密 碼 學 與 應 用 補 救 作 業 (二)

94/12/15 (四)

(Trappe 2nd Ed. 6.8.5)

Let p be a large prime. Suppose you encrypt a message x by computing $y \equiv x^e \pmod{p}$ for some (suitably chosen) encryption exponent e. How do you find a decryption exponent d such that $y^d \equiv x \pmod{p}$? Is this system secure? (explain the reasons)

(Trappe 2nd Ed. 6.8.10)

The exponents e = 1 and e = 2 should not be used in RSA. Why?

The exponent e = 34 should also not be used in RSA. Why?