Cryptography and Information Security

21510144 최민영

Contents

More Number Theory

Prime Numbers and Relatively prime number

Prime numbers

An integer p > 1 is a prime number , if and only if its only divisors are ± 1 and $\pm p$

Any integer $a > 1$ can be factored in a unique way as

$$a = {p_1}^{a_1} \times {p_2}^{a_2} \times {p_3}^{a_3} \times \cdots \times {p_t}^{a_t}$$

Where $p_t > p_{t-1} > \cdots > p_1$ are prime numbers , a_i is a positive integer.

Ex) Prime numbers

2 , 3 , 4 , 5 , 7 , 11 , 13 , 17 , 19 , 23 , 29 , 31 , 37 , 41 , 43 , 47 , 53 , 59 , 61 ,

67 , 71 , 73 , 79 , 83 , 89

$91 = 7^1 \times 13^1$

More Number Theory

Prime Numbers and Relatively prime number

Prime numbers

Ex) The integer 12 is represented by $\{a_2 = 2\,, a_3 = 1\}$ => $2^2 \times 3^1$

The integer 18 is represented by $\{a_2 = 1\,, a_3 = 2\}$ => $2^1 \times 3^2$

Multiplication of two numbers is equivalent to adding the exponents.

Ex)$12 \times 18 = (2^2 \times 3^1) \times (2^1 \times 3^2) = 2^{(2+1)} \times 3^{(1+2)} = (2^3 \times 3^3) = 216$

More Number Theory

Prime Numbers and Relatively prime number

Relatively prime number

When two numbers have no common factors other than 1.

Ex) 21 and 22 are relatively prime

- The factors of 21 are 1, 3, 7 and 21
- The factors of 22 are 1, 2, 11 and 22
  (The only common factor is 1)

Ex) But 21 and 24 are NOT relatively prime

- The factors of 21 are 1, 3, 7 and 21
- The factors of 24 are 1, 2, 3, 4, 6, 8, 12 and 24
  (the common factors are 1 AND 3)

GCD(21,24) = 3

GCD mean the greatest common divisor

More Number Theory

Modular Arithmetic

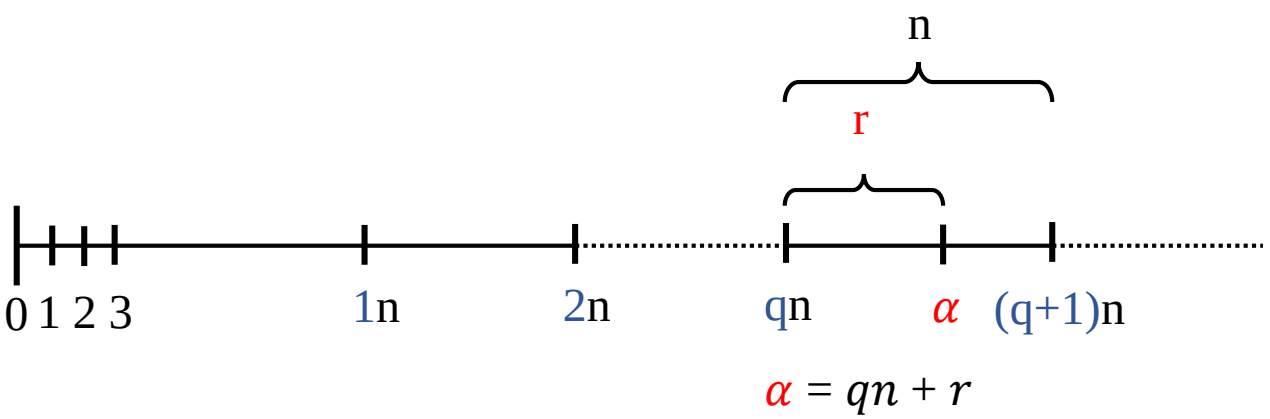
α = integer , n = positive integer

α mod n to be the remainder when α is divided by n.

$\alpha = qn + r$,$(0 <= r < n)$

q is Quotient

r is Remainder



More Number Theory

Modular Arithmetic

Two integers a , b are said to be congruent (modulo n,)

if **(a mod n) = (b mod n)**. This is written as **a ≡ b (mod n)**

Ex) 73 mod 23 { 73 = 23×3 + 4 } = 4

4 mod 23 { 4 = 23×0 + 4 } = 4

73 ≡ 4 (mod 23)

More Number Theory

Fermat's theorem

p prime number , α = positive integer not divisible by p

$$\alpha^{p-1} \equiv 1 \pmod{p}$$

Q) $7^{18} \equiv ? \pmod{19}$ [ex)$\alpha = 7$, $p = 19$]

A) 1 (By the fermat's theorem)

$7^2 = 49 \equiv 11 \pmod{19}$

$7^4 = 121 \equiv 7 \pmod{19}$

$7^8 = 49 \equiv 11 \pmod{19}$

$7^{16} = 121 \equiv 7 \pmod{19}$

$\therefore \alpha^{p-1} = 7^{18} = 7^{16} * 7^2 = 7 * 11 \equiv 1 \pmod{19}$

More Number Theory

Fermat's theorem

An alternative form of Fermat's theorem

p= prime number , α = a positive integer,

$$\alpha^p \equiv \alpha (\text{mod } p)$$

Ex) p =5 , α=3 $3^5 = 243 \equiv 3(\text{mod } 5)$

p =5 , α=10 $10^5 = 100000 \equiv 10(\text{mod } 5)$

Euler's Totient Function

In number theory , Euler's totient function is indicated by $\varphi(n)$

$\varphi(n)$ = the number of positive integers less than n and relatively prime to n.

n	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6

Characteristics of Euler Function

$\varphi(1) = 1$

A prime number = n	Two prime number p and q , n = p×q
$\varphi(n) = n - 1$	$\varphi(n) = \varphi(p \times q) = \varphi(p) \times \varphi(q) = (p - 1) \times (q - 1)$

n	$\phi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4

n	$\phi(n)$
11	10
12	4
13	12
14	6
15	8
16	8
17	16
18	6
19	18
20	8

n	$\phi(n)$
21	12
22	10
23	22
24	8
25	20
26	12
27	18
28	12
29	28
30	8

$$\phi(21) = \phi(3) \times \phi(7) = (3 - 1) \times (7 - 1) = 2 \times 6 = 12$$
where the 12 integers are $\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$.

More Number Theory

Euler's theorem

Every a , n that are relatively prime

$a^{\varphi(n)} \equiv 1 \pmod{n}$

Ex) a =3 ; n = 10 ; $\varphi(10) = 4$; $3^4 = 81 \equiv 1 \pmod{10}$

a =2 ; n = 11 ; $\varphi(11) = 10$; $3^{10} = 1024 \equiv 1 \pmod{11}$

An alternative form of the Euler's theorem

$a^{\varphi(n)+1} \equiv a \pmod{n}$

More Number Theory

Discrete Logarithm Problem : DLP

Consider the equation

$\mathbf{y} = g^{x} \bmod p$

Given g, x, and p, it is a **straightforward matter to calculate y**

$y = g^{\mathbf{x}} \bmod p$

However, given y, g, and p, **very difficult to calculate x**

The difficulty seems to be on the same order of magnitude as that of factoring primes required for RSA.

Symmetric cryptosystems

Symmetric encryption's two of the most difficult problems

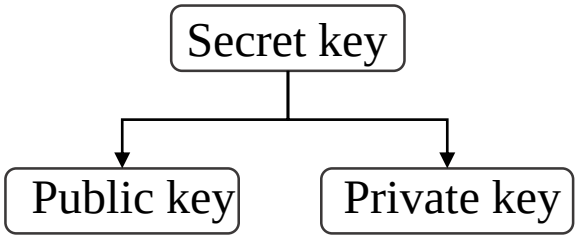
First problem = key distribution

1. Two communicants already share a symmetric key
2. The use of a key distribution center

Second problem = digital signatures

Symmetric cryptosystems

public-key cryptosystems

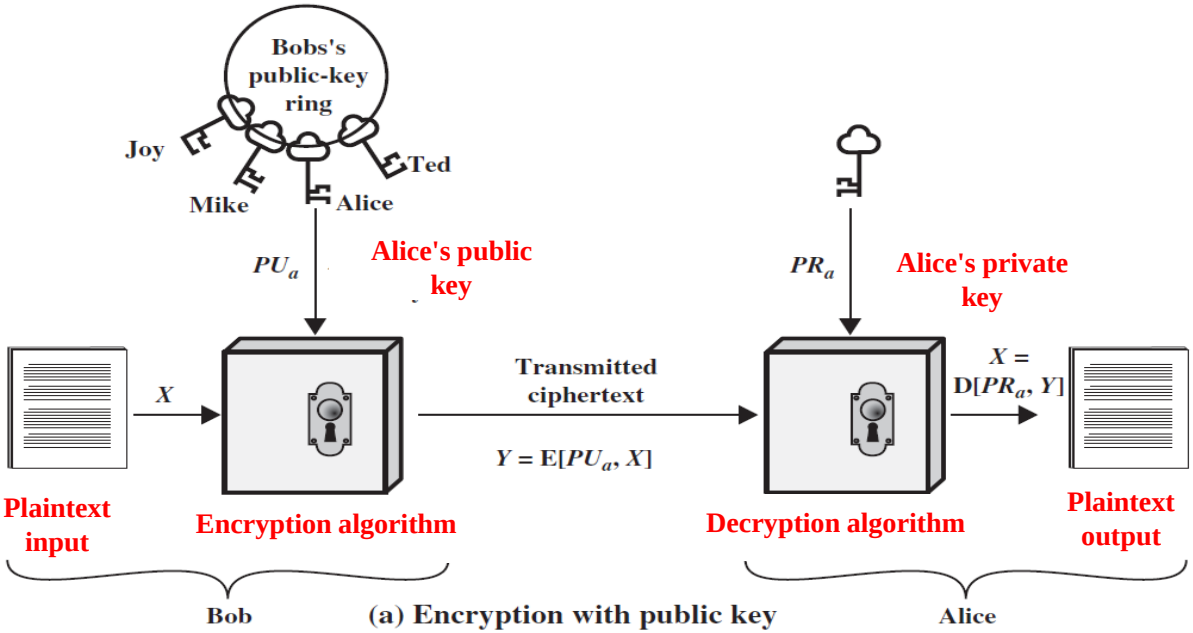


Public-Key Cryptography and RSA

Principles of Public-Key Cryptosystems

A public-key encryption scheme has six ingredients

1. Plaintext
2. Encryption algorithm
3. Public key
4. Private key
5. Ciphertext
6. Decryption algorithm

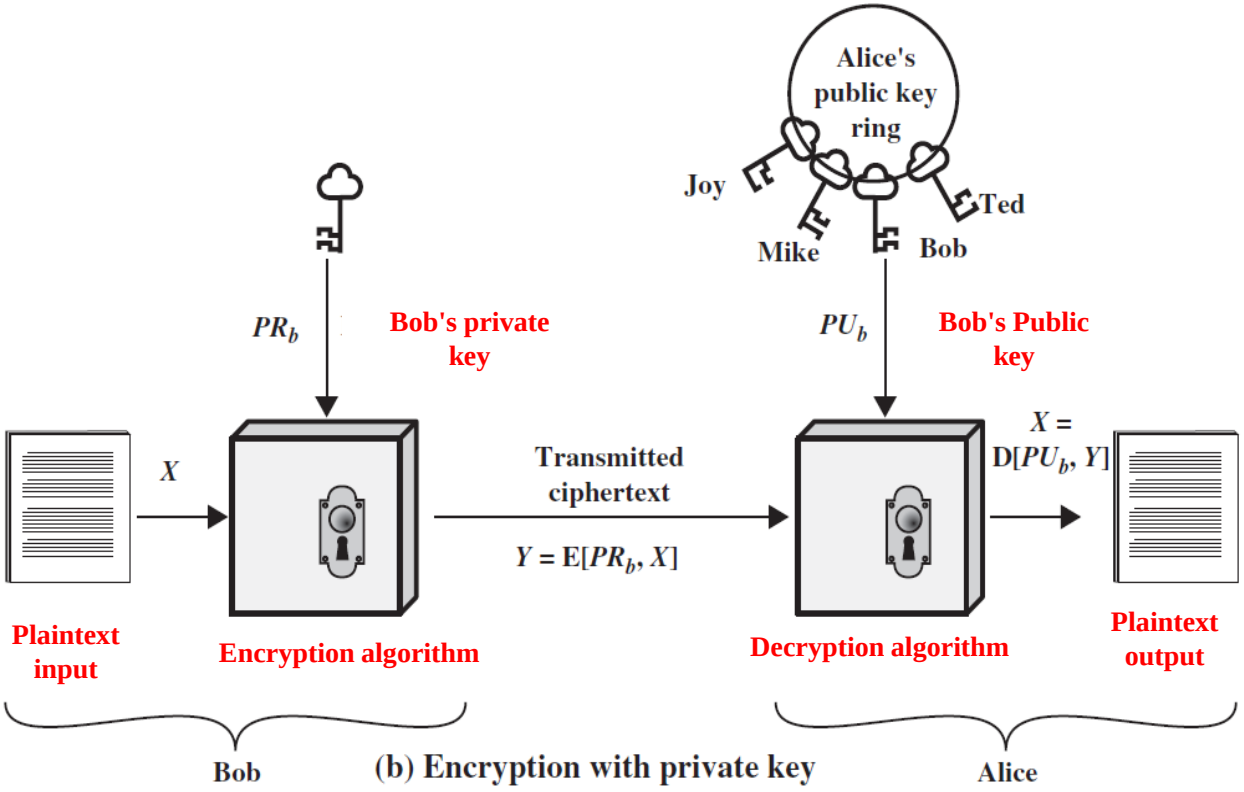


Public-Key Cryptography and RSA

Principles of Public-Key Cryptosystems

A public-key encryption scheme has six ingredients

1. Plaintext
2. Encryption algorithm
3. Public key
4. Private key
5. Ciphertext
6. Decryption algorithm

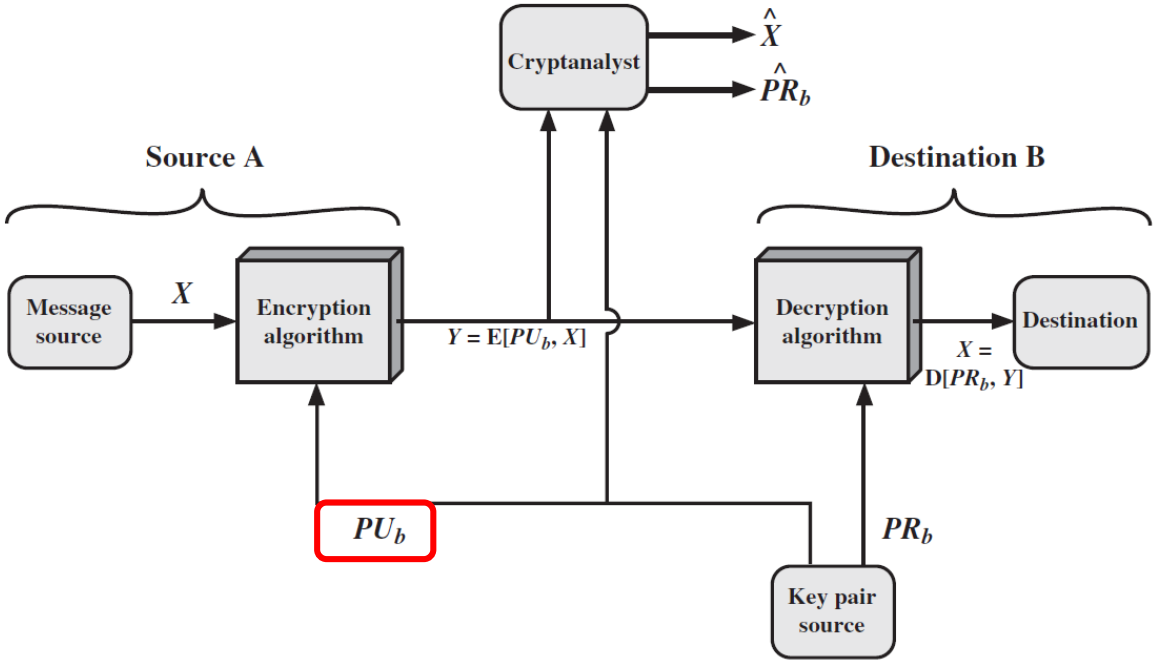


Conventional and Public-Key Encryption

Conventional Encryption	Public-Key Encryption
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key. *Needed for Security:* 1. The key must be kept secret. 2. It must be impossible or at least impractical to decipher a message if the key is kept secret. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	*Needed to Work:* 1. One algorithm is used for encryption and a related algorithm for decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not the same one). *Needed for Security:* 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if one of the keys is kept secret. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

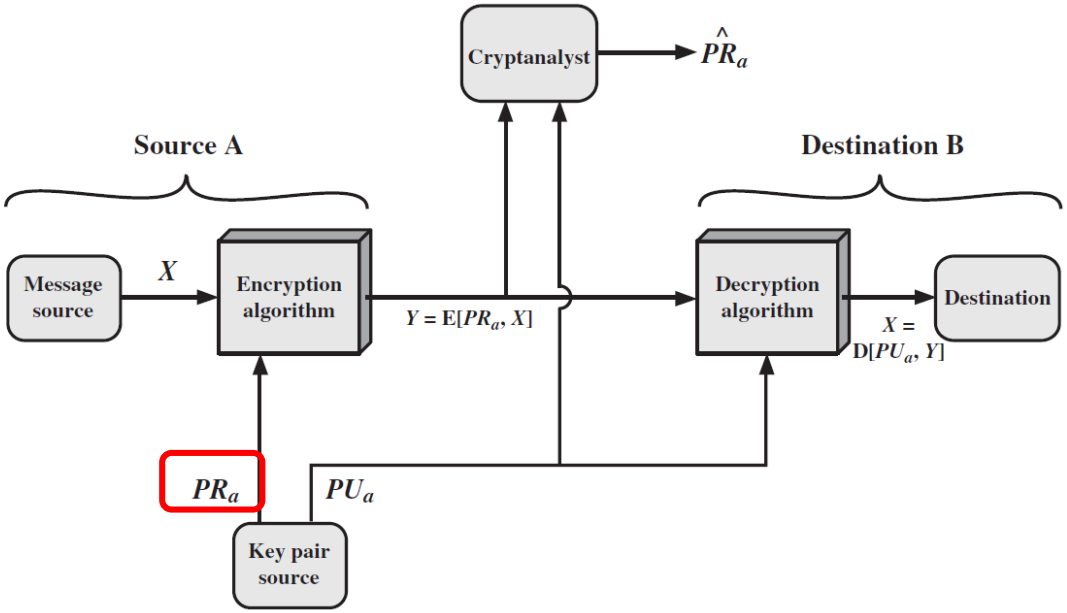
Public-Key Cryptosystem: Secrecy

- Source A that produces a message in plaintext{X = [X1, X2, … , XM]}
- The message's destination is destination B.
- Message X and the PU_b as input, A forms the ciphertext Y = [Y1, Y2, … , YN]
- Y = E(PU_b, X) (PU_b = public key)
- The receiver, in possession of the matching private key, is able to invert the transformation
- X = D(PR_b,



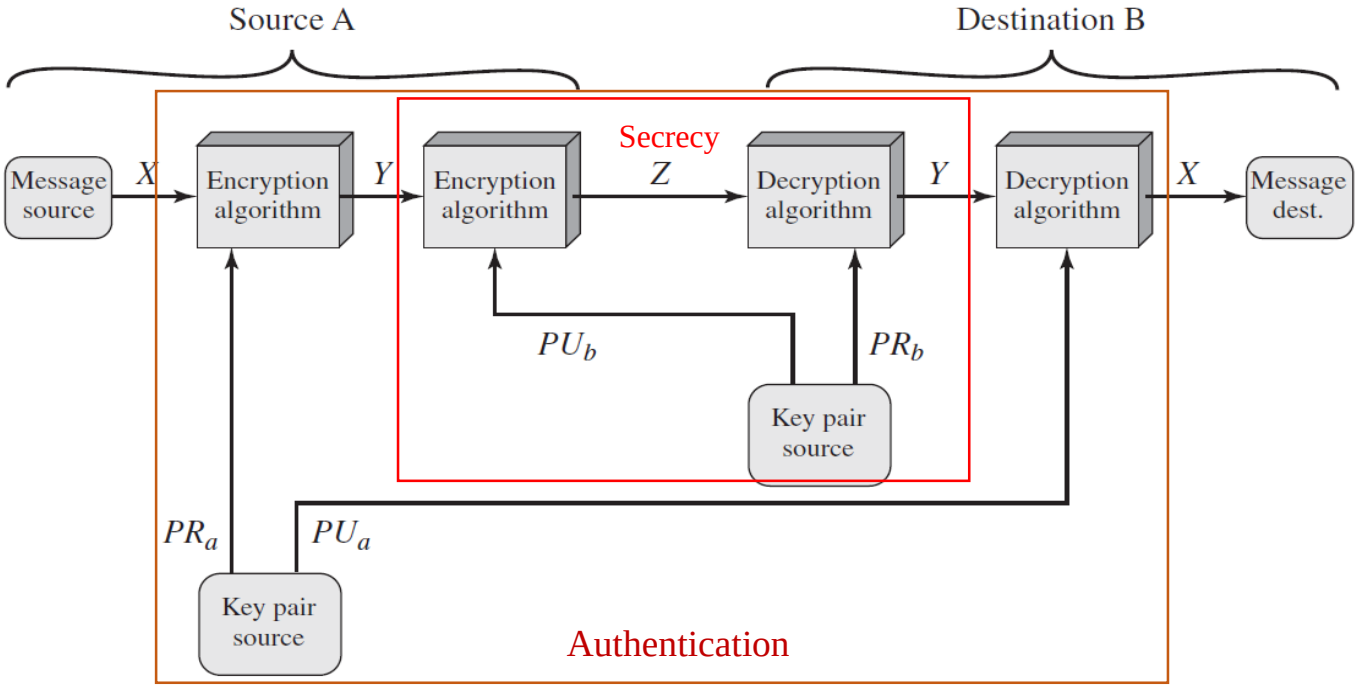
Public-Key Cryptosystem: Authentication

- $Y = E(PR_a, X)$
- $X = D(PU_a, Y)$
- Encrypts message using A's PR_a before transmitting it. B can decrypt it using A's PU_a.
- Encrypted using A's private key, only A could have prepared the message. = digital signature
- Authentication does not provide confidentiality.
- because any observer can decrypt the message by using the sender's public key(PU_a).



Public-Key Cryptosystem: Authentication and Secrecy

- Encrypting a message, using the sender's private key.(Digital signature)
- Next, we encrypt again, using the receiver's public key.
- Disadvantage = Complex public key algorithms should be performed four times.
- $Z = E(PU_b, E(PR_a, X))$
- $X = D(PU_a, D(PR_b, Z))$



Applications for Public-Key Cryptosystems

- Secrecy :Encryption/decryption(PU_b :The sender encrypts a message with the recipient's public key.)
- Authentication : Digital signature(PR_a : The sender "signs" a message with its private key.)
- Key exchange (to exchange a session key)

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No

Requirements for Public-Key Cryptography

- Public-Key algorithm's Conditions (Diffie and Hellman)
  1. It is easy to generate a pair
     PU_b , PR_b
  2. It is easy to generate the ciphertext
     $C = E(PU_b , M)$
  3. It is easy to recover the original message
     $M = D(PR_b, C) = D[PR_b, E(PU_b, M)]$
  4. It is infeasible knowing the public key, PU_b, to determine the private key, PR_b.
  5. It is infeasible knowing the public key, PU_b, a ciphertext, C, to recover the original message, M.
  6. The two keys can be applied in either order(add a sixth requirement)
     $M = D[PU_b, E(PR_b, M)] = D[PR_b, E(PU_b, M)]$

Trap-door one-way function

Easy to calculate in one direction and infeasible to calculate in the other direction unless certain additional information is known.

$Y = f_k(X)$ easy, if k and X are known

$X = f_{k-1}(Y)$ easy, if k and Y are known

$X = f_{k-1}(Y)$ infeasible, if Y is known but k is not known

Public-Key Cryptography and RSA

Principles of Public-Key Cryptosystems

- RSA is one of the public-key cryptography algorithm
- Developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman and published in 1978
- The plaintext and ciphertext are integers between 0 and (n – 1) for n
- A typical size for *n* is 1024 bits, or 309 decimal digits.
- Slower to calculate than the secret key cryptography DES.
- Safety is based on the difficulty of prime factorization

RSA Encryption Algorithm

- Public key = PU = {e, n}
- Private key = PR = {d, n}
- Encryption
  - $C = M^e \bmod n$
- Decryption
  - $M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

Generate order Key pair

1. Find the value of N
2. Find the value of L
3. Find the value of E
4. Find the value of D

Both sender and receiver must know the value of n.

The sender knows the value of e

The receiver knows the value of d

PU = {e, n}, PR = {d, n}

Ex) p = 17, q = 11, two prime numbers (private, chosen)

1. Find the value of **N**

   n = p×q = 17 ×11 =187 (public, calculated)

2. Find the value of **L= $\varphi(n)$**

   $\varphi(n) = \varphi(p \times q) = (p-1) \times (q-1)$=16 ×10=160

3. Find the value of **E**

   gcd($\varphi(n)$, e) = 1

   1 < e < $\varphi(n)$ = 1< e <160

   Select e such that e is relatively prime to $\varphi(n)$ = 160 and less than $\varphi(n)$

   Ex) choose e = 7

4. Find the value of **D**

   D < L = 160

   DE ≡ 1(mod L) = d × 7=161=(1mod160)

   D = 23

Public-Key Cryptography and RSA

Principles of Public-Key Cryptosystems

1. Find the value of N = 187
2. Find the value of L= $\varphi(n)$ =160
3. Find the value of E = 7
4. Find the value of D =23

PU = {7, 187}, PR = {23, 187} M = 88

PU = {e, n}, PR = {d, n}

Encryption

C = M^e mod n

C = 88^7 mod 187 = **11**

Decryption

M = C^d mod n

M = 11^{23}mod 187 = 88

Group-Ring-Field

Group

A GROUP $(G,*)$ is a set G which is CLOSED under an operation $*$ and satisfies the following properties:

- Ex) $(\mathbb{Z},+,0)$
- CLOSED
  - ✓ For any $x, y \in G$, $x * y \in G$
- $\mathbb{Z}$ is a set of integers
- Identity
  - ✓ There is an element e in G, such that for every $x \in G$, $x * e = e * x = x$.
  - ✓ $5 + 0 = 0 + 5 = 5$ (Identity element = 0)
- Inverse
  - ✓ For every x in G there is an element $y \in G$ such that $x * y = y * x = e$, where again e is the identity
  - ✓ $5 + (-5) = 0$, $8 + (-8) = 0$
- Associativity
  - ✓ The following identity holds for every $x, y, z \in G$: $x * (y * z) = (x * y) * z$
  - ✓ $(5+3)+(-2) = (5) + (3+(-2)) = 6$

Group-Ring-Field

Ring

A RING $(\mathbb{R},+,\times,0)$ is a set R which is CLOSED under two operations $+$ and $\times$ and satisfying the following properties:

- $\mathbb{R}$ is an "abelian group" under $(+)$ if $x * y = y * x$ for every $x, y \in G$.
- (R, +)
  - Identity
    - ✓ $a + 0 = 0 + a = a$
  - Inverse
    - ✓ $a + (-a) = (-a) + a = 0$
  - Commutative
    - ✓ $a + b = b + a$
  - Associative
    - ✓ $(a + b) + c = a + (b + c)$
- (R, ×)
  - Associative
    - ✓ $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- (R, +, ×)
  - Distributive
    - ✓ $a \times (b + c) = (a \times b) + (a \times c)$
    - ✓ $(b + c) \times a = b \times a + c \times a.$

Group-Ring-Field

Ring

A RING $(\mathbb{R},+,\times,0)$ is a set R which is CLOSED under two operations + and × and satisfying the following properties

- Commutative ring
  - ✓ A ring in which the multiplication operation is commutative.
  - ✓ $a \times b = b \times a$ (commutative)
- Ring with unity
  - ✓ $1 \in R$
  - ✓ $a \times 1 = a = 1 \times a$
- Division ring
  - ✓ every non-zero element of R has a (unique) non-zero product inverse.
  - ✓ Every non-zero element of R is a unit.
  - ✓ R has no proper elements.
  - ✓ $a \in R, a \neq 0$
  - ✓ $a \times a^{-1} = a^{-1} \times a = 1$

Group-Ring-Field

Field

A FIELD is a set F which is CLOSED under two operations + and × such that

- Commutative division ring
- (F, +) is a commutative (additive) group
  - ✓ (identity) : a + 0 = a = 0 + a
  - ✓ (inverse) : a + (-a) = 0 = (-a) + a
  - ✓ (associativity) : (a + b) + c = a + (b + c)
  - ✓ (commutativity) : a + b = b + a
- (F, - {o}, ·) is a commutative (multiplicative) group.
  - ✓ (identity) : $a \times 1 = a = 1 \times a$
  - ✓ (inverse) : $a \times a^{-1} = 1 = a^{-1} \times a$ if $a \neq 0$
  - ✓ (associativity) : $(a \times b) \times c = a \times (b \times c)$
  - ✓ (commutativity) : $a \times b = b \times a$
- (F,+, ·)
  - ✓ (distributivity) : $a \times (b + c) = a \times b + a \times c$

Attack on the RSA algorithm

Brute force , Mathematical attack

- Brute force
  - Trying all possible private keys.
  - Countermeasure
    - ✓ Use a large key space
  - However, the larger the size of the key, the slower the system will run.
- Mathematical attack
  - Three approaches
    - ✓ N a case that can be factorization into two primes
      - ✓ No suitable algorithm
    - ✓ p and q is the determined directly without determining L
      - ✓ Difficult as factorization
    - ✓ Determining a first D directly without determining the L
      - ✓ Difficult as factorization

Attack on the RSA algorithm

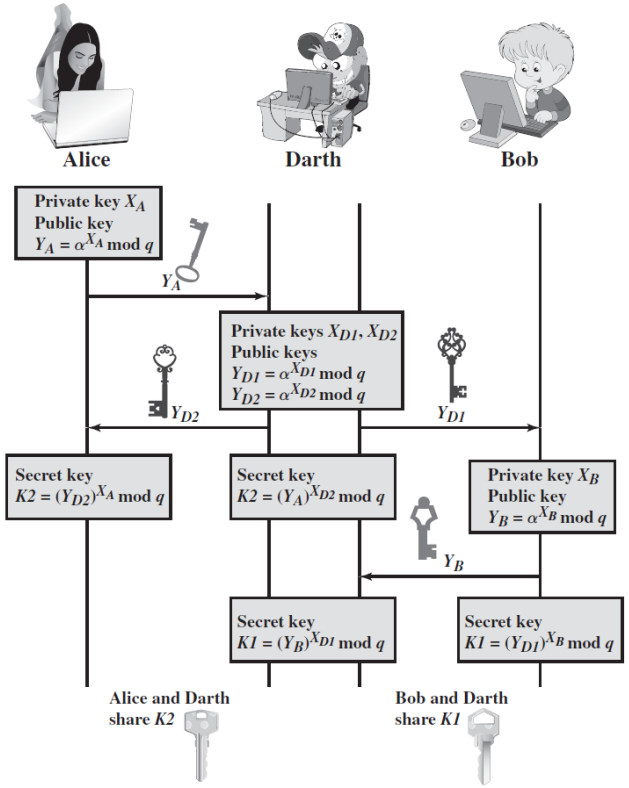
Timing attack

- When the running time of a cryptographic algorithm is nonconstant, timing measurements can leak information about the secret key.
- Countermearsures
  - Constant exponentiation time :
    - ✓ Ensure that all exponentiations take the same amount of time before returning a result.
  - Random delay :
    - ✓ Better performance could be achieved by adding a random delay to the exponentiation algorithm
  - Blinding :
    - ✓ Multiply the ciphertext by a random number before performing exponentiation.

Attack on the RSA algorithm

Man in the middle Attack

1. Alice sends an encrypted message M: E($K2$, M).
2. Darth intercepts the encrypted message and decrypts it to recover M.
3. Darth sends Bob $E(K1, M)$ or E($K1$, M'), where M' is any message.
4. In the first case, Darth simply wants to eavesdrop on the communication without Altering it.
5. In the second case, Darth wants to modify the message going to Bob.



Thank you