Introduction to Cyrptography
(交大資工系 2010 Fall)

Assignment #2

(Due 11/8/2010(Monday) Noon at EC 119)

No late homework after 11/8/2010 2:00 pm

(用 A4 紙按順序作答，並寫出計算過程)

[1] (10%)

(a) Find integers x and y such that 17x+101y=1

(b) Find the inverse of 17 (mod 101)

[2] (8%)

What are the last three digits in the ordinary decimal representation of 747^{88002}?

[3] (8%)

The cheapest way to calculate a^{11} is $((a^2)^2a)^2a$ which takes 5 multiplications. What is the cheapest way to calculate a^{457}? (Express your solution as a form as $((a^2)^2a)^2a$ for a^{11})

[4] (12%)

The power of 3 (mod 29) are 3, 9, 27, 23, 11, 4, 12, 7, 21, 5, 15, 16, 19, 28, 26, 20, 2, 6, 18, 25, 17, 22, 8, 24, 14, 13, 10, 1, so 3 is a generator for Z_{29}^*

(a) Find all generators in Z_{29}^*? (Actually you don't need to calculate all g^x to test if g is a generator)

(b) In general, how many generators in Z_p^* for a prime p?

[5] (10%)

Solve the following modular equation: $10x \equiv 15 \pmod{75}$

[6] (12%)

Solve the following modular equations: (Watch out that any two of 10, 15, or 84 are not all relatively prime. But you still can use Chinese Remainder Theorem to solve it)

$X \equiv 3 \pmod{10}$

$X \equiv 8 \pmod{15}$

$X \equiv 5 \pmod{84}$

[7] (10%)

Evaluate the following Legendre symbols.

(a) $(\frac{1234}{10007})$

(b) $(\frac{1009}{53003})$

You may use the following properties of Jacobi symbols:

For odd m, n > 2,

$(\frac{-1}{n}) = (-1)^{\frac{n-1}{2}} = \begin{cases} 1, & n \equiv 1 (\mathrm{mod}\ 4) \\ -1, & n \equiv 3 (\mathrm{mod}\ 4) \end{cases}$

$(\frac{2}{n}) = (-1)^{\frac{n^2-1}{8}} = \begin{cases} 1, & n \equiv \pm 1 (\mathrm{mod}\ 8) \\ -1, & n \equiv \pm 3 (\mathrm{mod}\ 8) \end{cases}$

$(\frac{m}{n}) = (\frac{n}{m})(-1)^{(\frac{m-1}{2})(\frac{n-1}{2})}$

[8] (8%)

In RSA cryptosystem, if Alice receives the ciphertext C = 15 from Bob and her public key (e,n) = (7,55), what is Alice's private key d? And what is the plaintext M?

[9] (10%)

In the quadratic sieve factorization algorithm we are trying to factor n=7429 and if

$$83^2 \equiv -1 \times 2^2 \times 3^3 \times 5 \mod 7429$$

we have $87^2 \equiv 2^2 \times 5 \times 7 \mod 7429$

$$88^2 \equiv 3^2 \times 5 \times 7 \mod 7429$$

Continue to finish this factoring job. (Show your steps)

[10] (12%)

(a) Why is Z_4 = {0,1,2,3} not a field?

(b) Describe a finite field of 4 elements.

(Construct an addition table and a multiplication table for these 4 elements).