Some Problems for Math 626
Cryptography

Michael E. O'Sullivan
mosulliv@math.sdsu.edu
www-rohan.sdsu.edu/ ~ mosulliv

A. Let τ and σ be permutations of a set A. Suppose that $(a_1, \ldots, a_t)$ is a cycle of σ (the a_i are distinct elements of A with $\sigma(a_i) = a_{i+1}$ and $\sigma(a_t) = a_1$). Show that $(\tau(a_1), \ldots, \tau(a_t))$ is a cycle for $\tau\sigma\tau^{-1}$.

B. This problem is a highly simplified ingredient of Turing's analysis of the Enigma. Recall that the permutation implemented by the enigma is represented by $\tau\sigma^{-1}\theta\sigma\tau$ where θ is constant (due to the reflector), τ is determined by the plugboard settings and σ is determined by the scrambler settings (the order in which the three scramblers are placed in the machine, and the setting for each). Suppose that you have managed to identify a plaintext string of characters $m_1, m_2, \ldots, m_t$ that is transformed into ciphertext $m_2, m_3, \ldots, m_t, m_1$, using a fixed plugboard setting τ and the sequence of scrambler settings $\sigma_1, \sigma_2, \ldots, \sigma_t$ (so $\tau\sigma_i^{-1}\theta\sigma_i\tau(m_i) = m_{i+1}$ and $\tau\sigma_t^{-1}\theta\sigma_t\tau(m_t) = m_1$). Let τ' be a different plugboard setting. Find a message $m_1', \ldots m_t'$ that is transformed into $m_2', m_3', \ldots, m_t', m_1'$ using plugboard setting τ' and the same sequence of scrambler settings. This fact can be used to separate the effect of the plugboard settings from the scrambler settings: the length of the orbit was independent of the plugboard settings.

C. Let p and q be odd primes. Use the Chinese Remainder theorem to express the four square roots of 1 in $\mathbb{Z}/pq$. Find them explicitly when $q = 2p + 1$.

D. Let $p = 29$ and $q = 43$ and consider the RSA cryptosystem with $n = pq$. Fiddle with the Chinese Remainder Theorem to find a simple formula for d, the decrypting exponent, as a function of e, the encrypting exponent.

E. To protect against the RSA attacks discussed in class we might choose $n = pq$ with

$$p = 2p' + 1 \qquad q = 2q' + 1$$
$$p' = 2p'' + 1 \qquad q' = 2q'' + 1$$

with all p's and q's prime numbers.

(a) How many enciphering exponents e give distinct RSA encryptions?

(b) What is the maximum possible order of an enciphering exponent, where the order is the minimal k such that $X^{(e^k)} = X \mod n$?

(c) How many e have this order?

(d) Answer the previous three questions for the following values of n i) 722329, and ii) 1,034,641 (only ii is in the form given above).

F. For each of the following RSA keys, one of the attacks described in class is very effective. Write Maple code for Fermat factorization, for attempting to find the decryption key, and for iterative attack. Then use these to factor n.

$$(n := 1571068647977 \quad e := 61165167623)$$
$$(n := 2117470765609, \quad e := 8609599)$$
$$(n := 18021426084869, \quad e := 17907786722857)$$

G. Different values of q can give fields with quite different structures. Consider $q = 121, 125, 127, 128, 131$. Answer each of the following questions for each value of q. Then discuss which would be best for a cryptosystem defending against the Silver-Pohlig-Hellman algorithm.

(a) Find a primitive element

(b) Find the total number of primitive elements.

(c) Identify all of the primitive elements.

H. In Koblitz' Exercise IV.3 #7 he says that using a Fermat prime for a discrete log system is "an astonishingly bad idea." The algorithm he describes for computing discrete logs is essentially a simple version of the Silver-Pohlig-Hellman algorithm. Write Maple code to implement the algorithm. For each of the Fermat primes 17, 257 and 65537 compute the discrete log of 5 base 3.

I. (from Stinson) Frank uses the Merkle-Hellman Cryptosystem with public key $t = (1394, 1256, 1508, 1987, 439, 650, 724, 339, 2303, 810)$. Suppose Oscar discovers that p=2503.

(a) By trial and error determine the value of a such that the list $t * a^{(-1)} \mod p$ is a permutation of a superincreasing list.

(b) Decrypt 5746.

J. Mc Suppose there were an error correcting code over $\mathbb{F}_{16}$ with parameters $n = 256$, and $k = 178$ correcting $t = 21$ errors with a computationally efficient decoding algorithm. Discuss the advantages/disadvantages of using this code in a McEliece type of cryptosystem instead of McEliece's original Goppa code with parameters $n = 1024$, $k = 524$, $t = 50$ over $\mathbb{F}_2$. Consider the construction of public/private keys, the key sizes, the rate of the code and the security of the cryptosystem.

K. Verify Bezout's theorem for the following pairs of curves over the Complex numbers.

(a) $y = x^3$ and $x = 0$.

(b) $y = x^3$ and $y = 1$

(c) $y = x^3 - x^2$ and $y = x^2$.

(d) $y^2 = x^3 - 3x$ and $x = y^2$.

(e) $y^2 = x^3 + x$ and $x = y^2$.