Math 435, Spring Semester 2000-01 NAME:
R.A. Brualdi
SOLUTIONS TO Mid-term Exam II: April 18, 2001 Total Points:

1. [25 points] **Show your work.**

(a) [5 points] Compute $\phi(385)$ (Euler phi-function)

$385 = 5 \cdot 7 \cdot 11$ so $\phi(385) = 385 \cdot (1 - 1/5)(1 - 1/7)(1 - 1/11) = 240$

(b) It is easy to check that 2 is a primitive root modulo 11 (you need not do so).

(bi) [5 points] What is the discrete log, base 2, of 10 in $Z/11$?

$2^5 = 10\%11$ so the discrete log is 5.

(bii) [5 points] Which element in $Z/11$ has discrete log, base 2, equal to 8?

$2^8 = 3\%11$ so 3 has discrete log equal to 8.

(c) [10] Let

$$A = \begin{bmatrix} 3 & 1 & 2 \\ 0 & 4 & 3 \\ 0 & 0 & 5 \end{bmatrix} \quad b = \begin{bmatrix} 1 \\ 5 \\ 1 \end{bmatrix}, \text{ and } E(x) = Ax + b, \; x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}.$$

Does $E(x)$ define a Hill cipher, block size 3, over $Z/26$? EXPLAIN.

$\det(A) = 3 \cdot 4 \cdot 5 = 60 = 8\%26$. Since 8 is not invertible in $Z/8$, it does not define a Hill Cipher. [Some of you argued, rightly so, that this is not a Hill cipher since it has an "affine part," namely b. This was my mistake.]

2. [25 points] THIS PROBLEM REFERS TO AES.

(a) [12 points] To what is the S-box applied and describe the two steps in its construction:

The S-box is applied to the input array. First each nonzero element is replaced by its (mult.) inverse in GF(2^8). Then an affine transformation (over $Z/2$) is applied to the resulting element consider as a byte.

(b) In the rounds of AES, the columns of the state array, considered as polynomials over the field $GF(2^8)$ are *mixed* by multiplying, modulo $x^4 + 1$ by the fixed polynomial

$$a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$$

whose coefficients come from $GF(2^8)$, given in hexadecimal form.

(bi) [8 points] Verify that $a(x)$ has an inverse modulo $x^4 + 1$.

$x^4 + 1 = (x + 1)^4$ and so 1 is its only root. But simple computation shows that $a(1) \neq 0$, and hence $a(x)$ has no factor in common with $x^4 + 1$, that is, they are relatively prime.

(bii) [5 points] Why is it important that $a(x)$ have such an inverse?

Otherwise, when we multiply we cannot invert, and so the operation is not one-to-one, and we cannot reverse the steps uniquely.

3. [25 points] EXPONENTIAL CIPHERS AND RSA

(a) [10 points] The integer $p = 101$ is a prime number. Let $e = 43$ and observe that $43 \cdot 7 = 1\%100$. If the integer 05 is received using an exponential cipher ($n = 1$) with parameters p and e, what integer was sent?

$x^{43} = 05\%101$ and so $(05)^7 = 52\%101$ by Fermat's Theorem.

(b) [15 points] Consider the two "large" primes $p = 5$ and $q = 7$ where $\phi(35) = 24$. Let $e = 11$. Into what is the integer 10 encrypted by RSA with these parameters?

$(10)^{11} = 5\%35$

4. [25 points] ElGamal and Knapsack Ciphers

(a) [15 points] Consider a ElGamal cipher, and suppose Alice's public key is p, b, c. Bob sends Alice an integer x ($0 \leq x < p$) which is encrypted by ElGamal to y. How does Bob do this (formula etc.) and how does Alice decrypt y to get x?

Alice's private key is the discrete log l of c with base b and modulo p. Bob chooses a random integer r, and sends $b^r\%p$ in the header, and $y = c^r x\%p$ in the message. Alice uses her private key (the discrete log l of c with base b) and computes $(b^r)^l = (b^l)^r = c^r\%p$. Then Alice computes $(c^r)^{-1}$ using the Euclidean algorithm e.g., and then decrypts with $x = (c^r)^{-1}y\%p$.

(b) [10 points] Consider a knapsack vector $\vec{a} = (2, 5, 8, 20)$. What is the knapsack function, and its domain, for this knapsack vector? If Alice wants to post this vector on her website as her public key for knapsack ciphers, what should she do/post? Describe the encryption function for encrypting an integer x with $0 \leq x \leq 15$.

The knapsack function is $f(x_1, x_2, x_3, x_n) = x_1a_1 + x_2a_2 + x_3a_3 + x_4a_4 = 2x_1 + 5x_2 + 8x_3 + 20x_4$; its domain is the set of all 4-tuples of bits, i.e. integers 0 to 15. The knapsack vector is superincreasing and so need to be disguised by choosing an integer $m > 2 + 4 + 8 + 20$ (the largest number in the range of f) and an integer t relatively prime to m. She then uses $(t2\%m, t5\%m, t8\%m, t20\%m)$ in place of the given vector (this is the vector posted on her website). Encryption is done as above but using this disguised vector.