1082 作業六

繳交日期 109/05/15(五) 13:10

1. Let p and q be distinct odd primes, and let $n = p \cdot q$. For all integer x satisfies $\gcd(x, pq) = 1$,
   (a) show that $x^{\phi(n)/2} \equiv 1 \pmod{p}$ and $x^{\phi(n)/2} \equiv 1 \pmod{q}$.
   (b) Use (a) to show that $x^{\phi(n)/2} \equiv 1 \pmod{n}$
   (c) For an integer e satisfying $\gcd(e, \phi(n)/2) = 1$, use (b) to show that one can find d such that $ed \equiv 1 (\bmod\, \phi(n)/2)$ and that $x^{ed} \equiv x \pmod{n}$ (This suggests that we could work with $\phi(n)/2$ as the modulus of exponent instead of $\phi(n)$ in RSA.) How much the decryption time will save in this case?

2. Suppose you know that
   $3^{62} \equiv 28 \pmod{137}$, $3^{76} \equiv 15 \pmod{137}$, $3^{85} \equiv 10 \pmod{137}$, and $3^{117} \equiv 35 \pmod{137}$
   Please use the index calculus method to find the value x, $1 \le x \le 136$ such that $3^x \equiv 126 \pmod{137}$

3. Solve the discrete log problem: $3^x \equiv 2 \pmod{65537}$
   (a) Show that 3 is a generator in Z_{65537}^*
   (b) Using Pohlig-Hellman algorithm to solve x (Note: $x_0 = x_1 = ... = x_{10} = 0$. This example shows that if $p-1$ has a special structure, for example, a power of 2, then this can be used to avoid exhaustive searches. Therefore, such primes are cryptographically weak.)