1082 作業四

繳交日期 109/04/17(五) 13:10

1. (a) Find all solutions to $x^2 \equiv 133 \pmod{221}$
   (b) Find all solutions to $x^2 \equiv 3074 \pmod{3937}$ note: 3937=31*127

2. (a) Solve $9x \equiv 1 \pmod{22}$
   (b) If we encode a message as an integer 1~22, and encrypt a message m as $c \equiv m^9 \pmod{23}$. How would you decrypt a cihpertext c? (please write down the encryption process of m=3 and the decryption process of its ciphertext)
   (c) Do you consider this a good cipher? (why? explain you considerations in symmetric and asymmetric encryption scenarios)

3. If n is the product of two unknown large prime numbers, then given a quadratic residue y in Z_n^*, it is difficult to find the square root of y (i.e. find x such that $y \equiv x^2 \pmod{n}$). Show that if we know the value $z \equiv x^e \pmod{n}$, where e is a known odd number and x the square root of y, then we can easily find out the value of x. (Hint: $\gcd(e, 2) = 1$ implies that there exist two integers a and b such that $a \cdot e + b \cdot 2 = 1$)