6.875J/18.425J Cryptography and Cryptanalysis September 5, 2001

Handout 1b: Problem Set 1

Instructor: Anna Lysyanskaya *Teaching Assistant: Moses Liskov*

This problem set will be due on Wednesday, September 12.

Problem 1

We define the Lily problem: given two integers n and S, determine whether S is relatively prime to $\varphi(n)$. Prove that if the Lily problem is hard, then RSA is hard to invert.

Problem 2

Assume one is using RSA with the same modulus n but different relatively prime public exponents e_1 and e_2 to encrypt a message m. Prove that the adversary can reconstruct m from the two encryptions (i.e. from $m^{e_1} \bmod n$ and $m^{e_2} \bmod n$).

Problem 3

Assume Alice, Bob and Carol have 3 randomly chosen moduli n_A, n_B and n_C, s.t. 3 is a common RSA exponent for all of them (i.e. $gcd(3, \varphi(n_X)) = 1$, $X = A, B, C$). A user U encrypts the same message m using their public keys. Show that an adversary can reconstruct m from the 3 encryptions (i.e. from $m^3 \bmod n_A$, $m^3 \bmod n_B$ and $m^3 \bmod n_C$).

Problem 4

Suppose $SQRT(a, p)$ is a polynomial-time algorithm that, if p is prime and a is a quadratic residue $a \in Z_p^*$, outputs (w.h.p.) some square root of a mod p.

(a) Prove that the following algorithm is a primality test (i.e. that on a prime input outputs PRIME with high probability, and on a composite input outputs COMPOSITE with probability at least 1/2.)

1. If $n = 2$, output PRIME.
2. If n is even or of the form $n = p^b$ for some $p, b > 1$, output COMPOSITE.
3. Choose a random $r \in \{1, \ldots, n-1\}$. If $gcd(r, n) > 1$, output COMPOSITE.
4. Compute $x \leftarrow SQRT(r^2 \bmod n, n)$.
5. If $x = \pm r \bmod n$, output PRIME. Otherwise, output COMPOSITE.

(b) Suppose $p = 4m + 3$ is a prime and that a is a quadratic residue modulo p. Prove that a^{m+1} is a square root of a modulo p.

(c) Use (a) and (b) to devise a primality testing algorithm for integers equivalent to 3 modulo 4.

Problem 5

Suppose p is a prime and g is a generator modulo p.

Experiment 1: Pick x at random in $\{1, \ldots, p-1\}$. Output g^x.

Experiment 2: Pick x, y at random in $\{1, \ldots, p-1\}$. Output g^{xy}.

Prove or disprove: Experiment 1 and Experiment 2 produce identically distributed outputs.