Lecture NS4 2018

Chapter 9

1. Describe components of the public-key cryptosystem.

A: Fig. 9.1 a, pp.286—288

- Plaintext: This is the readable message or data that is fed into the algorithm as input.
- Encryption algorithm: The encryption algorithm performs various transformations on the plaintext.
- Public and private keys: This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the algorithm depend on the public or private key that is provided as input.
- Ciphertext: This is the encrypted message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts.
- Decryption algorithm: This algorithm accepts the ciphertext and the matchingkey and produces the original plaintext.

2. List and explain the requirements for a public-key cryptosystem.

A: pp.292-293

1) It is computationally easy for a party B to generate a key pair (public key *PU*, private key *PR*).

2) It is computationally easy for a sender A, knowing the public key and the message to be encrypted, *M*, to generate the corresponding ciphertext:

$$C = E(PU, M)$$

3) It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message:

$$M = D(PR, C) = D[PR, E(PU, M)]$$

4) It is computationally infeasible for an adversary, knowing the public key, *PU*, to determine the private key, *PR*.

5) It is computationally infeasible for an adversary, knowing the public key, PU, and a ciphertext, C, to recover the original message, M.

3. What are three broad categories of applications of public-key cryptosystems?

A: p. 292

- **Encryption/decryption:** The sender encrypts a message with the recipient's public key, and the recipient decrypts the message with the recipient's private key.
- **Digital signature:** The sender "signs" a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message.
- **Key exchange:** Two sides cooperate to exchange a session key, which is a secret key for symmetric encryption generated for use for a particular transaction (or session) and valid for a short period of time. Several different approaches are possible, involving the private key(s) of one or both parties.

4. Compare symmetric cipher with asymmetric cipher.

A:

Similar:

a. Used to encrypt and decrypt;
b. Implemented by both hardware and software;
c. Security depends on the length of the keys.

Different:

a. Public-key cipher is based on some open math problems, while conventional cipher is based on substitution and permutation.
b. The key length of public-key is adjustable, while the key length of conventional cipher is fixed by design.
c. Public-key can serve as digital signature while conventional cipher basically cannot.
d. Public-key cipher is much slower than conventional cipher (about 1000 times).
e. Public-key cipher has two different keys: public key and private key, while conventional cipher has only one key.

RSA algorithm sec. 9.2

1. Summarize the RSA algorithm

A:

Key Generation by Alice	
Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calcuate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption by Bob with Alice's Public Key	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption by Alice with Alice's Public Key	
Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

2. Using the RSA algorithm:

a) For p = 3; q = 17; e = 5; M = 5; determine the **digital signature**.

b) For p = 11; q = 7; e = 11; M = 7; determine the **ciphertext.**

Answer:

- **Note: a*b mod n = ((a mod n) *(b mod n)) mod n**

a) n = p*q = 3*17 = 51 ; φ(n) = (p−1)*(q−1) = 2*16 = 32 ;

Find d such that e*d = 1 mod φ(n) ; d = 13 since 5*13 = 65 = 2*32 +1

Digital signature:

$C = M^d \bmod n = 5^{13} \bmod 51 = (5^3)^4 * 5 \bmod 51$ C

$= (125 \bmod 51)^4 * 5 \bmod 51 = 23^4 \bmod 51 * 5 \bmod 51 = 23*5 \bmod 51 * 23^3 \bmod 51$

$= 13*23 \bmod 51 * 23^2 \bmod 51 = 44*23*23 \bmod 51$

$= 2*23 \bmod 51 * 2*23 \bmod 51 * 11 \bmod 51 = 5*5*11 \bmod 51$

$= 4*5 \bmod 51 = 20;$

b) p = 11; q = 7; e = 11; M = 7;

n = p*q =11*7 = 77; φ (n) = 10*6 = 60;

e*d =1 mod φ (n); d = 11 ; (11*11 = 121 = 2*60+1)

Ciphertext

$C = M^e \bmod n = 7^{11} \bmod 77 = (7^3)^3 * 7^2 \bmod 77 = 343^3 * 7^2 \bmod 77$

$= 35^3 * 7^2 \bmod 77 = 7^3 5^3 7^2 \bmod 77 = 35 * 5^3 7^2 \bmod 77 = 5^4 * 7^3 \bmod 77$

$= 5^5 * 7 \bmod 77 = 45 * 7 \bmod 77 = 315 \bmod 77 = 7;$

2. Explain why with a very small public key, such as e = 3, RSA becomes vulnerable to a simple attack? (Textbook p.300)

Answer (from the textbook)

However, with a very small public key, such as $e = 3$, RSA becomes vulnerable to a simple attack. Suppose we have three different RSA users who all use the value $e = 3$ but have unique values of n, namely (n_1, n_2, n_3). If user A sends the same encrypted message M to all three users, then the three ciphertexts are $C_1 = M^3 \bmod n_1$, $C_2 = M^3 \bmod n_2$, and $C_3 = M^3 \bmod n_3$. It is likely that n_1, n_2, and n_3 are pairwise relatively prime. Therefore, one can use the Chinese remainder theorem (CRT) to compute $M^3 \bmod (n_1 n_2 n_3)$. By the rules of the RSA algorithm, M is less than each of the n_i; therefore $M^3 < n_1 n_2 n_3$. Accordingly, the attacker need only compute the cube root of M^3. This attack can be countered by adding a unique pseudorandom bit string as padding to each instance of M to be encrypted. This ap-

Chapter 10. Other Public-key Cryptosystems

Dong Han, 29184479

Question 1. Briefly explain Diffie–Hellman key exchange.

1_A: Two parties each create a public-key, private-key pair and communicate the public key to the other party. The keys are designed in such a way that both sides can calculate the same unique secret key based on each side's private key and the other side's public key.

Question 2. Alice and Bob use the Diffie–Hellman key exchange technique with a common prime q =157 and a primitive root α = 5.

a. If Alice has a private key XA = 15, find her public key YA.

b. If Bob has a private key XB = 27, find his public key YB.

c. What is the shared secret key between Alice and Bob?

2_A:

a. X_A=15, $Y_A=\alpha^{XA} \bmod q = 5^{15} \bmod 157 = 79$

b. X_B=27, $Y_B=\alpha^{XB} \bmod q = 5^{27} \bmod 157 = 65$

c. $K = (Y_B)^{X_A} \bmod q = (Y_A)^{X_B} \bmod q = 78$

Question 3. Suppose Alice and Bob use an Elgamal scheme with a common prime q =157 and a primitive root α = 5. If Bob has public key Y_B =10 and Alice chose the random integer k =3, what is the ciphertext of M = 9?

3_A:

$K = (Y_B)^k \bmod q = 10^3 \bmod 157 = 58$

$C_1 = \alpha^k \bmod q = 5^3 \bmod 157 = 125$

$C_2 = KM \bmod q = 58 * 9 \bmod 157 = 51$

So, the ciphertext of M is (125, 51).

Tutorial —— Elliptic Curve Cryptography

Wang Shuai

1

On the elliptic curve over the real numbers $y^2 = x^3 - 36x + 1$, Let P = (-3.5, 9.5) and Q = (-2.5, 8.5). Find P + Q and 2P.

A:

For two distinct points,

P = (x_P , y_P) and Q = (x_Q, y_Q), that are not negatives of each other, the slope of the line l that joins them is $\Delta = (y_Q - y_P) / (x_Q - x_P)$. There is exactly one other point where l intersects the elliptic curve, and that is the negative of the sum of P and Q. After some algebraic manipulation, we can express the sum R = P + Q as

$$x_R = \Delta^2 - x_P - x_Q$$
$$y_R = -y_P + \Delta(x_P - x_R)$$

We also need to be able to add a point to itself: P + P = 2P = R. When $y_P \neq 0$, the expressions are

$$x_R = \left(\frac{3x_P^2 + a}{2y_P}\right)^2 - 2x_P$$
$$y_R = \left(\frac{3x_P^2 + a}{2y_P}\right)(x_P - x_R) - y_P$$

i. First we calculate R = P + Q, using the above equations.

Δ = (8.5 – 9.5)/(–2.5 + 3.5) = – 1

x R = 1 + 3.5 + 2.5 = 7

y R = –8.5 – (–3.5 – 7) = 2

R = (7, 2)

ii. For R = 2P, with a = -36

x_r = [(36.75-36) / 19]^2 + 7 = 7

y_R = [(36.75 - 36) / 19](-3.5-7) – 9.5 = 9.9

2

For E_{11} (1, 7), consider the point G = (2, 7). Compute the multiple of 2G

A:

The operation rule of elliptic curve under modulo p is:

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q \\ \dfrac{3x_1^{\,2} + a}{2y_1} & \text{if } P = Q \end{cases}$$

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

To compute 2G = (2, 7) + (2, 7), we first compute

λ = (3 × 2 2 + 1)/(2 × 7) mod 11 = 13/14 mod 11 = 2/3 mod 11 = 8

Then we have

x_3 = 8^2 – 2 – 2 mod 11 = 5

y_3 = 8(2 – 5) – 7 mod 11 = 2

2G = (5, 2)

3

The cryptosystem parameters are E_{11} (1, 7) and G = (2, 7). B's private key is n_B= 7.

a. Find B's public key P_B.

b. A wishes to encrypt the message P_m = (10, 9) and chooses the random value k = 3. Determine the ciphertext C_m .

c. Show the calculation by which B recovers P_m from C_m .

A:

Calculated according to the process of elliptic curve encryption:

① User A selects an elliptic curve Ep(a, b) and takes a point on the elliptic curve as the base point G.

② User A selects a private key k and generates a public key K=kG .

③ User A passes Ep(a, b) and points K, G to User B.

④ After receiving the information, User B encodes the plaintext to be transmitted to a point M on Ep(a, b) (the encoding method is many, not discussed here), and generates a random integer r(r<n).

⑤ User B calculates point C1=M+rK; C2=rG .

⑥ User B passes C1 and C2 to User A.

⑦ After user A receives the information, it calculates C1 − kC2 and the result is point M. $C1 - kC2 = M + rK - k(rG) = M + rK - r(rG) = M$

⑧ The plaintext can be obtained by decoding the point M.

a. P_B = n_B× G = 7 × (2, 7) = (7, 2).

b. C_m = {kG, P_m + kP_B } = {3(2, 7), (10, 9) + 3(7, 2)} = {(8,3), (10, 9) + (3, 5)} ={(8, 3), (10, 2)}

c. P_m = (10, 2) – 7(8, 3) = (10, 2) – (3, 5) = (10, 2) + (3, 6) = (10, 9)