

Assignment #5

Due: Tuesday, November 16th, 2004.

Problem 1 (10 pts) Alice uses the “double RSA” cipher. She makes public a modulus n , which is the product of two secret primes, and two public encryption exponents e_1 and e_2 . She tells people to encipher messages M in $0 < M < n$ to her by computing $C_1 = M^{e_1} \bmod n$ and then $C = C_1^{e_2} \bmod n$ and sending just C to her.

- Tell how Alice decipheres C , using her knowledge of the secret prime factors of n .
- Is there an easy way to factor n , given e_1 and e_2 .
- Is the “double RSA” cipher more secure, less secure or just as secure as the regular RSA cipher with the same modulus n but only one encryption exponent?
- Chunk got Alice’s instructions confused, and enciphered a message M for Alice using e_1 and e_2 in the reverse order. What would happen when Alice, unaware of Chunk’s error, try to decipher the ciphertext using her usual procedure? Did she get M or nonsense? If nonsense, could she recover M anyway?

Problem 2 (15 pts) Let $n = pq$ with p and q being distinct large primes.

- Prove that $-1 \in \text{QR}_n$ if and only if $p \equiv q \equiv 1 \pmod{4}$.
- Prove that $\left(\frac{-1}{n}\right) = -1$ if and only if $p \not\equiv q \pmod{4}$.

Problem 3 (10 pts) Consider the group \mathbb{Z}_p^* , let q be the order of $g \in \mathbb{Z}_p^*$. Is the following problem hard? Knowing p , q , and g , given g^c , find g^a and g^b such that $ab \equiv c \pmod{q}$, that is, to construct a Diffie-Hellman tuple (g, g^a, g^b, g^c) from (g, g^c) . If you think that the problem is not hard, give an efficient algorithm for solving it. If you think that the problem is hard, explain why.

Problem 4 (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.

Problem 5 (25 pts) Parties A_1, \dots, A_n and B wish to generate a secret conference key. All parties should know the conference key, but an eavesdropper should not be able to obtain any information about the key. They decide to use the following variant of Diffie-Hellman: there is a public prime p and a public element $g \in \mathbb{Z}_p^*$ of order q for some large prime q dividing $p - 1$. User B picks a secret random $y \in [1, q - 1]$ and computes $\gamma = (g^y \bmod p)$. Each party A_i picks a secret random $x_i \in [1, q - 1]$ and computes $\alpha_i = (g^{x_i} \bmod p)$. User A_i sends α_i to B . User B responds to party i by sending $\beta_i = (\alpha_i^y \bmod p)$.

- a. (5 pts) Show that party i given β_i (and x_i) can determine γ .
- b. (5 pts) Explain why (a hash of) γ can be securely used as the conference key. Namely, give a brief informal explanation why an eavesdropper cannot determine γ .
- c. (15 pts) Formally prove part b. Namely, show that if there exists an efficient algorithm \mathcal{A} that given the public values in the above protocol, outputs γ , then there also exists an efficient algorithm \mathcal{B} to break the Diffie Hellman protocol (using p and g as the public values). Note that \mathcal{B} takes $(g^a \bmod p)$ and $(g^b \bmod p)$ as input and should output $(g^{ab} \bmod p)$.

Problem 6 (30 pts) Let $N = pq$ be an RSA composite. Let $g \in [0, N^2]$ be an integer satisfying $g = (aN+1 \bmod N^2)$ for some $a \in \mathbb{Z}_N^*$. Consider the following encryption scheme. The public key is $\langle N, g \rangle$. The private key is $\langle p, q, a \rangle$. To encrypt a message $m \in \mathbb{Z}_N$ do: (1) pick a random $h \in \mathbb{Z}_{N^2}^*$, and (2) compute $C = g^m \cdot h^N \bmod N^2$. Our goal is to develop a decryption algorithm.

- a. (10 pts) Show that the discrete log problem $\bmod N^2$ base g is easy when knowing the private key. That is, show that given g and $B = g^x \bmod N^2$ there is an efficient algorithm to recover $x \bmod N$. Use the fact that $g = aN + 1$ for some integer $a \in \mathbb{Z}_N^*$.
- b. (10 pts) Show that given the public key and the private key, decrypting $C = g^m \cdot h^N \bmod N^2$ can be done efficiently.
Hint: consider $C^{\phi(N)} \bmod N^2$. Use the fact that by Euler's theorem $x^{\phi(N^2)} = 1 \bmod N^2$ for any $x \in \mathbb{Z}_{N^2}^*$.
- c. (10 pts) Show that this encryption scheme enables limited computation on ciphertexts. Let a, b, c be integers in $[1, N]$. Show that given N and c , and the encryption of a and b it is possible to construct the encryption of $a + b$ and the encryption of $c \cdot a$. More precisely, show that given N and an integer c , and ciphertexts $C_1 = E[a]$, $C_2 = E[b]$, it is possible to construct the ciphertexts $C_3 = E[a + b]$ and $C_4 = E[c \cdot a]$.