Introdução à Chave Pública

- Troca de chaves Diffie-Hellman
- Grupos finitos
- Grupos cíclicos

Troca de Chaves de Diffie-Hellman

- Parâmetros públicos p, α
- Alice:
  1 Sorteia $a = K_{prA} \in \{2, 3, \ldots, p-2\}$
  3 Envia para Bob $A = \alpha^a \mod p$
  5 Calcular $K_{AB} = B^a \mod p$
- Bob:
  2 Sorteia $b = K_{prB} \in \{2, 3, \ldots, p-2\}$
  4 Envia para Alice $B = \alpha^b \mod p$
  5 Calcular $K_{BA} = K_{AB} = A^b \mod p$
- Depois da troca de chaves, usar K_{AB} como chave secreta (simétrica) no AES!

Explicando Diffie-Hellman

- Como escolher primo p?
- Como escolher inteiro α?
- Como o uso desses parâmetros garante a segurança?

Ideias gerais

- Garantia é dada por álgebra em grupos de números inteiros
- Grupos cíclicos permitem avaliar, controlar e garantir nível de segurança
- Temos técnicas baseadas em teoremas de grupos finitos cíclicos que permitem construir grupos em que as operações de troca de chave de Diffie-Hellman são seguras
  - Problema do log discreto
  - Problema das curvas elípticas
- Operações de D-H são seguras porque constituem uma função de 1 via
  - Ida é barata (computar chave pública) = exponenciação
  - Volta é cara (descobrir parâmetro privado) = log discreto

Álgebra de grupo e subgrupos finitos e cíclicos

- Grupo $(G, \circ)$:
  - 4 propriedades obrigatórias: $a \circ b \in G$, $a \circ (b \circ c) = (a \circ b) \circ c$, $1 \circ a = a$, $a^{-1} \circ a = 1$
  - 1 propriedade para grupo abeliano: $a \circ b = b \circ a$
- Exemplos de grupos
  - Grupo aditivo: $(\mathbb{Z}, +)$,
  - Grupos multiplicativo: $(\mathbb{C}, \cdot)$

Criado um grupo finito

- Vejamos $(\mathbb{Z}_n, \times \mod n)$.
- Exemplo
  - $\mathbb{Z}_9 = 0, 1, 2, 3, 4, 5, 6, 7, 8$
  - Mas existe inversa somente quando $i \in \mathbb{Z}_9$ tem $mdc(9, i) = 1$
  - Então $(\mathbb{Z}_n, \times \mod n)$ NÃO é um grupo

Grupo especial $(\mathbb{Z}_n^*, \times \mod n)$

- Grupo multiplicativo $(\mathbb{Z}_n^*, \times \mod n)$
  - Serve como base para construir um grupo "seguro" que exponenciação é rápida e log é lento
  - $\mathbb{Z}_n^*$ é conjunto de inteiros $1 \leq i \leq n - 1$ coprimos de n
    - Se $mdc(i, n) = 1$, então i é coprimo de n
    - Contém somente número com inversa (ao contrário de $\mathbb{Z}_n$)
  - Propriedade: ordem ou cardinalidade é $|\mathbb{Z}_n^*| = \Phi(n)$
    - Exercício: $|\mathbb{Z}_1^*6| =?$
    - Exercício: qual é o n tal que $|\mathbb{Z}_n^*| = 8$?
    - Exercício: fazer um programa que, para um dado $\Phi(n)$, encontre n.

Exemplo: grupo especial ($\mathbb{Z}_9^*, \times \mod 9$)

- $\mathbb{Z}_n^* = \{1, 2, 4, 5, 7, 8\}$
- Exercício: prencher

$\times \mod 9$	1	2	4	5	7	8
1						
2						
4						
5						
7						
8						

Operação de exponenciação

- Dado $(\mathbb{Z}_n^*, \times \mod n)$, elementos do grupo estão de alguma forma ligados entre si quando fazemos exponenciação por causa da operação $\mod n$
- Exemplo
  - $\mathbb{Z}_{11}^*$ e um elemento $a = 3 \in \mathbb{Z}_{11}^*$
  - Potências $\mod 11$:
    - $\{1, 3, 9, 5, 4, 1, 3, \ldots\}$ ... um ciclo!
- Exercício: obter ciclo para $\mathbb{Z}_{11}^*$ e um elemento $a = 2$

Ordem de um elemento

- Seja $(\mathbb{Z}_n^*, \circ = \times \mod n)$
- Ordem de a é $ord(a)$ é o menor inteiro k que forma um ciclo
  - $a^k = a \circ a \circ \ldots \circ a = 1 \mod n$
- Se grupo tem N elementos e $ord(a) = N$ então a ordem de a é máxima e a é chamado de primitivo ou gerador
  - 2 é gerador de $\mathbb{Z}_n^*$
- Exercício: escrever algoritmo para encontrar a ordem de um elemento a para $\mathbb{Z}_p^*$, dados a e p.

Grupo cíclico

- Um grupo cíclico é um grupo que tem pelo menos 1 elemento com ordem máxima
- Exemplo:
  - Se 2 é gerador de $\mathbb{Z}_n^*$ então para qualquer elemento a em $\mathbb{Z}_n^*$ existe um i tal que $2^i = a \mod n$
- Grupos cíclicos são a base de sistemas de criptografia assimétrica!

Se n é primo, então $\mathbb{Z}_n^*$ é grupo finito cíclico abeliano!

Propriedade importante 1: só existem elementos com *ord* que divide $|G|$

- Se $a \in G$, G é grupo cíclico
  1. $a^{|G|} = 1$
  2. $ord(a)$ divide $|G|$ (resto zero)
- Comentário: se existem elementos de diferentes ordens em G então, essas propriedades indicam a possibilidade de seleção de um subgrupo com todos os elementos com ordem máxima (todas as ordem são iguais exceto para o elemento 1)
- Exercício: $|\mathbb{Z}_{11}^*| = 10$, quais são as possíveis ordens de elementos?

Propriedade importante 2: número de elementos primitivos

- Se G é grupo finito cíclico, então
  1. número de geradores α é $\Phi(|G|)$
     - Exemplo: em $\mathbb{Z}_{11}^*$
       $H_1 = \{1\}$, $\alpha = 1$
       $H_2 = \{1, 10\}$, $\alpha = 10$
       $H_3 = \{1, 3, 4, 5, 9\}$, $\alpha = 3, 4, 5, 9\}$
     - Exercício: escrever algoritmo que recebe $p_1, e_1, p_2, e_2 \ldots$ de $\mathbb{Z}^*_{p_1^{e_1} \times p_2^{e_2} \times \ldots}$ e encontra seus subgrupos cíclicos
  2. Se $|G|$ for primo, então todos elementos exceto 1 são geradores, ou seja, existem $|G| - 1$ elementos primitivos
- Importante usar grupos com ordem igual a um número primo para garantir que são cíclicos e elementos são todos geradores e é difícil obter x tal que $\alpha^x = \beta \mod n$ para α e β conhecidos!
- Se é difícil usar grupo com ordem prima, usar grupo com poucos subgrupos de alta ordem prima

Como escolher um bom grupo cíclico de maneira fácil?

- Se $(G, \circ)$ é cíclico, então $a \in G$ com $ord(a) = k$, então a é gerador de algum subgrupo cíclico com k elementos!!
- Indica que podemos criar subgrupos com (quase) todos elementos geradores facilmente!
- Exemplo:
  - Exercício: verificar propriedade no grupo $\mathbb{Z}_{11}^*$ e subgrupo de $a = 3$, $ord(3) = 5$
- Teorema de Lagrange: se H é subgrupo de G, então $|H|$ divide $|G|$
  - $|\mathbb{Z}_{11}^*| = 10 = 1 \cdot 2 \cdot 5$, ou seja, temos H_1, H_2, e H_3.
    - Exercício: mostrar esses subgrupos

Construção de (sub)grupos de ordem prima. Finalmente!

- Sejam G cíclico de ordem $|G| = n$ e um α gerador de G
- Para todo k que divide n, existe exatamente um subgrupo cíclico H, $|H| = k$.

> H é construído (gerado) a partir do elemento $\alpha^{n/k}$!

- Exemplo:
  - Temos $\alpha = 8$, $\mathbb{Z}_{11}^*$ e queremos um gerador para subgrupo de ordem 2:
    - $\alpha^{n/k} = 8^{10/2} = 8^5 \equiv 10 \mod 11$
    - então 10 vai gerar subgrupo com 2 elementos
    - Exercício: encontrar esses elementos