Problem Set 4

Due: April 16

1. Stinson, problem 6.13, p.247. Only decipher the first three ciphertext message units in Table 5.1: 12423, 11524, 7243

2. Stinson, problem 6.16, p.250. (When Stinson says, "encrypt each residue modulo 26 as a separate plaintext character", he just means that each letter A-Z is encrypted separately.)

3. Stinson, problem 6.17, p.250.

4. Recall our discussion of partial information on RSA. We defined the functions,

$$parity(x^e \bmod n) = \begin{cases} 0 & \text{if } x \bmod n \text{ is even} \\ 1 & \text{if } x \bmod n \text{ is odd} \end{cases}$$

$$half(x^e \bmod n) = \begin{cases} 0 & \text{if } x \bmod n < n/2 \\ 1 & \text{if } x \bmod n > n/2 \end{cases}$$

Here e and n are the usual RSA public key parameters, and x is an RSA plaintext message, which means that it's an integer less than n.

Prove the following:

$$\text{if } half(x^e \bmod n) = 1, \text{ then } parity((2x)^e \bmod n) = 1.$$

[**Hint:** Just as in our class discussion, this problem involves reasoning about intervals. It does not involve any heavy-duty mathematical analysis.]

5. Find all generators of Z_{13}^*.

For problems 6 and 7, you may use without proof any result in the first three sections of the number theory notes. As in the previous problem set, you should prove (using results in the first three sections of the notes) any result you use that does not appear in those sections.

6. Suppose that p is prime, $r > 0$, $a^r \equiv 1 \bmod p$, and $gcd(r, p-1) = d$. Prove that $a^d \equiv 1 \bmod p$.

7. Prove that if p is prime and $x^2 \equiv 1 \bmod p$, then

$$x \equiv 1 \bmod p \quad \text{or} \quad x \equiv -1 \bmod p.$$

For problem 8, you may use without proof any result in the first six sections of the number theory notes. As in the previous problem set, you should prove (using results in the first six sections of the notes) any result you use that does not appear in those sections.

8. Prove that if $x \equiv y \bmod \phi(m)$, then for any $a \in Z_m^*$, $a^x \equiv a^y \pmod m$.