Gx 2016

OLLSCOIL NA hÉIREANN, GAILLIMH
NATIONAL UNIVERSITY OF IRELAND, GALWAY

SUMMER EXAMINATIONS 2004

CRYPTOGRAPHY (CS402)

Dr Dave Johnson
Dr Dane Flannery

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

1. (a) An affine encryption function $f(n) \equiv an + b \bmod 41$ has been used on plaintext composed of symbols from the alphabet

   ABCDEFGHIJKLMNOPQRSTUVWXYZØ123456789;,.?!

   to produce the following ciphertext:

   7NIIXI9ONPEBX,BG7QP7IULVQEOE7I9

   Use frequency analysis to determine the encryption key (a, b) (assume that after "E", "T" is the most frequently occurring letter in plaintext messages of reasonable length written in English). Hence determine the decryption function and the plaintext.

   (b) Consider the affine encryption function $f(n) \equiv an + b \bmod p$, where p is prime and $a \not\equiv 1$. Show that there is always a symbol in the message alphabet that is the same when encrypted. What is that symbol in part (a)?

2. You intercept the following message

   ANXW□BAJIJEVPKX?GNUI?FP!

   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 (i.e. each unit consists of two symbols) in the 29-letter alphabet

   A=Ø,...,Z=25,□ = 26,?=27,!=28

   The last six letters of plaintext are the sender's signature "SHEILA". Determine the inverse of the encryption matrix A and decrypt the message. Then use A to encrypt "TOO□RIGHT!".

p.t.o.

3. (a) What are the basic features of a *public key* cryptosystem? Briefly describe encryption and decryption in the RSA cryptosystem (omit proofs).

   (b) Calculate $482^{13} \bmod 2911$ by repeated squaring.

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

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

   the encryption key ($n = 2911 = 41 \times 71$, $e = 13$), digraph plaintext message units, and trigraph (i.e. 3 symbols) ciphertext message units, to encrypt the message "SOSO". Calculate d such that (n, d) is the decryption key.

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

   (b) A knapsack cryptosystem with $m = 61$, $a = 17$ and decryption key

   $$K_D = \{v_0 = 2, v_1 = 3, v_2 = 7, v_3 = 15, v_4 = 31\}$$

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

   $$23 \quad 58 \quad 85$$

   Determine the corresponding plaintext. Find the encryption key. Encrypt the message "WHY".

5. (a) Define: (i) *pseudoprime to the base b*, (ii) *Carmichael number*.

   (b) Let $n = pq$ where p and q are primes, $p \neq q$. Set $d = \gcd(p-1, q-1)$. Let b be an integer coprime to n, $1 < b < n$. Prove that n is pseudoprime to the base b if and only if $b^d \equiv 1 \bmod n$.

   (c) Suppose that $b^{n-1} \equiv 1 \bmod n$ for k choices of base b. If n is not a Carmichael number, show that the probability that n is prime is at least $1 - \frac{1}{2^k}$. Discuss how this fact may be used in a probabilistic primality test.

6. (a) Use the Fermat factorisation technique to find proper factors of 92296873. State (with justification) whether the factors you obtain are prime. What is the relevance of Fermat factorisation to RSA?

   (b) Describe Pollard's factorisation method. Carefully explain why the method is unlikely to find the prime factorisation 383×1283 of 491389.

7. (a) What is an *elliptic curve* over a field of characteristic different from 2 or 3? Describe, using a suitable picture, how to add two points on an elliptic curve over $\mathbb{R}$, to obtain a uniquely defined third point on the curve.

   (b) Sketch a graph of the elliptic curve over $\mathbb{R}$ determined by $y^2 = x^3 - x$, and from this sketch determine the sum of the points $(-1, 0)$ and $(1, 0)$ on the curve.

   (c) Find the order of the group of points on the elliptic curve over $\mathbb{Z}_p$ determined by $y^2 = x^3 - x$, where p is a prime, $p \equiv 3 \bmod 4$.