GX1592

OLLSCOIL NA hÉIREANN, GAILLIMH

NATIONAL UNIVERSITY OF IRELAND, GALWAY

SUMMER EXAMINATIONS 1999

CRYPTOGRAPHY (CS402)

Professor J. Wiegold
Dr. M. Batty

Time allowed: three hours.
Attempt *five* questions.

1. (a) An affine enciphering transformation $x \mapsto \alpha x + \beta$ of single letter message units in a 26-letter alphabet

$$A = 0, \ldots, Z = 25$$

is used to produce the following ciphertext.

NJIHIENEITIQNSULGINYAYSLIQTIQNSQ

Use frequency analysis to determine the deciphering key and the first three words of plaintext.

(b) Why would $(\alpha = 12, \beta)$ not be a valid enciphering key, regardless of the value of β? How many valid enciphering keys are there?

P. T. O.

2. You intercept the 16-letter message

DDA? CCQ'JRY H'R

which was sent using a linear matrix cryptosystem

$$\begin{bmatrix} x \\ y \end{bmatrix} \mapsto A \begin{bmatrix} x \\ y \end{bmatrix}$$

on digraph message units in a 29-letter alphabet

$$A = 0, \ldots, Z = 25, \langle \text{space} \rangle = 26, ? = 27, ' = 28.$$

The last five letters of plaintext are the sender's signature "ALICE". Determine the inverse of the enciphering matrix A and decipher the message. Then use the enciphering matrix to encipher "IT'S BOB".

3. (a) Use modular exponentiation to calculate $288^{13} \bmod 2911$.

   (b) Describe the RSA cryptosystem (omitting any proofs) and explain how it may be regarded as a public key cryptosystem.

   (c) Use the RSA cryptosystem with the 26-letter alphabet

   $$A = 0, \ldots, Z = 25,$$

   enciphering key ($n = 2911 = 41 \times 71, e = 13$), digraph plaintext message units and trigraph ciphertext message units to encipher the message "HI". Calculate d such that (n, d) is the deciphering key.

P. T. O.

4. (a) What is (i) the *knapsack problem*? (ii) the *superincreasing* knapsack problem. Describe an algorithm to solve the superincreasing knapsack problem.

   (b) The knapsack cryptosystem with $N = 61$, $b = 18$ and deciphering key

   $$K_D = \{n_1 = 2, n_2 = 3, n_3 = 7, n_4 = 15, n_5 = 31\}$$

   is used on single letter message units in a 26-letter alphabet to produce the ciphertext

   120 143 103 120

   Determine the corresponding plaintext. Find the enciphering key and encipher the message "YES".

5. (a) Define the following terms: (i) *pseudoprime to the base b*, (ii) *Carmichael number* and (iii) *square-free number.*

   (b) Show that if n is a square-free number and $p - 1$ divides $n - 1$ for every prime p which divides n then n is a Carmichael number.

   (c) Hence show that if m is a positive integer such that $6m+1$, $12m+1$ and $18m + 1$ are all primes then

   $$n = (6m + 1)(12m + 1)(18m + 1)$$

   is a Carmichael number. (Hint: show that $n - 1$ is divisible by $36m$).

6. (a) Describe Fermat's factorisation technique. Use it to express the integer 809009 as a product of two primes. When, in general, will Fermat's method work?

   (b) Let $Q(x) = x^2 - 2041$. Find an integer v such that

   $$v^2 = Q(46)Q(47)Q(49)Q(51).$$

   Then use Kraitchik's method to express 2041 as a product of two primes.

P. T. O.

7. (a) What is an *elliptic curve* over a field of characteristic different from 2 or 3? Describe by means of pictures the operation under which the points on an elliptic curve form an abelian group, distinguishing carefully between cases.

   (b) If $P = (x, y)$ with $y \neq 0$ on the elliptic curve $y^2 = x^3 - x$ over $\mathbb{Z}_5$ then the point $2P = P + P$ is given by the formula

$$\left(x', -y + (2y)^{-1}(3x^2 - 1)(x - x')\right),$$

   where

$$x' = ((2y)^{-1}(3x^2 - 1))^2 - 2x.$$

   Show that the point $(2, 1)$ lies on the elliptic curve $y^2 = x^3 - x$ over $\mathbb{Z}_5$. Find the point $2(2, 1)$.

8. (a) What is meant by the *discrete logarithm problem* in $(\mathbb{Z}^n)^*$? Show that $\log_2 7 = 6 \bmod 19$.

   (b) Describe the ElGamal cryptosystem and explain how a procedure to solve the discrete logarithm will crack the cryptosystem.

   (c) Explain briefly how the ElGamal cryptosystem may be adapted to give an elliptic curve cryptosystem.