MATH/CS/ECE 435; Mid-Term Exam, 100 points, March 10, 2005 (R.A.Brualdi)

TOTAL SCORE (6 problems; 100 points possible):

Name:

1. [10 points] Determine the all the **units** in $Z/24Z$.

The $\phi(26) = 8$ integers between 1 and 26 that are relatively prime to 26, that is, 1, 5, 7, 11, 13, 17, 19, 23.

2. [15 points] Use the **technique of the Chinese Remainder Theorem** to find the least nonnegative solution of the simultaneous congruences:

$$\begin{aligned} x &\equiv 1 \bmod 7 \\ x &\equiv 5 \bmod 12 \\ x &\equiv 3 \bmod 5. \end{aligned}$$

Let $m = 7 \cdot 12 \cdot 5 = 420$ and let $M_1 = m/7 = 60, M_2 = m/12 = 35$, $M_3 = m/5 = 84$. We need to compute the inverses of the M_1, M_2, M_3 modulo 7, 12, 5, respectively. Since 60 mod 7 is 4, 35 mod 12 is 11, and 84 mod 5 is 4, by inspection we see that these inverses are 2, 11, and 4, respectively. Now let

$$x = 1 \cdot 2 \cdot 60 + 5 \cdot 11 \cdot 35 + 3 \cdot 84 \cdot 4 = 3053 \equiv 113 \bmod 420.$$

Then 113 is the required solution.

3. [20 points] The ciphertext YIFZMA was encrypted by a Hill/linear cipher of block length 2 with the matrix

$$A = \begin{bmatrix} 9 & 13 \\ 2 & 3 \end{bmatrix}.$$

Find the plaintext.

We use the identification:

A-0, B-1, C-2, D-3, E-4, F-5, G-6, H-7, I-8, J-9, K-10, L-11, M-12, N-13, O-14, P-15, Q-16, R-17, S-18, T-19, U-20, V-21, W-22, X-23, Y-24, Z-25 and the arithmetic in $Z/26Z$.

Let the plaintext to be determined by abcdef where $a, b, c, d, e, f \in Z/26Z$. One checks that the determinant of A is 1, and that

$$A^{-1} = \begin{bmatrix} 3 & 13 \\ 24 & 9 \end{bmatrix}.$$

Since YIFZMA is 24, 8, 5, 25, 12, 0, we have

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 3 & 13 \\ 24 & 9 \end{bmatrix} \begin{bmatrix} 24 \\ 8 \end{bmatrix} = \begin{bmatrix} 7 \\ 25 \end{bmatrix}, \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} 3 & 13 \\ 24 & 9 \end{bmatrix} \begin{bmatrix} 5 \\ 25 \end{bmatrix} = \begin{bmatrix} 2 \\ 7 \end{bmatrix}$$

$$\begin{bmatrix} e \\ f \end{bmatrix} = \begin{bmatrix} 3 & 13 \\ 24 & 9 \end{bmatrix} \begin{bmatrix} 12 \\ 0 \end{bmatrix} = \begin{bmatrix} 10 \\ 2 \end{bmatrix}$$

So the plaintext is UYCHKC.

4. [20 points] A Vigenère cipher, where the alphabet is $Z/5Z$ (the integers mod 5) is being used. The encipherment of the plaintext
$1, 4, 3, 2, 0, 1, 1, 4, 3, 3, 1, 2$ is $3, 0, 1, 0, 4, 3, 3, 0, 1, 1, 0, 4$.

Decipher the encrypted message: $3, 3, 2, 4, 1, 1, 1, 0, 3, 4, 2, 1$.

We have that

$$3, 0, 1, 0, 4, 3, 3, 0, 1, 1, 0, 4 - 1, 4, 3, 2, 0, 1, 1, 4, 3, 3, 1, 2 = 2, 1, 3, 3, 4, 2, 2, 1, 3, 3, 4, 2$$

so we guess the key length is 6 and the key is 2,1,3,3,4,2. Thus the plaintext is

$$3, 3, 2, 4, 1, 1, 1, 0, 3, 4, 2, 1 - 2, 1, 3, 3, 4, 2, 2, 1, 3, 3, 4, 2 = 1, 2, 4, 1, 2, 4, 4, 4, 0, 1, 3, 4.$$

5. [20 points] Suppose that $\mathcal{P} = \{a, b\}$, $\mathcal{K} = \{k, l\}$, and $\mathcal{C} = \{X, Y\}$. Let the probability distributions on $\mathcal{P}$ and $\mathcal{K}$ be:

$$Pr(a) = 1/3 \text{ and } Pr(b) = 2/3; \quad Pr(k) = 1/4 \text{ and } Pr(l) = 3/4.$$

Let the encryption function work like:

$$E_k(a) = X, E_k(b) = Y, \quad \text{and } E_l(a) = Y, E_l(b) = X.$$

1. Compute $Pr(X)$ and $Pr(Y)$

$$Pr(X) = Pr(0)Pr(k) + Pr(b)Pr(l) = (1/3)(1/4) + (2/3)(3/4) = 7/12;$$

   so $Pr(Y) = 1 - Pr(X) = 5/12$.

2. Compute $Pr(a|X)$, $Pr(b|X)$, $Pr(a|Y)$, and $Pr(b|Y)$.

$$Pr(A|X) = \frac{Pr(a \cap X)}{Pr(X)} = \frac{(1/3)(1/4)}{7/12} = \frac{1}{7};$$

   so $Pr(b|X) = 1 - (1/7) = 6/7$.

   Also

$$Pr(a|Y) = \frac{(a \cap Y)}{Pr(Y)} = \frac{(1/3)(3/4)}{5/12} = \frac{3}{5};$$

   so $Pr(b|Y) = 1 - (3/5) = 2/5$.

3. Does this cryptosystem have perfect secrecy? **Explain.**

   No, since e.g. $Pr(a|X) = 1/7 \neq Pr(a) = 1/3$.

6. [15 points] There are 4 basic steps for the computation of the Feistel Cipher $f_K(R)$ in DES, where R has 32 bits. Explain them.

(1) Expansion of R to 48 bits $E(R)$

(2) $E(R) \oplus K = B_1 B_2 \dots B_8$ where each B_i has 6 bits

(3) $B_i = a_{i1}a_{i2}a_{i3}a_{i4}a_{i5}a_{i6}$ and the S-box S_i is used with $a_{i1}a_{i6}$ designating the row and $a_{i2}a_{i3}a_{i4}a_{i5}$ designating the column of S_i to give $S_i(B_i) = C_i$ a 4-tuple of bits. We then get the 32 bits sequence $C = C_1C_2, \dots, C_8$.

(4) A permutation is then applied to C.