Introduction to Cryptography

(交大資工系 2014 Fall)

Midterm (A 卷)

(請按順序作答，並列出演算過程)

Time: 10:10-12:00   11/12/2014

Place: ED 027

(9 problems and 110 points in total)

[1] (a) List the powers of 16 (mod 19) to show ~~16~~ 15 is a generator of Z_{19}^*. (5 points)

(b) Find all generators in Z_{19}^*. (Don't use brute force method.) (5 points)

(c) How many generators for Z_{101}^*? (5 points)

(d) In Diffie-Hellman key exchange, let α = ~~16~~ 15 be a generator in Z_{19}^*. Suppose You are an eavesdropper and get $\alpha^a = 10$ from Alice and $\alpha^b = 4$ from Bob, then what the shared secret key α^{ab} is. (5 points)

[2] Solve the following modular equations: (10 points)

$$\begin{cases} 9X \equiv 12 \pmod{51} \\ 4X \equiv 6 \pmod{10} \end{cases}$$

[3] (a) $GF(2^4)$ is the finite field with 2^4 elements, which can be expressed as $\{a_0+a_1x+a_2x^2+a_3x^3 \mid a_i=0,1\}$ with an irreducible polynomial $1+x+x^4$. Prove that x is a generator of $GF^*(2^4)$ by calculating x^i for i=1, …, 15. (7 points)

(b) Prove that $(X-1)(X-2)\ldots(X-(p-1)) = X^{p-1}-1 \bmod p$. (8 points)

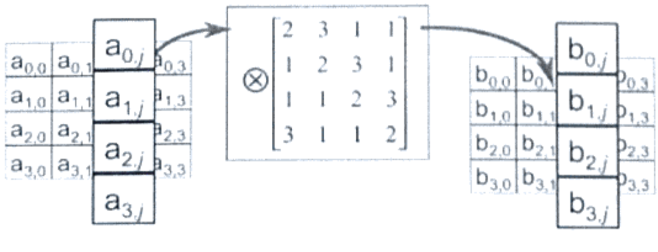
[4] The operation MixColumns(State) in AES is described below.

If the first column of the State A is

$[a_{00}, a_{10}, a_{20}, a_{30}]$ = [00101001, 01100011, 00000111, 00101100],

calculate the first column $[b_{00}, b_{10}, b_{20}, b_{30}]$ of B = MixColumns(A).

(10 points)



[5] In DES, the round function g: $g(L^{i-1}, R^{i-1}, K^i)=(L^i, R^i)$, where

$$L^i = R^{i-1}$$
$$R^i = L^{i-1} \oplus f(R^{i-1}, K^i).$$

Express L^{i-1}, R^{i-1} with L^i, R^i, f, and K^i and thus show the algorithm is invertible. (10 points)

[6] Factoring Algorithms

(a) Let n (= pq) = 351467. We have $2^{10!} \equiv 56160 \pmod{351467}$.
Use Pollard's p-1 algorithm to factor n. (7 points)

(b) Let n (= pq) = 3837523. We also have the following relations

$$9398^2 \equiv 5^5 \times 19 \pmod{3837523}$$
$$19095^2 \equiv 2^5 \times 5 \times 11 \times 13 \times 19 \pmod{3837523}$$
$$1964^2 \equiv 3^2 \times 13^3 \pmod{3837523}$$
$$17078^2 \equiv 2^6 \times 3^2 \times 11 \pmod{3837523}$$

By multiplying these together, we obtain the congruence

$$2230387^2 \equiv 2586705^2 \pmod{3837523}$$

Factor n. (7 points)

[7] Alice uses the RSA cryptosystem with primes $p = 13$ and $q = 23$ and public exponent $e = 5$.

(a) What is Alice's public modulus n? What is her private key d?

(b) Bob would like to encrypt $M = 100$ to Alice. What is the ciphertext?
(12 points)

[8] In Baby-step Giant-step algorithm, suppose $p = 29$, and we wish to find $\log_3 2$. So we have $\alpha = 3$, $\beta = 2$, and $m = \lceil \sqrt{28} \rceil = 6$. Then, $\alpha^{-6} \equiv 22 \pmod{p}$. Assume we have two lists L_1 and L_2. L_1 is the list of ordered pairs $(j, 3^j \bmod p)$ for $0 \leq j \leq 5$:

(0, 1) (1, 3) (2, 9) (3, 27) (4, 23) (5, 11)

and L_2 is the list of ordered pairs $(i, 2 \times 3^{-6i} \bmod p)$ for $0 \leq i \leq 5$:

(0, 2) (1, 15) (2, 11) (3, 10) (4, 17) (5, 26)

Use these two lists L_1 and L_2 to calculate $\log_3 2$. (8 points)

[9] Alice and Bob are communicating using the ElGamal cryptosystem with prime $q = 23$ and generator $\alpha = 7$.

(a) Bob creates his public key by choosing the exponent $X_B = 5$. What is Bob's public key Y_B? (3 points)

(b) Alice wants to send M=3 to Bob. Demonstrate how Alice encrypts M if the random number k she chooses is k=2. (4 points)

(c) If Bob receives the encrypted message $(C_1, C_2) = (9, 6)$, what is the plaintext M? (4 points)