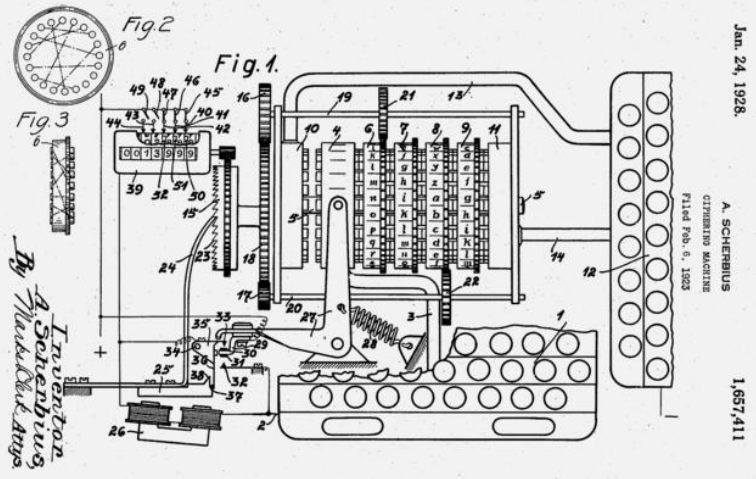
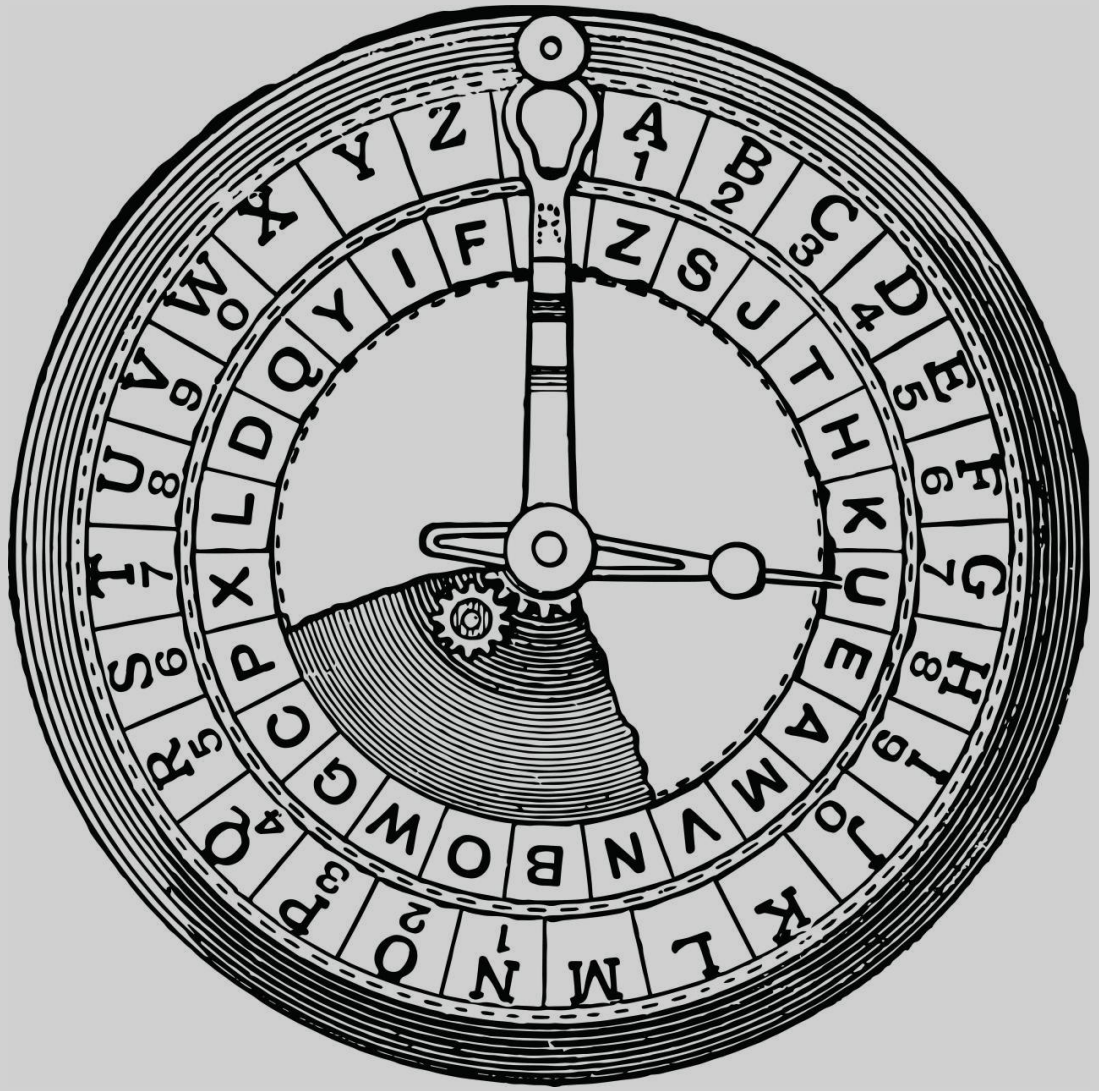
Logaritmo Discreto e Diffie-Hellman

Fundamentos da Criptografia

Nicollas Mocelin Sdroievski



Nas últimas aulas



Teoria de números

- O *maior divisor comum* (MDC ou GCD) de dois inteiros a e b, denotado por $\gcd(a, b)$ é o maior inteiro c tal que $c \mid a$ e $c \mid b$
  - Se $\gcd(a, b) = 1$, dizemos que a e b são relativamente primos
- **Proposição 8.2.** Sejam a e b inteiros positivos. Então existem $X, Y \in \mathbb{Z}$ tal que $Xa + Yb = \gcd(a, b)$. Além disso, $\gcd(a, b)$ é o menor inteiro positivo que pode ser escrito desta maneira.
- O algoritmo de Euclides pode ser usado para computar o $\gcd(a, b)$ em tempo polinomial (no tamanho das entradas)
  - A versão estendida do algoritmo também computa X, Y tal que $Xa + Yb = \gcd(a, b)$

Definição de grupos

- **Definição 8.9.** Um *grupo* é o um conjunto $\mathbb{G}$ junto de uma operação binária $\circ$ para os quais o seguinte é verdade:
  - **(Fechamento).** Para todos $g, h \in \mathbb{G}$, $g \circ h \in \mathbb{G}$.
  - **(Identidade).** Existe um elemento *identidade* $e \in \mathbb{G}$ tal que, para todo $g \in \mathbb{G}$, $e \circ g = g = g \circ e$.
  - **(Inversos).** Para todo $g \in \mathbb{G}$, existe um elemento $h \in \mathbb{G}$ tal que $g \circ h = e = h \circ g$. Este elemento h é chamado de *inverso* de g.
  - **(Associatividade)**. Para todos $g_1, g_2, g_3 \in \mathbb{G}$, $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$
- Vamos lidar com grupos finitos e abelianos, que obedecem a seguinte propriedade adicional
  - **(Comutatividade).** Para todos $g, h \in \mathbb{G}$, $g \circ h = h \circ g$.
- A ordem de um grupo finito $\mathbb{G}$, denotada por $|\mathbb{G}|$, é o número de elementos de $\mathbb{G}$

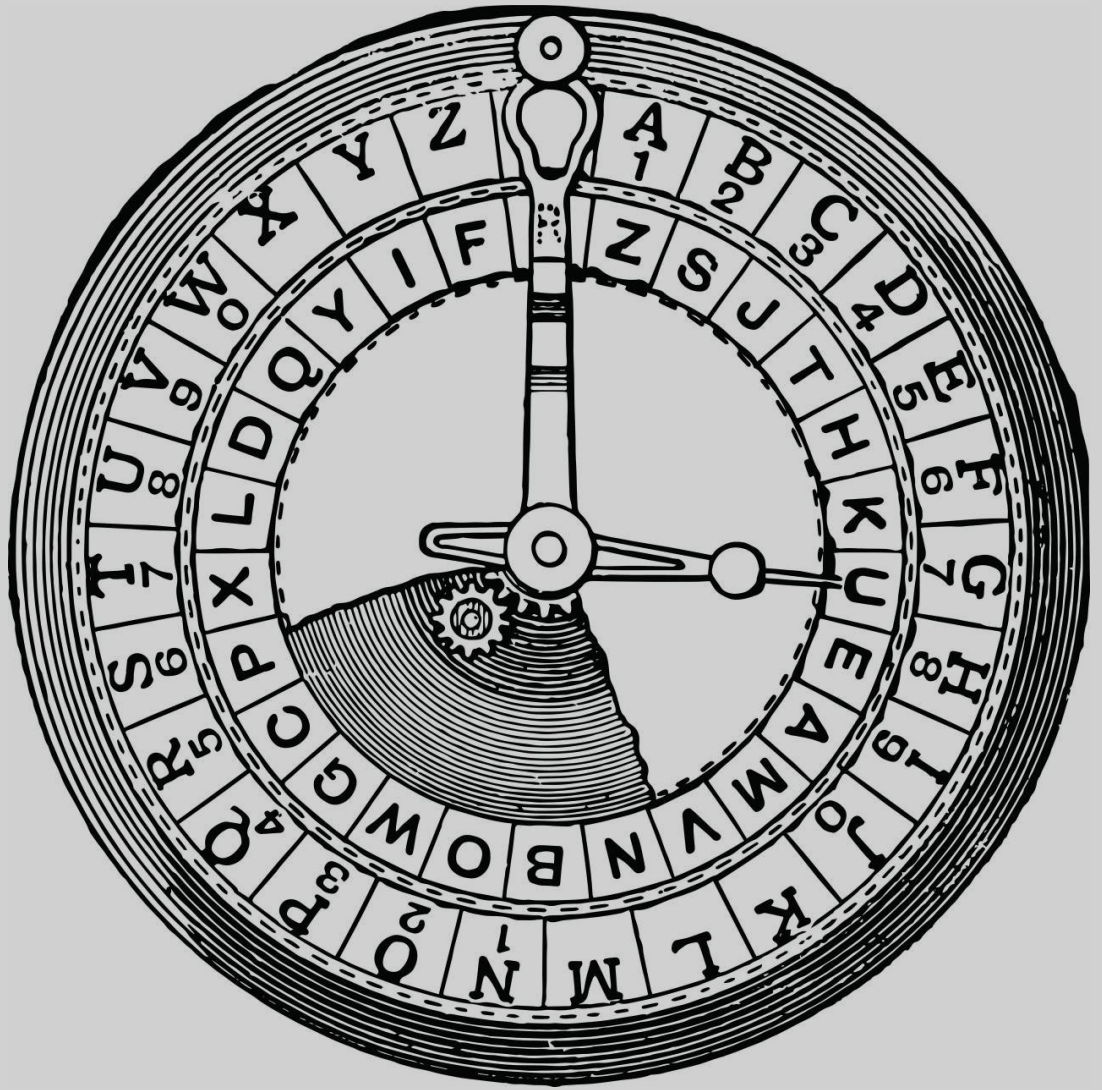
Alguns resultados

- **Lema 8.13.** Seja $\mathbb{G}$ um grupo e $a, b, c \in \mathbb{G}$. Se $ac = bc$, então $a = b$. Em particular, se $ac = c$ então a é a identidade de $\mathbb{G}$.

- **Teorema 8.14.** Seja $\mathbb{G}$ um grupo finito com ordem $|\mathbb{G}| = m$. Então, para qualquer elemento $g \in \mathbb{G}$, $g^m = 1$.

- **Corolário 8.15.** Seja $\mathbb{G}$ um grupo finito com ordem $|\mathbb{G}| = m > 1$. Então, para qualquer elemento $g \in \mathbb{G}$ e inteiro x, temos $g^x = g^{[x \bmod m]}$.

Um pouco mais sobre grupos



Grupos cíclicos e geradores

- Seja $\mathbb{G}$ um grupo de ordem m, e considere, para $g \in \mathbb{G}$, o conjunto
$$\langle g \rangle \doteq \{g^0, g^1, \dots\}$$
- Sabemos que $g^m = 1$, e seja $i \leq m$ o menor inteiro positivo tal que $g^i = 1$, segue que
$$\langle g \rangle \doteq \{g^0, g^1, \dots, g^{i-1}\}$$
- Chamamos $\langle g \rangle$ do subgrupo gerado por g, de ordem i
  - E também falamos que g tem ordem i
- **Proposição 8.52.** Seja $\mathbb{G}$ um grupo finito e $g \in \mathbb{G}$ um elemento de ordem i, então para todo inteiro x, temos $g^x = g^{[x \bmod i]}$.

Grupos cíclicos e geradores

- Podemos provar algo um pouco mais forte
- **Proposição 8.53.** Seja $\mathbb{G}$ um grupo finito, e $g \in \mathbb{G}$ um elemento de ordem i. Então $g^x = g^y$ se e somente se $x = y \bmod i$
- **Demonstração:** lembre que $g^i = 1$
- ($\Leftarrow$) Se $x = y \bmod i$, então pelo proposição anterior:

$$g^x = g^{[x \bmod i]} = g^{[y \bmod i]} = g^y$$

- ($\Rightarrow$) Se $g^x = g^y$, então $1 = g^{x-y} = g^{[x-y \bmod i]}$
  - Como $[x - y \bmod i] < i$, mas i é o menor inteiro positivo tal que $g^i = 1$, deve valer que $[x - y \bmod i] = 0$

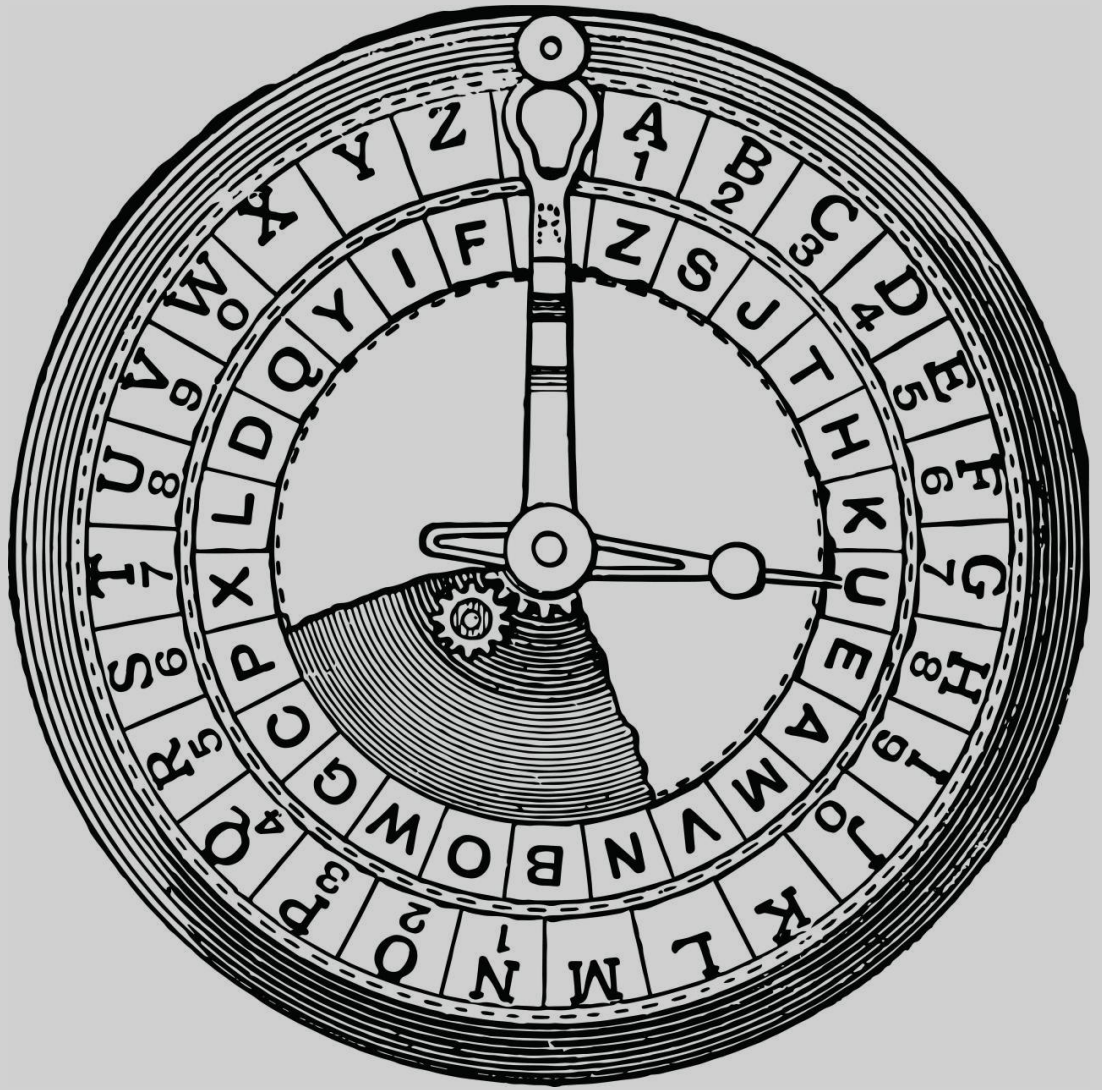
Mais alguns resultados

- **Proposição 8.54.** Seja $\mathbb{G}$ um grupo finito de ordem m, e seja $g \in \mathbb{G}$ um elemento com ordem i. Então $i \mid m$.
- **Demonstração:**
  - Sabemos, pelo Teorema 8.14 que $g^m = 1 = g^0$.
  - Também sabemos que $g^i = 1$.
  - Pela Proposição 8.53, $m = 0 \bmod i$.
- **Corolário 8.55.** Seja $\mathbb{G}$ um grupo finito de ordem p, então $\mathbb{G}$ é cíclico. Além disso, todo elemento de $\mathbb{G}$ com exceção da identidade é um gerador de $\mathbb{G}$.

Exemplos

- O grupo $\mathbb{Z}_p$ com a operação de adição módulo p é cíclico
  - Geradores?
    - Qualquer elemento que não seja a identidade é um gerador!
  - Exemplo $\mathbb{Z}_5$ e $4 \in \mathbb{Z}_5$
    - $0 \cdot 4 = 0$
    - $1 \cdot 4 = 4$
    - $2 \cdot 4 = 8 = 3 \bmod 5$
    - $3 \cdot 4 = 12 = 2 \bmod 5$
    - $4 \cdot 4 = 16 = 1 \bmod 5$
- O grupo $\mathbb{Z}_p^*$ com a operação de multiplicação modular é cíclico
  - Ordem?
    - $p - 1$, que não é primo!
  - Não tão fácil, porém possível encontrar um gerador em tempo polinomial caso se conheça a fatoração de $p - 1$

Logaritmo discreto e Diffie-Hellman



Introdução

- Veremos alguns problemas computacionais em grupos
  - Considerados difíceis para algumas escolhas específicas de grupos
- Vamos assumir algumas coisas sobre o grupo $\mathbb{G}$
  - Existe um algoritmo de geração de grupo $\mathcal{G}$ que, ao receber 1^n como entrada, produz a descrição de um grupo cíclico $\mathbb{G}$, sua ordem q e um gerador $g \in \mathbb{G}$ a
    - A descrição indica como cada elemento é representado (unicamente) através de uma string binária
    - $|q| = n$
  - Devem existir algoritmos eficientes para
    - A operação de grupo em $\mathbb{G}$
    - Testar se uma string é um elemento do grupo
    - Computar inversos
  - De graça, temos algoritmos eficientes para
    - Exponenciação
    - Sortear elementos uniformes de $\mathbb{G}$

Logaritmo discreto

- Se $\mathbb{G}$ é um grupo cíclico de ordem q com gerador g, então

$$\mathbb{G} = \{g^0, g^1, \dots, g^{q-1}\}$$

- Para cada $h \in \mathbb{G}$ existe um único valor $x \in \mathbb{Z}_q$ tal que $g^x = h$
  - Chamamos x do *logaritmo discreto de h com respeito à g* (ou na base g)
  - E escrevemos $x = \log_g h$
  - Note que se $g^{x'} = h$, então $x' = x \bmod q$

O experimento $\mathrm{DLog}_{\mathcal{A},\mathcal{G}}(n)$

Desafiante

Adversário $\mathcal{A}$
Tempo poli(n)



$(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$

$h \leftarrow \mathbb{G}$

$(\mathbb{G}, q, g, h)$

$x \in \mathbb{Z}_q$



- Observação: $\mathbb{G}$ possui ordem q com $|q| = n$
- $\mathcal{A}$ obtém sucesso (indicado por $\mathrm{DLog}_{\mathcal{A},\mathcal{G}}(n) = 1$) se $g^x = h$

Definição de dificuldade

- **Definição 8.62.** Dizemos que o problema do logaritmo discreto é difícil relativo à $\mathcal{G}$ se para todos os algoritmos probabilísticos polinomiais $\mathcal{A}$ existe uma função negligenciável negl tal que

$$\Pr\left[\mathrm{DLog}_{\mathcal{A},\mathcal{G}}(n) = 1\right] \leq \mathrm{negl}(n)$$

- Dificuldade depende da escolha de $\mathcal{G}$, e em particular, do grupo $\mathbb{G}$
  - Fácil para $(\mathbb{Z}_p, +)$ onde p é um número primo
  - Considerado difícil para $(\mathbb{Z}_p^*, \times)$
  - Considerado ainda mais difícil para pontos em curvas elípticas

Fácil para $(\mathbb{Z}_p, +)$ onde p é um número primo

- Exemplo:
  - $p = 17$
  - $g = 3$
  - $x \cdot g = 8$
  - Como descobrir x tal que $3 \cdot x = 8 \mod 17$?
    - Basta encontrar o inverso **multiplicativo** de 3 módulo 17
    - $x = 3^{-1} \cdot 8 \bmod 17$
    - Possível computar de maneira eficiente com o algoritmo estendido de Euclides
    - $3^{-1} = 6 \bmod 17$
    - $x = 6 \cdot 8 = 48 = 14 \bmod 17$
    - Conferindo: $14 \cdot 3 = 42 = 8 \bmod 17$

Os problemas de Diffie-Hellman

- Relacionados, porém não necessariamente equivalentes, à computar logaritmos discretos
  - Tema razoavelmente comum em criptografia
- Duas versões
  - Versão de busca (*Computational Diffie-Hellman*)
  - Versão de decisão (*Decisional Diffie-Hellman*)

Versão de busca

- Fixe um grupo cíclico $\mathbb{G}$ e um gerador $g \in \mathbb{G}$.
- Dados elementos $h_1, h_2 \in \mathbb{G}$, definimos

$$\mathrm{DH}_g(h_1, h_2) = g^{\log_g h_1 \cdot \log_g h_2}$$

- Isto é, se $h_1 = g^{x_1}$ e $h_2 = g^{x_2}$, então

$$\mathrm{DH}_g(h_1, h_2) = g^{x_1 \cdot x_2} = h_1^{x_2} = h_2^{x_1}$$

Dificuldade e relação com logaritmo discreto

- A versão computacional CDH do problema envolve computar $\mathrm{DH}_g(h_1, h_2)$ para h_1 e h_2 aleatórios
  - Relativamente direto construir um experimento que captura essa dificuldade
- Se o problema do logaritmo discreto relativo à $\mathcal{G}$ é fácil, então CDH também é
  - Dados h_1 e h_2, basta computar
    - $x_1 = \log_g h_1$
    - $x_2 = \log_g h_2$
    - E então retornar $g^{x_1 \cdot x_2}$
- Não se sabe se a dificuldade do problema CDH implica na dificuldade do problema do logaritmo discreto

Versão de decisão

- De maneira simplificada, envolve distinguir $\mathrm{DH}_g(h_1, h_2)$ de um elemento uniforme do grupo quando h_1 e h_2 são uniformes
- Duas maneiras de definir
  - Experimento em que o adversário tenta adivinhar se o valor recebido é $\mathrm{DH}_g(h_1, h_2)$ ou um elemento uniforme do grupo
  - Tratar o adversário como um distinguidor (no estilo PRG, PRF)
- Potencialmente “mais fácil” do que a versão de busca

Experimento $\mathrm{DDH}_{\mathcal{A},\mathcal{G}}(n)$

Desafiante



$(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$

$x, y, z \leftarrow \mathbb{Z}_q$

$b \leftarrow \{0,1\}$

$(\mathbb{G}, q, g, g^x, g^y, g^z)$ **OU** $(\mathbb{G}, q, g, g^x, g^y, g^{xy})$

b' = chute para b

Adversário $\mathcal{A}$
Tempo poli(n)



- Se $b = 0$, desafiante envia $(\mathbb{G}, q, g, g^x, g^y, g^z)$
  - g^z é aleatório, sem relação com $g^x = h_1$ e $g^y = h_2$
- Se $b = 1$, desafiante envia $(\mathbb{G}, q, g, g^x, g^y, g^{xy})$
- Se $\mathcal{A}$ acerta, temos que $\mathrm{DDH}_{\mathcal{A},\mathcal{G}}(n) = 1$ e dizemos que o experimento foi um sucesso

Dificuldade (duas definições equivalentes)

- **Definição 8.63.** Dizemos que o problema DDH é difícil em relação à $\mathcal{G}$ se para todos os algoritmos probabilísticos polinomiais $\mathcal{A}$ existe uma função negligenciável negl tal que

$$\Pr\left[\mathrm{DDH}_{\mathcal{A},\mathcal{G}}(n) = 1\right] \leq \frac{1}{2} + \mathrm{negl}(n)$$

- Equivalentemente (definição do livro): para todo $\mathcal{A}$ eficiente existe uma função negligenciável negl tal que

$$\left|\Pr[\mathcal{A}(\mathbb{G}, q, g, g^x, g^y, g^z) = 1] - \Pr[\mathcal{A}(\mathbb{G}, q, g, g^x, g^y, g^{xy}) = 1]\right| \leq \mathrm{negl}(n)$$

Dificuldade na prática

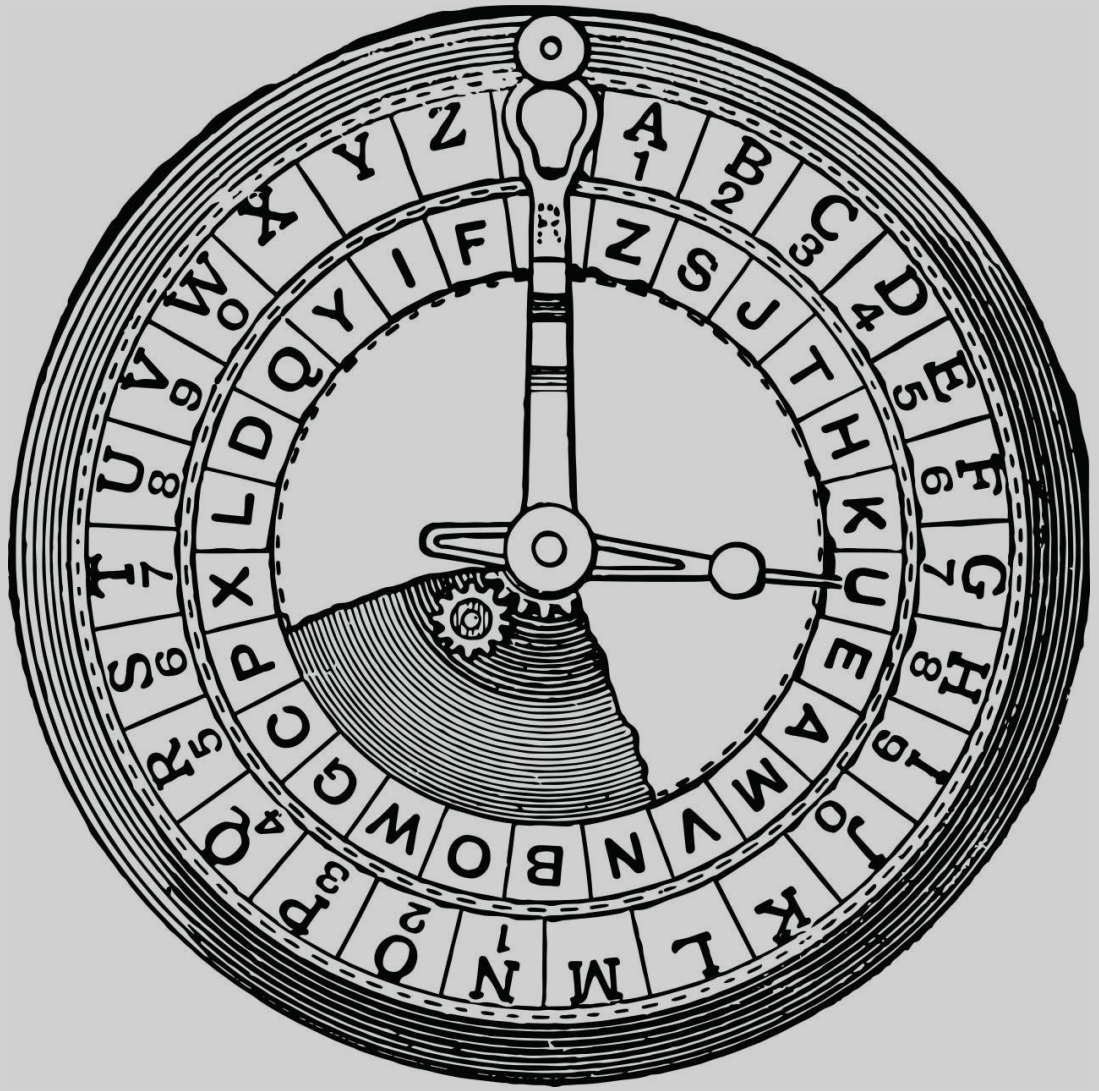
- Fácil para $(\mathbb{Z}_p, +)$ onde p é um número primo
  - Assim como o problema do logaritmo discreto
- "Fácil" para $(\mathbb{Z}_p^*, \times)$
- Considerado difícil para

$$\mathbb{G} = \{ [h^r \bmod p] \mid h \in \mathbb{Z}_p^* \}$$

onde $p = rq + 1$ para p, q primos

- E também em curvas elípticas

Para fechar



Para fechar

- Hoje
  - Um pouco mais de teoria de grupos
  - Logaritmo discreto
  - Diffie-Hellman (decisão e busca)
- Próxima aula
  - Mantendo e distribuindo chaves privadas
  - O protocolo de Diffie-Hellman