitive root modulo 37. [2]

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

(d) Explain the operation of the El-Gamal system for sending encrypted messages. [8]

Question 6 (20 marks)

(a) Describe the basic protocols of public-key cryptography: *message encryption*, *key exchange*, and *digital signature*. In each case, describe a situation in which it might be used in practice. [10]

(b) Describe in detail an implementation of digital signatures, using either the RSA or the El-Gamal cryptosystem to sign encrypted messages. [10]

Question 7 (20 marks)

(a) Define an *orthogonal array* of *strength* t and *degree* k over an alphabet A, and describe how it can be used to create a secret-sharing scheme. [8]

(b) Give an example of an orthogonal array of strength 2 and degree 3 over the alphabet $\{a,b,c,d\}$. [2]

(c) Let F be any field, and let $a_1,\ldots,a_t$ and $b_1,\ldots,b_t$ be any elements of F. Prove that there is a unique polynomial $f(x)$ of degree less than t, with coefficients in F, satisfying $f(a_i) = b_i$ for all $1 \le i \le t$. [4]

(d) Show how this property of polynomials can be used to construct an orthogonal array. [6]

© Queen Mary, University of London 2007 **END OF EXAMINATION**