

Assignment #3

Due: Tuesday, November 2nd, 2004.

Problem 1 (15 pts) RSA Parameter Generation

- (6 pts) Suppose that $q - p = 2d > 0$ and $n = pq$. Prove that $n + d^2$ is a perfect square, i.e., there exists an integer x such that $x^2 = n + d^2$.
- (6 pts) Given an integer n which is the product of two odd primes, and a small positive integer d such that $n + d^2$ is a perfect square, show how this information can be used to factor n .
- (3 pts) Comment on the impact of the above results on choosing p and q in the RSA encryption scheme.

Problem 2 (15 pts) Exercise 5.16 on Page 222 (10 pts for (a) and 5 pts for (b))

Hint and Additional Requirements: When proving Part (a), first show that $c_2 = (c_1 b_1 - 1)/b_2$ is an integer. When working on Part (b), write out the values c_1 and c_2 and the intermediate steps for computing c_1 if you compute it manually. If you write a program to compute c_1 , include the source code. You will need to compute two more inverses in the following problem.

Problem 3 (20 pts) Exercise 5.13 on Page 221 (10 pts for (a) and 5 pts each for (b) and (c))**Corrections and Additional Requirements:**

- Line two, “ $d_K(y) = y^a \bmod n$ ” should be “ $d_K(y) = y^d \bmod n$ ”.
- When proving part (a), if you use a Theorem to prove any step, mention the name of the Theorem being used.
- In parts (b) and (c), use $d = 1234577$.

Hint: The basic ideas of the algorithm in this problem are as follows. Given an RSA ciphertext y , the decryption is to find x s.t. $1 \leq x \leq n - 1$ and $x = (y^d \bmod n)$. Let $x_p = (y^d \bmod p)$ and $x_q = (y^d \bmod q)$, then $x \equiv x_p \pmod{p}$ and $x \equiv x_q \pmod{q}$. We can use the Chinese Remainder Theorem to solve it. Furthermore, instead of computing $x_p = (y^d \bmod p)$, the problem computes $x_p = (y^{d_p} \bmod p)$ where $d_p = (d \bmod (p - 1))$.

Problem 4 (50 pts) Read the article “New Directions in Cryptography” by Diffie and Hellman, and answer the following problems.

- (8 pts) The paper gives rationales for building encryption schemes that are secure against known plaintext attacks and chosen plaintext attacks, by discussing how such schemes remove restrictions that are placed on the ways of using them. Discuss these rationales in your own words.
- (6 pts) List all the limitations and shortcomings discussed in the paper about symmetric encryption schemes.
- (6 pts) List all the limitations and shortcomings discussed in the paper about symmetric message authentication schemes.

- d (10)** The paper describes Lamport's one-time signature scheme. To sign a message that has N bits, the private signing key consists of $2N$ random numbers, and the public signature verification key consists of $2N$ numbers that are the results of applying a one-way function f to each number in the signing key.
- Can one use the same public key to sign another message? Why or why not? The paper also describes an improvement to the Lamport scheme. Describe this improvement.
- e (10 pts)** The paper establishes the relationships among (1) public-key encryption, (2) public key distribution, and (3) digital signature (referred to in the paper as one-way authentication). By relationships, we mean using one scheme to implement another scheme. List these relationships, and explain the constructions involved to use one scheme to implement another.
- f (10 pts)** The encryption function of a public-key encryption function \mathcal{E}_K should run in polynomial time in the size of its input. Explain why the decryption function corresponding to \mathcal{E}_K must be in **NP**. Explain why this means that public key encryption schemes cannot have perfect secrecy in the Shannon sense.