

Assignment #4

Due: Thursday, April 15, 2004.

Problem 1 (15 pts) RSA Parameter Generation

- a. (5 pts) Suppose that $q - p = 2d > 0$ and $n = pq$. Prove that $n + d^2$ is a perfect square.
- b. (5 pts) Given an integer n which is the product of two odd primes, and given a small positive integer d such that $n + d^2$ is a perfect square, show how this information can be used to factor n .
- c. (5 pts) Comment on the impact of the above results on choosing p and q in the RSA encryption scheme.

Problem 2 (10 pts) Rabin Signatures.

Rabin suggested a signature scheme very similar to RSA signatures. In its simplest form, the public key is a product of two large primes $N = pq$ and the private key is p and q . The signature S of a message $M \in \mathbb{Z}_N$ is a square root of M modulo N . For simplicity, assume that the message being signed are always quadratic residues modulo N . To verify the signature, simply check that $S^2 = M \pmod{N}$. Note that we did not include any hashing of M prior to signing. Show that a chosen message attack on the scheme can result in a total break. More precisely, if an attacker can get Alice to sign messages chosen by the attacker then the attacker can factor N .

Hint: recall that a quadratic residue modulo $N = pq$ has four square roots in \mathbb{Z}_N . First show that there are two square roots of M that enable the attacker to factor N . Then show how using a chosen message attack the attacker can get a hold of such a pair of square roots. Note that proper hashing prior to signing prevents this attack.

Problem 3 (25 pts) RSA

Let N be a 1024 bit RSA modulus, and d a secret decryption exponent. To protect the private key d one may wish to split it into three pieces and store each piece on a different server. An attacker who breaks into one or two of the servers should learn no information about d . Consider the following scheme: pick three random numbers d_1, d_2, d_3 in $[-N, N]$ so that $d_1 + d_2 + d_3 = d \pmod{\phi(N)}$. Store d_i on server i .

- a. (5 pts) Suppose Alice wants to encrypt a ciphertext C . Show that Alice can do the following: (1) she sends C to the three servers, (2) each server i performs a local computation (using d_i) and responds with M_i to Alice, and (3) given M_1, M_2, M_3 Alice can easily construct the message M . Explain how server i computes M_i and how Alice combines M_1, M_2, M_3 to obtain M . There is no need to reconstruct the key d and there is no interaction between the servers. You may assume all communication between Alice and the servers is private.
- b. (10 pts) To provide fault tolerance, show how the key d can be shared among the three servers so that any two of three can be used to decrypt a ciphertext C as in part (a). This way, if one of the servers is down Alice can still decrypt messages. You may store multiple d_i 's on each server. An attacker who breaks into one of the servers should learn no information about d .

- c. (10 pts) Explain how to provide t -out-of- n solutions. Namely, explain how the key can be shared among k servers so that any t of them can be used to decrypt C while an attacker on $t - 1$ servers reveals no information about d . You may assume that t and k are relatively small numbers.

Problem 4 (20 pts) Commitment Schemes.

A commitment scheme enables Alice to commit a value x to Bob. The scheme is *secure* if the commitment does not reveal to Bob any information about the committed value x . At a later time Alice may *open* the commitment and convince Bob that the committed value is x . The commitment is *binding* if Alice cannot convince Bob that the committed value is some $x' \neq x$. Here is an example commitment scheme:

Public values: (1) a 1024 bit prime p , and (2) an element g of \mathbb{Z}_p^* of prime order q , and (3) a random element h in the subgroup of \mathbb{Z}_p^* generated by g . Alice does not know the discrete log of h base g .

Commitment: To commit to an integer $x \in [1, q - 1]$ Alice does the following: (1) she picks a random $r \in [1, q - 1]$, (2) she computes $b = (g^x \cdot h^r \pmod p)$, and (3) she sends b to Bob as her commitment to x .

Open: To open the commitment Alice sends (x, r) to Bob. Bob verifies that $b = g^x \cdot h^r \pmod p$.

Show that this scheme is secure and binding.

- a. (10 pts) To prove security show that b does not reveal any information to Bob about x . In other words, show that given b , the committed value can be any value x' in $[1, q - 1]$.
Hint: show that for any x' there exists a unique $r' \in [1, q - 1]$ so that $b = g^{x'} h^{r'}$.
- b. (10 pts) To prove the binding property show that if Alice can open the commitment as (x', r') where $x \neq x'$ then Alice can compute the discrete log of h base g . In other words, show that if Alice can find an (x', r') such that $b = (g^{x'} h^{r'} \pmod p)$ then she can find the discrete log of h base g . Recall that Alice also knows the (x, r) used to create b .

Problem 5 (20 pts) El Gamal Signatures

In El Gamal signatures, a public key has the form (p, g, y) and the corresponding secret key is a such that $y = (g^a \pmod p)$. The signature of a message M is (r, s) , where $r = (g^k \pmod p)$ and $s = (k^{-1}(h(M) - ar) \pmod (p - 1))$. The signature is valid if $y^r r^s \equiv g^{h(M)} \pmod p$.

- a. (10 pts) Assume that Alice signs two messages using El Gamal, and for both messages she uses the same k . Show how an attacker can totally break the signature scheme (recover the signing key), without solving an instance of the Discrete Log Problem.
- b. (10 pts) Show that if the s part of a signature is 0, then one can recover the signing key.

Problem 6 (10 pts) Malleability of El Gamal Encryption

An encryption scheme is malleable if an attacker can modify a ciphertext of a message M in a way such that the modified ciphertext can be decrypted into a plaintext related to M . Give an example that shows that the El Gamal encryption scheme is Malleable.