September 1, 2004

Math 65S
Cryptography and Society
Assignment 2

Due: Monday, September 6, 2004.

Journal: Write a one-page (12 pt, single-spaced) explication of the second chapter of Singh's book. Summarize what you feel are the major points made about the nature and use of cryptography.

1. How many divisors does 945 have? List them all.

2. Find the greatest common divisor $(360, 294)$ in two ways, first by finding all the divisors of 360 and of 294, then using the definition of the greatest common divisor, and second by means of the Euclidean Algorithm.

3. Use the Euclidean Algorithm to find the greatest common divisor of each of the following pairs of integers:

(i) 15, 35
(ii) 0, 111
(iii) -12, 18
(iv) 99, 100
(v) 100, 102
(vi) -27, -45
(vii) 233, 144

4. Use the definition of greatest common divisor to prove that if p is prime and a is an integer, then either $(a, p) = 1$ or $(a, p) = p$.

5. The rule

$$\bar{c} = \bar{13}\bar{p} + \bar{1}$$

cannot be the encryption function for an affine cipher, where as usual, $A = \bar{0}$, $B = \bar{1}, \ldots, Z = \bar{25}$. Why not?

6. Find an integer d such that $11d \equiv 1 \pmod{26}$. (This is called a *multiplicative inverse* of 11 mod 26.) Use this to solve the congruence

$$y \equiv 11x + 3 \pmod{26}$$

for x. (Your answer should be of the form $x \equiv ay + b \pmod{26}$ for suitable integers a and b.)

7. Identify the letters $A, B, \ldots, Z$ of the alphabet as usual with the congruence classes (buckets) mod 26, $\bar{0}, \bar{1}, \ldots, \bar{25}$, respectively. Define

an affine cipher by taking the letter corresponding to $\bar{x}$ to the letter corresponding to $\bar{11}\bar{x} + \bar{3}$, *i.e.*, $E(\bar{x}) = \bar{11}\bar{x} + \bar{3}$.

(i) Encrypt the word ATTRITION using this affine cipher.
(ii) Use the answer to Problem 6 to find the decryption function for this affine cipher.
(iii) Decrypt KVZVMENBQ (which was again encrypted using the affine cipher with $E(\bar{x}) = \bar{11}\bar{x} + \bar{3}$.)

8. You examine the frequencies of letters in an affine-encrypted ciphertext and *guess* that the cipher letters Q and H correspond to the two most common letters of standard English plaintext, E and T, respectively. Find the decryption function and use it to decrypt

$$EKWIDQDYUJH$$

(*Suggestion:* Start by showing that your guess implies that the decryption function $\bar{p} = \bar{a}\bar{c} + \bar{b}$ satisfies the two equations in two unknowns $\bar{a}$ and $\bar{b}$

$$\bar{4} = \bar{16}\bar{a} + \bar{b}$$
$$\bar{19} = \bar{7}\bar{a} + \bar{b}$$

and then solve for $\bar{a}$ and $\bar{b}$.)