# Asymmetric Ciphers: Discrete Logarithmic algorithms

2019. 3. 25

# Contents

# 3 kinds of public key crypto

- There are 3 kinds of mathematically hard one-way functions on which the public key crypto are based.
  - Factoring integers
    - RSA
  - Discrete Logarithm
    - Diffie-Hellman, Elgamal, DSA
  - Elliptic curve: generalized discrete log
    - ECDH, ECDSA

# Group

Def:
A set G and an binary operation ☺ on elements of G have the following properties:

1. The operation is closed.
2. The operation is associative.
3. There is an element $1 \in G$ called identity, such that $a☺1=1☺a=a$ for all $a \in G$.
4. There is an element $a^{-1}$ called inverse, such than $a☺a^{-1}=a^{-1}☺a=1$ for all $a \in G$.
5. A set G is called abelian Group if the operation is commutative.

# Examples of Group

(1)($Z$, $+$) ;
(2)($C$, $\cdot$)
(3)($Z^*_{11}$, multiplicative modulo p)

# Order of an element

Def:

An order, ord(a), of an element a of a group (G, ☺) is the smallest positive integer k such that

$$a^k = \underbrace{a☺a☺a☺a☺ \ldots ☺a}_{\text{k times}} = 1$$

where 1 is the identity of G.

# Cyclic Group

Def:
A group G which contains an element a with maximum order ord(a) = |G| is said to be cyclic.
(|G| is a finite number of elements, called cardinality or order of group G)

Elements with maximum order are called primitive elements or generators.

# Example of Cyclic Group

Suppose a group $Z^*_{11}$={1,2,3,…,10).

What happens if we compute $2^x$ mod 11.

Observation:
"2" generates all members of $Z^*_{11}$ at every $11^{th}$ computation.

So, $Z^*_{11}$ is a cyclic group, and 2 is called a generator of $Z^*_{11}$.
(ord(2) = | $Z^*_{11}$ | )

$2^1$ mod 11=2
$2^2$mod 11=4
$2^3$mod 11=8
$2^4$mod 11=5
$2^5$mod 11=10
$2^6$mod 11=9
$2^7$mod 11=7
$2^8$mod 11=3
$2^9$mod 11=6
$2^{10}$mod 11=1
$2^{11}$mod 11=2
$2^{12}$mod 11=4

a cyclic group $Z^*_{11}$={1,2,3,...,10).

ord(5) = ?
ord(10) = ?

For a group $Z^*_{11}=\{1,2,3,\ldots,10)$,

ord(1) =1, ord(2)=10, ord(3) = 5, ord(4) = 5, ord(5) = 5,
ord(6) =10, ord(7)=10, ord(8) = 10, ord(9) = 5, ord(10) = 2

## How can we constitute a cyclic group $Z^*_p$?

Theorem:

For every prime p, $(Z^*_p, \cdot)$ is a finite cyclic group.

# Discrete Logarithm Problem(DLP)

Given a finite cyclic group $Z_p^*$ of order p-1 and a primitive element $g \in Z_p^*$ and another element $y \in Z_p^*$.

The DLP is the problem of determining the integer x such that

$1 \leq x \leq p-1$

$g^x = y \bmod p$, i.e., $x = \log_g y \bmod p$

In the previous example,

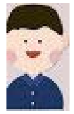
$2^x = 3 \bmod 11$, then what is x?

$5^x = 41 \bmod 47$, then what is x?

# Diffie-Hellman key exchange

Alice 

$p$, $g$ : public

Bob 

Select $a \in \{2,3,\ldots,p-2\}$
(private to Alice)
Compute $A = g^a \bmod p$

Select $b \in \{2,3,\ldots,p-2\}$
(private to Bob)
Compute $B = g^b \bmod p$

$$\xrightarrow{\quad A \quad}$$

$$\xleftarrow{\quad B \quad}$$

$K_{AB} = B^a \bmod p = g^{ab} \bmod p$

$K_{AB} = A^b \bmod p = g^{ab} \bmod p$

Message $m$
Encrypt: $x = E_{K_{AB}}(m)$

$$\xrightarrow{\quad x \quad}$$

Decrypt: $m = D_{K_{AB}}(x)$

# Security of D-H

- Suppose an attacker can only listen the channel(passive attack).
  - What can he know? g, p, A, B
  - What does he want to know? $K_{AB}=g^{ab} \bmod p$
- One way of solving the problem is:
  - Compute $a = \log_g A \bmod p$ or $b = \log_g B \bmod p$
- This computation is a very hard problem if p is large enough.

# Brute Force Attack

- Attacks against the DLP
  - Goal: solve $g^x = y \bmod p$ or $x = \log_g y \bmod p$
    - g, y$\in Z_p^*$,
    - n=the number of elements of $Z_p^*$(cardinality of $Z_p^*$= p-1)
  - Brute force attack requires O(n) steps.
  - If this is the only possible attack, $n \geq 2^{80}$. (more than 80 bits)

# Square-Root Attacks

- This attack is possible for any group.
- the Square-Root method can compute x in $\sqrt{n}$ steps.
- So, choose $n=2^{160}$.

- (ref: Handbook of Applied Cryptography, Alg 3.56, 3.60)

# Attack: Index-Calculus Methods

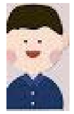
- This attack works for a certain group, especially $Z_p$* and $GF(2^m)$*.
- For this reason, in practice $p=2^m \geq 2^{1024}$

- (ref: Handbook of Applied Cryptography, Alg 3.68)

# Encryption with D-H

Alice 

$p, g$ : public

Bob 

Select $a \in \{2,3,\ldots,p-2\}$
(private to Alice)
Compute $A = g^a \bmod p$

Select $b \in \{2,3,\ldots,p-2\}$
(private to Bob)
Compute $B = g^b \bmod p$

$\xrightarrow{\quad A \quad}$

$\xleftarrow{\quad B \quad}$

$K_{AB} = B^a \bmod p = g^{ab} \bmod p$

$K_{AB} = A^b \bmod p = g^{ab} \bmod p$

Message $m$
Encrypt: $x = m \cdot K_{AB} \bmod p$

$\xrightarrow{\quad x \quad}$

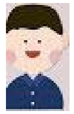
Decrypt: $m = x \cdot K_{AB}^{-1} \bmod p$


18

# Elgamal Encryption algorithm

- Was published around 1985
- Very similar to D-H, but the steps are reordered.
- Is a probabilistic encryption.

Alice 

Bob 

Select p, $g \in \{2,3,\ldots,p-2\}$

$K^{-} = d \in \{2,3,\ldots,p-2\}$

$K^{+} = \beta = g^{d} \bmod p$

$(K^{+}=\beta, g, p)$ ←

Select $i \in \{2,3,\ldots,p-2\}$

$K_E = g^i \bmod p$ (ephemeral key)

$K_M = \beta^i \bmod p$ (session key)

Message m

Encrypt: $x = m \cdot K_M \bmod p$

→ $(x, K_E)$

$K_M = K_E^{\,d} \bmod p$

Decrypt: $m = x \cdot K_M^{-1} \bmod p$

# Proof

Bob computes:

$$
\begin{aligned}
x \cdot K_M^{-1} &= x(K_E^{d})^{-1} \\
&= m\, K_M\, K_E^{-d} \\
&= m\, \beta^{i}\, (g^{i})^{-d} \\
&= m\, (g^{d})^{i}\, (g^{i})^{-d} \\
&= m
\end{aligned}
$$

In Elgamal encryption, the public key($K^{+}=\beta$) is fixed, but i is chosen for each message. So, $K_E$ must be different for every plaintext. And the procedures are reduced to two steps.