PMAT 329 Introduction to Cryptography ASSIGNMENT 3

Set: Monday, Nov. 22, 2004
Due: Monday, Dec. 6, 2004

Total: 60 points

1. Consider the RSA encryption scheme with public keys n = 55 and e = 7.
   (a) [4 points] Encipher the plaintext $M = 19$. Use the binary exponentiation algorithm and show your work.
   (b) [4 points] Break the cipher by finding p, q, and d.
   (c) [4 points] Decipher the ciphertext C = 35. Use the binary exponentiation algorithm and show your work.
2. [6 points] It is obvious that if one can factor an RSA modulus $n = pq$, i.e. one knows the prime factors p, q of n, then one can compute $\phi(n) = (p - 1)(q - 1)$. Prove the converse, i.e. if both n and $\phi(n)$ are known, then p and q can be found without factoring n.
3. This problem describes a "difference of squares" attack on RSA. Suppose two RSA primes p and q(q > p) are very close to one another, i.e. $q = p + \delta$ where $\delta \in \mathbb{N}$ is small (i.e. small enough that it is feasible to try all possible values 1, 2, 3, ... for δ; for example, we could have $\delta \approx \log p$). Note that in this case, $p + q$ is only slightly larger than $\sqrt{n}$. .
   (a) [5 points] Using the identity

   $$\left(\frac{q+p}{2}\right)^2 = n - \left(\frac{q-p}{2}\right)^2,$$

   describe an algorithm to recover $p + q$.
   (b) [3 points] Using the technique of part (a), describe a way to recover p and q efficiently without factoring n.
   (c) [2 points] Explain why $n = 23614161161$ is a particularly bad choice as an RSA modulus (apart from the fact that it's too small to guarantee a decent level of security).
4. After the discovery of RSA, several writers suggested using it with a small encryption exponent e (for example, $e = 2, 3$). Show why using such a small exponent is insecure in the following scenarios:
   (a) [8 points] Two people send the same message M to two different receivers. A different modulus is used for each transmission, but $e = 2$ for both.
   (b) [8 points] Two different messages which differ by only a few characters (the adversary can deduce the position of these characters) are sent under the same key. Here, $e = 2$ and n is the same for both messages.

   Hint: The adversary does not have to do any factoring in either case.

5. [10 points] Rabin's public-key encryption scheme enciphers a message M as

$$C \equiv M\left(M+b\right)\left(\bmod n\right), \qquad \left(0 \le C < n\right)$$

where b and n are public and $n = pq$ for secret primes p and q. Give a deciphering algorithm for the case where $p+1$ and $q+1$ are divisible by 4.

Hint 1: Compute d such that $2d \equiv b\left(\bmod n\right)$. Then

$$C + d^2 \equiv (M + d)^2 \pmod n.$$

Hint 2: If $x^2 \equiv a \pmod p$ and p is a prime such that $p \equiv 1 \pmod 4$, then

$$x \equiv \pm\, a^{(p+1)/4} \pmod p$$

are the two square roots of a mod p (prove this).

6. [6 points] Let $n = pq$ for distinct primes p and q. Given a, $0 < a < n$, let x and y, $0 < x, y < n$, be square roots of a modulo n, so

$$x^2 \equiv a \pmod n \quad \text{and} \quad y^2 \equiv a \pmod n.$$

Show that $\gcd(x+y,n) = p$ or q if $y \neq x$ and $y \neq n-x$, i.e., finding such x and y allows one to factor n.