Section 6

1. In the RSA encryption algorithm let $p = 3$, $q = 5$ and $e = 7$.

(a) What is the public key?

(b) What is the private key?

(c) Encrypt the message $x = 3$.

(d) Decrypt the message $y = 10$.

2. A certain course has one professor and three GSIs on its staff. The staff want to password-protect the software that lets them alter student midterm grades. To prevent malicious tinkering, they don't want to allow anyone to access the system alone. Instead, they would like it so that the system can be entered only with the consent of either (1) the professor and any one GSI, or (2) all three GSIs together. Suppose the password is some message m, and let p be a prime.

Consider the following scheme:
Generate two numbers s_1 and s_2 at random and choose s_3 such that $s_1 + s_2 + s_3 \equiv m \pmod{p}$. Let $t_1 = s_2 + s_3, t_2 = s_1 + s_3$, and $t_3 = s_1 + s_2$. Give s_1 to the first GSI, s_2 to the second GSI, and s_3 to the third GSI. Finally, give t_1, t_2 and t_3 to the professor. If the three GSIs want to compute the password, they can pool their information to compute $s_1 + s_2 + s_3 \equiv m \pmod{p}$. If a GSI and the professor want to comptue the password, they can compute $s_i + t_i \equiv m \pmod{p}$.

(a) Is this a valid solution? Why or why not?

(b) Modify the above scheme to make it more secure.

3. The Chinese Remainder Theorem states that if

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\cdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

and each pair of n_i and n_j is co-prime (i.e. $\gcd(n_i, n_j) = 1$), then x has a unique solution modulo $n_1 n_2 \cdots n_k$.

The proof of this fact is constructive and uses Euclid's Algorithm.

Consider the following system of equations:

$$\begin{aligned} x &\equiv 13 \pmod{27} \\ x &\equiv 7 \pmod{16} \end{aligned}$$

(a) Find the solution to the following, modulo $432 = 27 \cdot 16$:

$$\begin{aligned} x_1 &\equiv 1 \pmod{27} \\ x_1 &\equiv 0 \pmod{16} \end{aligned}$$

Using the solution above, determine a solution for the following, modulo 432:

$$\begin{aligned} x_2 &\equiv 13 \pmod{27} \\ x_2 &\equiv 0 \pmod{16} \end{aligned}$$

(b) Now find the solution to the following, modulo 432:

$$x_3 \equiv 0 \pmod{27}$$
$$x_3 \equiv 1 \pmod{16}$$

Using the solution above, determine a solution for the following, modulo 432:

$$x_4 \equiv 0 \pmod{27}$$
$$x_4 \equiv 7 \pmod{16}$$

(c) Now find a solution to the original system of equations, modulo 432.

(Hint: $16^{-1} \equiv 22 \pmod{27}$ and $27^{-1} \equiv 3 \pmod{16}$.)

4. Let $a \in \mathbb{N}$ be a natural number, and define the *sign* of a to be the quantity formed by alternatively adding and subtracting the digits of a. For example, if $a = 39250$ then the sign of a is $3 - 9 + 2 - 5 + 0 = -9$. Prove that a is divisible by 11 if and only if its sign is divisible by 11.

5. Consider the following game: Alice picks a degree d polynomial $p(x)$ in $GF(m)$ (where m is a large prime). Bob picks a different degree d polynomial $q(x)$ (i.e. $q(x) \neq p(x)$). Bob gets one point for each value $x \in \{0, \ldots, m-1\}$ where $p(x) \equiv q(x) \pmod{m}$. What is the highest score Bob can get?

(a) Prove your answer using the following fact: a non-zero polynomial of degree d in $GF(m)$ has at most d roots.

(b) Now, prove your answer again using the following fact: $d + 1$ points in $GF(m)$ uniquely specify a polynomial of degree d.

6. Consider the alphabet $A = 0$, $I = 1$, $N = 2$, $S = 3$, $T = 4$. Suppose a message of length 3 is sent using the error correction scheme discussed in class over $GF(5)$, with no more than one erasure. If you receive the following packets, what was the original message?

(a) N _ A A

(b) _ A N N

(c) N T _ N