Introduction to Cyrptography
(交大資工系 2010 Fall)

Assignment #3

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

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

(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)

Sol:

(a) Event E: some bin contains at least 2 balls

Complement event $\overline{E}$ of E: no bin contains at least 2 balls

(each bin contains at most one ball)

$\Rightarrow P(E) = 1 - P(\overline{E}) = 1 - \frac{6\times5\times4}{6\times6\times6} = 1 - \frac{5}{9} = \frac{4}{9}$.

(b) Pr(at least two people have the same birthday among 23 people) > 0.5.

(c) A hash function **h** which satisfies that it is computationally infeasible to find messages m_1 and m_2 with $h(m_1) = h(m_2)$ is called a collision resistant hash function.

(d) According to birthday attack, for SHA-1, a 160-bit message digest, to find a collision with probability 1/2 will need just over 2^{80} random hashes, which can be done in 2100. So SHA-1 is unsecure.

[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)

Sol:

(a) Compute powers of generator a:

2, 4, 8, 16, 32≡13, 26≡7, 14, 28≡9, 18≡-1, -2≡17, -4≡15, -8≡11, …

$\therefore 2^5 \equiv 13 \bmod 19, 2^{12} \equiv 11 \Rightarrow a = 12, b = 5$

$\therefore 2^{ab} = 2^{12\times 5} = 2^{60} \equiv 2^6 \equiv 7 \bmod 19.$

(b) We can forge a valid signature (x', y') where $x' = x_1x_2$ and $y' = y_1y_2$.

[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 $\alpha^{11} \bmod 113 = 76$

Assume we have two lists L_1 and L_2, where L_1 is the list of ordered pairs $(j, 76^j \bmod 113)$ 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 $(i, 53\times 3^{-i} \bmod 113)$, $0 \le i \le 10$:

(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)

Sol:

In Shank's algorithm, after getting these two lists, we find elements have the same value in the second position in

$\Rightarrow$ Find (4, 56) in list L_1 and (8, 56) in list L_2, so we get

$$76^4 = 56 = 53 \times 3^{-8} \bmod 113$$

$$\therefore 53 = 76^4 \times 3^8 = 3^{11\times 4} \times 3^8 = 3^{52}$$

So we find $\log_3 53 = \log_3 3^{52} = 52$. (mod 112)

[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):

$2^{1593} \bmod 2027 = 33 = 3\times 11$

$2^{983} \bmod 2027 = 385 = 5\times 7\times 11$

$2^{1318} \bmod 2027 = 1408 = 2^7\times 11$

$2^{293} \bmod 2027 = 63 = 3^2 \times 7$

$2^{1918} \bmod 2027 = 1600 = 2^6 \times 5^2$

(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 $13 \times 2^{1397} \bmod 2027 = 110 = 2 \times 5 \times 11$. Calculate $\log_2 13$. (5 points)

Sol:

(a)
$$1593 = \log_2 3 + \log_2 11 \mod 2026,$$
$$983 = \log_2 5 + \log_2 7 + \log_2 11 \mod 2026,$$
$$1318 = \log_2 2^7 + \log_2 11 = 7 + \log_2 11 \mod 2026,$$
$$293 = \log_2 3^2 + \log_2 7 = 2\log_2 3 + \log_2 7 \mod 2026,$$
$$1918 = \log_2 2^6 + \log_2 5^2 = 6 + 2\log_2 5 \mod 2026.$$

(b)
$$\Rightarrow \log_2 13 + \log_2 2^{1397} = \log_2 2 + \log_2 5 + \log_2 11 = 1 + 1969 + 1311$$
$$\Rightarrow \log_2 13 = 3281 - 1397 = 1884 \mod 2026.$$

[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)

Sol:

(a)
$$(a_7a_6a_5a_4a_3a_2a_1a_0) = (11111110)$$
$$z \leftarrow \text{BinaryToField}(a_7a_6a_5a_4a_3a_2a_1a_0) = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x$$
$$z \leftarrow \text{FieldInv}(z) = x^6 + 1$$
$$(a_7a_6a_5a_4a_3a_2a_1a_0) \leftarrow \text{FieldToBinary}(z) = (01000001)$$
$$(c_7c_6c_5c_4c_3c_2c_1c_0) \leftarrow (01100011)$$
$$b_i \leftarrow (a_i + a_{i+4} + a_{i+5} + a_{i+6} + a_{i+7} + c_i) \bmod 2$$
$$(b_7b_6b_5b_4b_3b_2b_1b_0) = (10111011)$$

$S_{ub}B_{ytes}$(FE)=BB

$$z \leftarrow \text{BinaryToField}(a_7a_6a_5a_4a_3a_2a_1a_0) = x^6 + x^5 + x^4 + x^3 + x^2 + 1$$
$$z \leftarrow \text{FieldInv}(z) = x^7 + x^6 + x^5 + x^4 + x^3 + x$$
$$(a_7a_6a_5a_4a_3a_2a_1a_0) \leftarrow \text{FieldToBinary}(z) = (11111010)$$
$$(b_7b_6b_5b_4b_3b_2b_1b_0) = (11111111)$$

$S_{ub}B_{ytes}$(7D)=FF

(b) $t_0 = x^4 + x^3 + x$

$t_1 = x^5 + x^3 + x + 1$

$t_2 = x^5 + x^4 + x^3 + x^2$

$t_3 = x^6 + x^3 + x^2 + 1$

$u_0 = x^5 + x^4 + x^2 \oplus x^6 + x^5 + x^4 + x^3 + x^2 + 1 \oplus t_2 \oplus t_3 = x^5 + x^4 + x^3$

$u_1 = x^6 + x^4 + x^2 + x \oplus x^6 + x^2 \oplus t_3 \oplus t_0 = x^6 + x^2 + 1$

$u_2 = x^6 + x^5 + x^4 + x^3 \oplus x^7 + x^6 + x^4 + x^2 + x + 1 \oplus t_0 \oplus t_1$

$= x^7 + x^4 + x^3 + x^2 + x$

$u_3 = x^7 + x^4 + x^3 + x \oplus x^5 + x^3 + x^2 + x \oplus t_1 \oplus t_2 = x^7 + x^5 + x + 1$

$M_{ix}C_{olumn}$(1A2B3C4D)=38459EA3

[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={ $(p, \alpha, a, \beta) : \beta = \alpha^a \bmod p$ }

p, α, β are the public key, a is the private key

For a (secret) random number k, define

sig (x,k)=(γ, δ), where

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

For a message (γ, δ), define

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

(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 $Z_p^* = <\alpha>$ 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)

Sol:

(a) If the signature was constructed correctly, then

$$\beta^\gamma \gamma^\delta = (\alpha^a)^\gamma (\alpha^k)^{(x-a\gamma)k^{-1}} = \alpha^{a\gamma + kxk^{-1} - ka\gamma k^{-1}} = \alpha^{a\gamma + x - a\gamma} = \alpha^x.$$

∴ the verification will succeed.

(b) Observe δ:

$\delta = (x - a\gamma)k^{-1} \bmod p - 1 \quad \Rightarrow \quad \delta k = x - a\gamma \bmod p - 1,$

$\Rightarrow a\gamma = x - \delta k \bmod p - 1 \quad \Rightarrow \quad a = (x - \delta k)\gamma^{-1} \bmod p - 1,$

∴ If k is known, the adversary can obtain Alice's signing key by compute

$a = (x - \delta k)\gamma^{-1} \bmod p - 1.$

(c) Define $K = \{(p, q, E, P, m, Q) : q = \text{ord}(P), P \in E(F_p), Q = mP\}$,

p, q, P, Q are the public key, m is the private key.

For a (secret) random number k, define

$\text{sig}(x, k) = (r, s)$, where

$kP = (u, v), r = u \bmod q$ and

$s = k^{-1}(H(x) + mr) \bmod q$

For a message(r, s), define

$i = H(x) \times s^{-1} \bmod q$

$j = r \times s^{-1} \bmod q$

$(u, v) = iP + jQ$

and

$\text{ver}(x, (r, s)) = \text{true}$ iff $u \bmod q = r$.

[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 one colonel and 2 desk clerks 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)

Sol:

(a) $S(x)=19+6x+14x^2$

$$\ell_1(x) = \frac{x-3}{2-3} \cdot \frac{x-5}{2-5} = (x^2 - 8x + 15) \cdot 3^{-1} = 8x^2 + 5x + 5$$

$$\ell_2(x) = \frac{x-2}{3-2} \cdot \frac{x-5}{3-5} = (x^2 - 7x + 10) \cdot (-2)^{-1} = 11x^2 - 8x - 5$$

$$\ell_3(x) = \frac{x-2}{5-2} \cdot \frac{x-3}{5-3} = (x^2 - 5x + 6) \cdot 6^{-1} = 4x^2 + 3x + 1$$

$$p(x) = 18 \cdot (8x^2 + 5x + 5) + 2 \cdot (11x^2 - 8x - 5) + 8 \cdot (4x^2 + 3x + 1)$$
$$= 14x^2 + 6x + 19$$

secret M=p(0)=19

(b) (5,16) Shamir Scheme

General: 5 shares

Colonel: 3 shares

Clerk: 1 share

[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)

Sol:

(a)

- Voter wants $\langle M, H(M)^{d_{EA}} \rangle$.
- Voter knows the public key (e_{EA}, n_{EA}) of EA(Election Authority).
- The signing procedure
  - **Blinding:** Voter randomly chooses $r \in \mathbb{Z}^*_{n_{EA}}$, and sends EA $H(M) \cdot r^{e_{EA}}$.
  - **Singing:** EA signs $H(M) \cdot r^{e_{EA}}$, and returns $H(M)^{d_{EA}} \cdot r$.
  - **Unblinding:** Voter knows r, so he can calculate $H(M)^{d_{EA}}$.

(b)

- The signing procedure for message (M, c)
  - The user and the signer have a common information c.
  - The user randomly chooses $r \in \mathbb{Z}^*_n$, and send the signer $Z = H(M)r^{e\tau(c)}$.
  - The signer compute the private key $d_c = \frac{1}{e\tau(c)} \pmod{\phi(n)}$ corresponding to c. Then, send the user $\Phi = Z^{d_c} \pmod{n} = H(M)^{d_c} \cdot r$.
  - The user can get the signature $\delta = \frac{\Phi}{r} = H(M)^{d_c}$.
  - The signed message is $\langle (M, c), \delta \rangle$
- The verification procedure
  - The verifier check if $\delta^{e\tau(c)} = H(M)$.

[9] A non-adjacent form (NAF) is a signed binary representation (c_{l-1}, ⋯, 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)

Sol:

(a) $247 = (11110111)_2 = (1,0,0,0,0,-1,0,0,-1)_2$ in NAF form.

(b) Use the same concept of double-and-(add or subtract) algorithm, we can modify the square-and-multiply algorithm as following:

Square-and-(multiply/divide) algorithm $\left(a,(c_{l-1},\dots,c_0)\right)$, where $c_i \in \{0,1,-1\}$

$B \leftarrow a$

For $i \leftarrow l-1$ to 0

$$\text{do}\begin{cases} b \leftarrow b^2 \\ \text{if } c_i = 1,\ b \leftarrow b \cdot a \\ \text{else if } c_i = -1,\ b \leftarrow b \cdot a^{-1} \end{cases}$$

return b

Applying the above algorithm to compute a^{247}, we get

$$a^{247} = a^{(10000(-1)00(-1))_2} = (((((((a^2)^2)^2)^2)^2 \cdot a^{-1})^2)^2)^2 \cdot a^{-1}$$

$\Rightarrow$ 8 squarings and 2 multiplications.

Compare with square-and-multiply algorithm:

$$a^{247} = a^{(11110111)_2} = ((((((a^2 \cdot a)^2 \cdot a)^2 \cdot a)^2)^2 \cdot a)^2 \cdot a)^2 \cdot a$$

$\Rightarrow$ 7 squarings and 6 multiplications.

[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)

Sol:

Let $P = (x_1, y_1) = (1, 39)$,

1. 2P:

Let $2P = (x_2, y_2)$, then

$$\lambda = \frac{3x_1^2 + a}{2y_1} = \frac{3 \cdot 1^2 + 2}{2 \cdot 39} = \frac{5}{78} = \frac{5}{-4} = 5 \cdot (-4)^{-1} = 5 \cdot 10 = 50$$

$$= 9 \bmod 41$$

$$x_2 = \lambda^2 - 2x_1 = 9^2 - 2 \cdot 1 = 81 - 2 = 79 = 38 \bmod 41$$

$$y_2 = (x_1 - x_2)\lambda - y_1 = (1 - 38) \cdot 9 - 39 = \big(1 - (-3)\big) \cdot 9 - (-2)$$

$$= 36 + 2 = 38 \bmod 41$$

$\therefore 2P = (38, 38)$.

2. 3P:

Let $3P = (x_3, y_3)$, then

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{38 - 39}{38 - 1} = \frac{-1}{37} = \frac{-1}{-4} = 4^{-1} = -10 = 31 \bmod 41$$

$$x_3 = \lambda^2 - x_1 - x_2 = 31^2 - 1 - 38 = 18 - 39 = 18 + 2 = 20 \bmod 41$$

$$y_3 = (x_1 - x_3)\lambda - y_1 = (1 - 20) \cdot 31 - 39 = (-19) \cdot (-10) - (-2)$$

$$= 26 + 2 = 28 \bmod 41$$

$\therefore 3P = (20, 28)$.