密 碼 學 與 應 用 作 業 (三)

94/12/22 (四)

1. (Trappe 2nd Ed. 6.8.3 modified)
   The ciphertext 229 was obtained using RSA with n = 437 and e = 3. Suppose you know that the plaintext is either 68 or 69. Determine which it is without factoring n. (Note: you probably do not need to do any modulo exponentiation computations.)

2. (Trappe 2nd Ed. 6.8.11)
   Suppose that there are two users on a network. Let their RSA moduli be n_1 and n_2, with n_1 not equal to n_2. If you are told that n_1 and n_2 are not relatively prime, how would you break their systems?

3. (Trappe 2nd Ed. 6.8.13)
   Suppose you discover that
   $$880525^2 \equiv 2,\ 2057202^2 \equiv 3,\ 648581^2 \equiv 6, \text{ and } 668676^2 \equiv 77 \pmod{2288233}$$
   How would you use this information to factor 2288233? Explain what the steps you would do, but do not perform the numerical calculations.

4. (Trappe 2nd Ed. 6.8.15)
   Suppose n is a large odd number. You calculate $2^{(n-1)/2} \equiv k \pmod n$, where k is some integer with $k \not\equiv \pm 1 \pmod n$.
   (a) Suppose $k^2 \not\equiv 1 \pmod n$. Explain why this implies that n is not prime.
   (b) Suppose $k^2 \equiv 1 \pmod n$. Explain how you can use this information to factor n.

5. (Trappe 2nd Ed. 6.8.20)
   Suppose n = p q r is the product of three distinct primes. How would an RSA-type scheme work in this case? In particular, what relation would e and d satisfy?
   Note: There does not seem to be any advantage in using three primes instead of two. The running times of some factorization methods depend on the size of the smallest prime factor. Therefore, if three primes are used, the size of n must be increased in order to achieve the same level of security as obtained with two primes.
   In the case n = p q, we know that using CRT would cut the computation time of

decryption into 1/4. If the smallest prime factor of the three factor scheme has the same length of the two factor scheme, show that CRT can only cut the computation time of decryption into 3/8, which is worse than the two factor scheme.

6. (Trappe 2nd Ed. 6.8.22)
   (a) Show that if gcd(e, 24) = 1, then $e^2 \equiv 1 \pmod{24}$.
   (b) Show that if n = 35 is used as an RSA modulus, then the encryption exponent e always equals the decryption exponent d.