Note: Please cite any resources used, and mention any classmates that you worked with on this assignment. If you worked alone, please also say so. We will start taking points off if this is missing.

Problem 1. RSA Digital Signatures

Alice and Bob are discussing their favorite numbers in person. Alice tells Bob she'll send him her favorite number, but include an RSA signature so that Bob will know for sure it came from Alice. Alice's private key $d = 7$, public key $e = 3$, and $N = 33$.

(a) Alice's favorite number is 5, so she'll send the pair (5, S) where S is her RSA Signature of 5. What is S?

(b) Show Bob's work to verify that the pair (5, S) came from Alice.

(c) Why does this process guarantee that nobody but Alice could have sent the message?

Problem 2. Homomorphisms

(a) Describe the homomorphic property in your own words using a few sentences.

(b) RSA's homomorphic property under multiplication is a problem. Explain in a few sentences how padding helps to avoid this problem.

Problem 3. Shamir Secret Sharing

An organization of 10 individuals is using Shamir Secret Sharing to protect their private data. The quorum they have decided to use is 4, and they're working (mod 17).

5 members of the team come together to reveal the secret, and reveal the following information:

$$f(1) = 0, f(5) = 5, f(6) = 5, f(8) = 10, f(10) = 6$$

(a) What is the minimum number of equations that we need to solve in order to recover the secret a_0?

(b) Write down a system of linear equations that, if solved simultaneously, would let us recover the secret a_0.

Note: there may be more than one possible answer for (b), and there is no need to actually solve the system of equations.

Problem 4. Modular arithmetic, and Chinese Remainder Theorem Notation

(a) Write out the Chinese Remainder Theorem Notation for all integers (mod 15)

(b) Do the following modular aritmetic calculations (mod 15). All answers should be in the range $[0, 14]$.

(1) $4 + 7$ (mod 15)
(2) $8 - (3 \times 4)$ (mod 15)
(3) 7^{-1} (mod 15)
(4) $\frac{3^2+6}{7}$ (mod 15)
(5) $3^2 - 4$ (mod 15)

(c) Do the following modular arithmetic calculations using Chinese Remainder Theorem Notation. Example: $1 + 1$ (mod 15) : $< 1\ mod\ 3, 1\ mod\ 5 > + < 1\ mod\ 3, 1\ mod\ 5 > = < 2\ mod\ 3, 2\ mod\ 5 >$.

(1) $4 + 7$ (mod 15)
(2) $8 - (3 \times 4)$ (mod 15)
(3) $3^2 + 6$ (mod 15)
(4) $3^2 - 4$ (mod 15)

Problem 5. Simultaneous Congruences using the Chinese Remainder Theorem
Solve each of the following simultaneous systems of congruences, or explain why no solution exists.

(a) $x \equiv 3$ (mod 7), and $x \equiv 4$ (mod 9)

(b) $x \equiv 137$ (mod 423), and $x \equiv 87$ (mod 191)

(c) $x \equiv 133$ (mod 451), and $x \equiv 237$ (mod 697)

(d) $x \equiv 5$ (mod 9), $x \equiv 6$ (mod 10), and $x \equiv 7$ (mod 11)

(e) $x \equiv 37$ (mod 43), $x \equiv 22$ (mod 49), and $x \equiv 18$ (mod 71)

Taken from Hoffstein 2.18