Introduction to Cyrptography
(交大資工系 2010 Fall)

Assignment #3

(Due 1/3/2011(Monday) Noon at EC 119)

<u>No late homework after 1/3/2011 2:00 pm</u>

(用 A4 紙按順序作答，並寫出計算過程)

(10 problems and 100 points in total)

[1] (a)One throws 3 balls randomly into 6 bins. What is the probability that some bin contains at least 2 balls? (Show your steps)(3 points)

(b)What is the birthday paradox?(3 points)

(c)What is a collision resistant hash function? (3 points)

(d)If the computer device is able to make lists of length 2^{80} in 2100 and store them in reason time, is SHA-1 still secure then? Why? (3 points)

[2] (a)In Diffie-Hellman key exchange, let $\alpha = 2$ be a generator in Z_{19}*. Suppose you are an eavesdropper and get $\alpha^a = 11$ from Alice and $\alpha^b = 13$ from Bob, find the shared secret key α^{ab}.(5 points)

(b) If you have two signed messages of RSA signature: (x_1, y_1) and (x_2, y_2), create an existential forgery by using these two. (5 points)

[3] In Shanks' algorithm (baby-step giant-step algorithm), suppose $p = 113$, and we wish to find $\log_3 53$. So we have $\alpha = 3$, $\beta = 53$ and $m = \lceil \sqrt{112} \rceil = 11$. Then α^{11} mod 113 = 76

Assume we have two lists L_1 and L_2, where L_1 is the list of ordered pairs (j, 76^j mod 113) for $0 \le j \le 10$:

(0, 1) (1, 76) (2, 13) (3, 84) (4, 56) (5, 75) (6, 50)
(7, 71) (8, 85) (9, 19) (10, 88)

and L_2 is the list of ordered pairs (i, 53×3^{-i} mod 113), $0 \le i \le 10$:

(0, 53) (1, 93) (2, 31) (3, 48) (4, 16) (5, 43)
(6, 52) (7, 55) (8, 56) (9, 94) (10, 69)

Use these two lists L_1 and L_2 to calculate $\log_3 53$. (8 points)

[4] Let p = 2027. The element $\alpha = 2$ is a generator of Z_{2027}*. Consider $\beta = 13$. Then $\log_2 13$ is computed as follows, using the index-calculus method.

1. The factor base is chosen to be the first 5 primes: S={2, 3, 5, 7, 11}
2. The following five relations involving elements of the factor base are obtained (unsuccessful attempts are not shown):

2^{1593} mod 2027 = 33 = 3×11

2^{983} mod 2027 = 385 = $5\times7\times11$

2^{1318} mod 2027 = 1408 = $2^7\times11$

2^{293} mod 2027 = 63 = $3^2\times7$

2^{1918} mod 2027 = 1600 = $2^6\times5^2$

(a) List the five equations involving the logarithms of elements in the factor base. (You should put a proper modulo in each equation.) (5 points)

(b) Solving the linear system of five equations (in (a)) in five unknowns yields the solutions $\log_2 2=1$, $\log_2 3=282$, $\log_2 5=1969$, $\log_2 7=1755$, and $\log_2 11=1311$. Suppose that integer k=1397 is selected and 13×2^{1397} mod 2027 = 110 = $2\times5\times11$. Calculate $\log_2 13$. (5 points)

[5] (a) Calculate $S_{ub}B_{ytes}$(FE) and $S_{ub}B_{ytes}$(7D) by using Algorithm B in AES.(5 points)

(b) Calculate $M_{ix}C_{olumn}$(1A2B3C4D) by using Algorithm D in AES.(5 points) (Show your steps)

[6] ElGamal signature scheme is stated as below:

Let p be a prime such that DL problem in Z_p is intractable, and let α be a generator in Z_p*. Define K={ (p,α,a,β) :$\beta=\alpha^a$ mod p }

p,α,$\boldsymbol{\beta}$ are the public key, a is the private key

For a (secret) random number k, define

sig (x,k)=(γ,δ), where

$\gamma=\alpha^k$ mod p and $\delta=(x-a\gamma)k^{-1}$ mod (p-1)

For a message ($\boldsymbol{\gamma}$,$\boldsymbol{\delta}$), define

ver (x, (γ,δ))=true iff $\beta^{\gamma}\gamma^{\delta}=\alpha^{x}$ mod p

(a) Prove if the signature was constructed correctly, the verification will succeed.(3 points)

(b) Prove that when k is known, an adversary can obtain Alice's signing key (3 points)

(c) Design an elliptic curve version of ElGamal signature scheme by replacing the original ElGamal multiplication group Z_p*= <α> by an addition group G = <P>, where P is a generator of an elliptic curve $y^2 = x^3 + ax + b$ defined over Z_p. (4 points)

[7] (a) In a (3,5) Shamir secret sharing scheme with modulus p=23, the following were given to Alice, Bob, and Charles: (2, 18), (3, 2), (5, 8). Calculate the corresponding Lagrange interpolating polynomial, and identify the secret. (6 points)

(b)A certain military office consists of one general, two colonels, and five desk clerks. They have control of a powerful missile but don't want the missile launched unless the general decides to launch it, or the 2 colonels decide to launch it, or <u>one colonel and 2 desk clerks</u> decide to launch it, or the 5 desk clerks decide to launch it. Describe how you would do this with a (5, 16) Shamir scheme. (6 points)

[8] (a) Describe the blind signature proposed by Chaum in 1983.(5 points)

(b) Describe the partially blind signature proposed by Abe and Fujisaki in 1996.(5 points)

[9] A non-adjacent form (NAF) is a <u>signed</u> binary representation ($c_{l-1}, \cdots, c_0$) of an integer c is said to be in non-adjacent form provided that no two consecutive c_i's are non-zero.

(a) Determine the NAF representation of the integer 247. (4 points)

(b) How to use NAF expressed in (a) to speed up the calculation of a^{247} if you know a^{-1}? (Show the steps) (4 points)

[10] Let E be the elliptic curve $y^2 = x^3 + 2x + 1$ defined over Z_{41}. P = (1, 39) is a pointof E. Calculate 2P, 3P. (Show your steps.) (10 points)