Math 435, Spring Semester 2000-01
R.A. Brualdi
Mid-term Exam: March 7, 2001

NAME:

Total Points:

1. [20 points] Consider an alphabet of fifteen characters labeled as 0, 1, 2, . . . , 14. How many affine ciphers (including the identity cipher $x \rightarrow x$) are there for this alphabet?

In order for the affine cipher $E_{a,b}(x) = (ax + b) \mod 15$ to be one-to-one, $a$ has to be an invertible element modulo 15. The invertible elements among 0, 1, 2, . . . , 14 are those which are relatively prime to 15, and so are the eight elements 1, 2, 4, 7, 8, 11, 13, 14. Thus there are 8 choices for $a$ and 15 choices for $b$, and so 120 such affine ciphers.

2. [20 points] (a) A key $k = (k_1, k_2, \ldots, k_N)$ of length $N$ is selected by choosing $k_1, k_2, \ldots, k_N$ independently at random from an alphabet of size $n$. Assume that $N \leq n$. What is the probability that at least two of the characters of the key are identical?

It is 1— the probability that all the characters are different, and so

$$1 - \frac{n(n-1)(n-2)\cdots(n-(N+1))}{n^N}.$$ 

(The numerator is the number of sequences of length $N$ with no repeats, and the denominator is the total number with or without repeats.)

(b) If the key is used for a "periodic one-time pad," what do identical characters mean?

Identical characters in the key means two different places are subject to the same cyclic shift; i.e. two identical shift ciphers in each block. This does not necessarily mean less secure; consider e.g. if we are working with bits. Note that if all characters of the key are identical, then we have an ordinary shift cipher.

3. [10 points] The following message is the ciphertext of a plaintext encrypted using a keyed columnar transposition based on the keyword EMINEM:

```
ASOOARNMYSGKTANNAFRDIDPMSEIERE
```

Saint Basil (330-379)

Greek Theologian

Decrypt the message. SEE YOUR CLASS NOTES.
So: ANGER IS A KIND OF TEMPORARY MADNESS.

4. [10 points] How many permutations of \{1, 2, \ldots, 9\} have, in their cycle decomposition, one 3-cycle, one 4-cycle, and two 1-cycles (fixed points)? How many have two 3-cycles and three 1-cycles?

\[
\binom{9}{3} \cdot \frac{3!}{2!} \cdot \binom{9}{4} \cdot \frac{4!}{2!} \cdot \frac{5!}{2!}
\]

E.g. the 3! is the number of ways to arrange 4 things in a cycle.

\[
\binom{9}{3} \cdot \frac{3!}{2!} \cdot \binom{9}{4} \cdot \frac{4!}{2!} \cdot \frac{5!}{2!}
\]

One needs to divide by 2 since the same pair \(A, B\) of subsets of size 3 can be chosen both as \(A\) then \(B\), and \(B\) then \(A\). In the first case one does not need to divide, since the subsets have different cardinality.

5. [20 points] (a) Give a formula for encryption of a plaintext \(x = x_1x_2x_3 \ldots\) using a Vigenère cipher with key \(k = (k_1, k_2, \ldots, k_m)\).

\[
E_k(x_i) = (x_i + k_{\text{ch}i}) \mod 26
\]

(b) Describe a known plaintext attack on this cipher.

If I know that plaintext \(x_1x_2 \ldots x_m\) is encrypted as \(y_1y_2 \ldots y_n\), then \(k_i = (y_i - x_i) \mod 26\).

6. [20 points] Tell me all that you know DES: how it works, its weaknesses, its strengths, ...

See Susan Landau's article on DES (class handout) and the book.