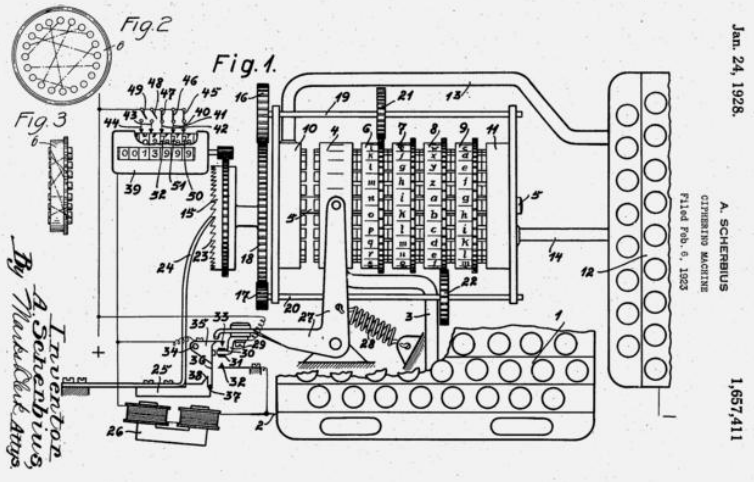
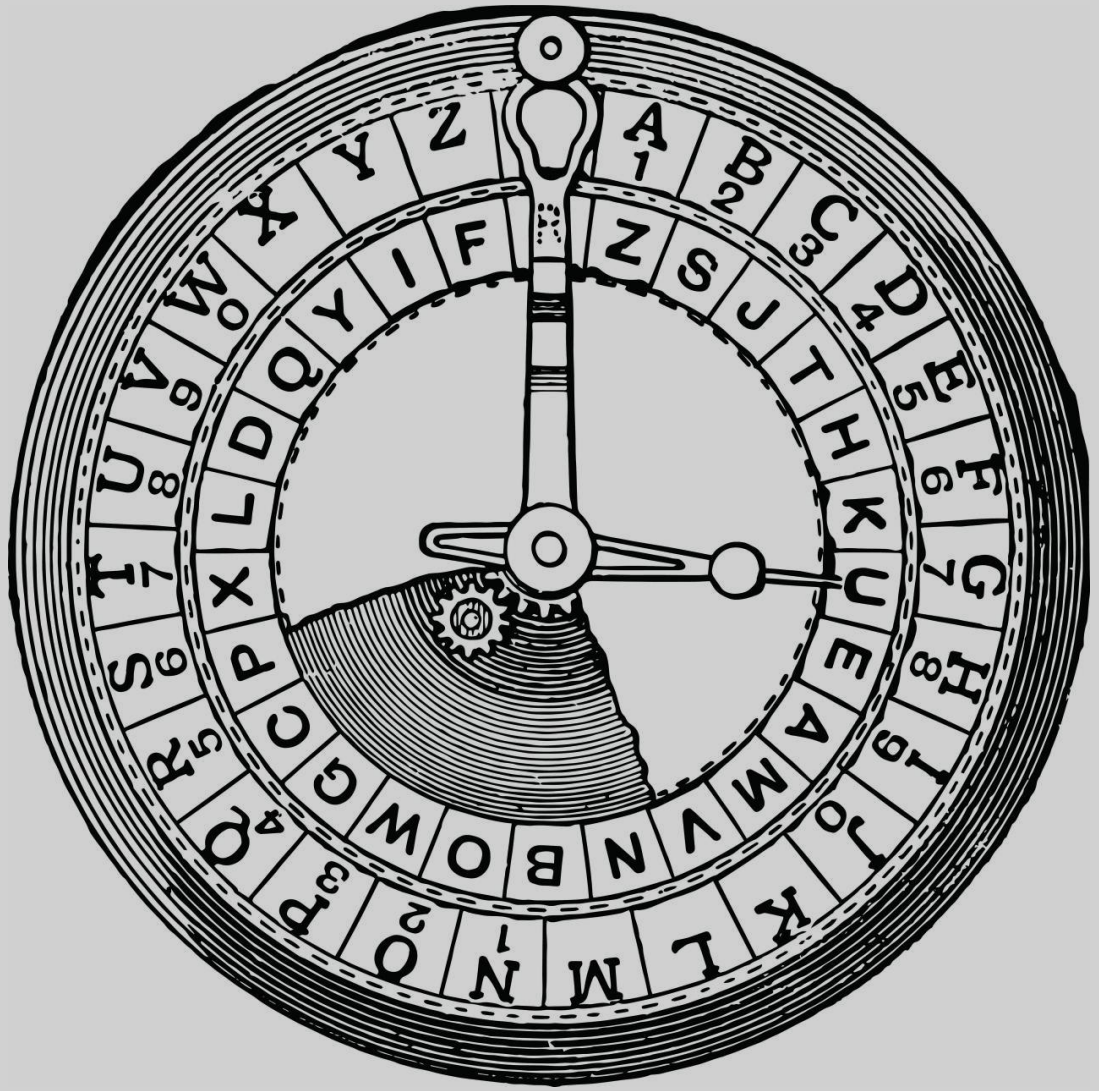
Cifra El Gamal

Fundamentos da Criptografia

Nicollas Mocelin Sdroievski



Nas últimas aulas

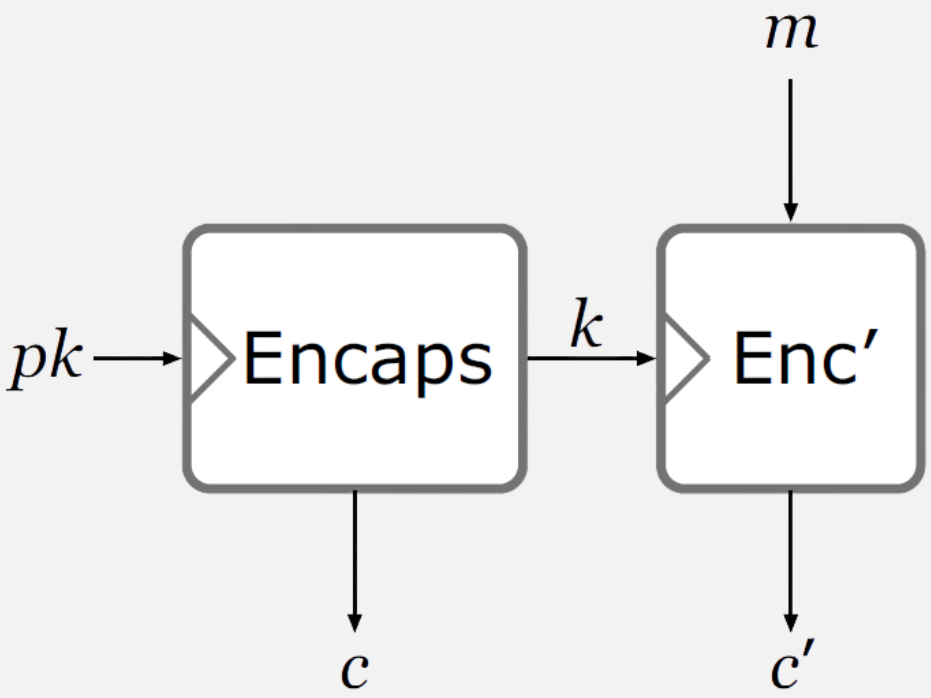


KEM (*Key Encapsulation Mechanism*)

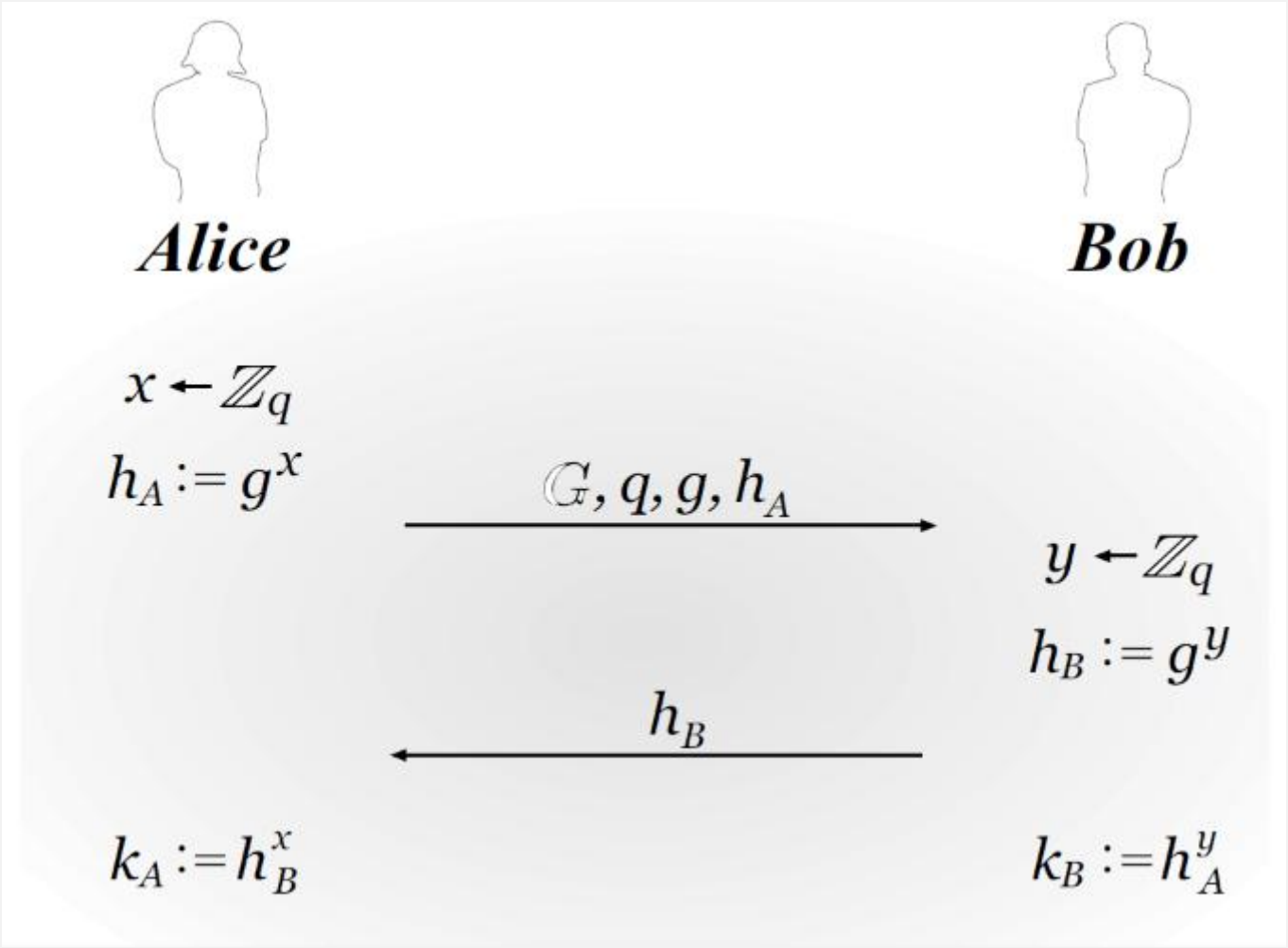
- Para compartilhar a chave em uma cifra híbrida, dois passos
  - Sortear uma chave uniforme k
  - Cifrar k com uma cifra de chave pública
- Um KEM faz os dois “ao mesmo tempo”
- Vantajoso de duas maneiras
  - Conceitual
  - Eficiência (hoje veremos um exemplo!)
- Três algoritmos
  - Geração de chaves
  - Encapsulamento (produz a chave simétrica e um texto cifrado)
  - Desencapsulamento (recupera a chave do texto cifrado)

KEM/DEM para criptografia simétrica

- Um KEM pode ser usado em criptografia híbrida como ao lado
- A cifra de chave privada utilizada é chamada de DEM (*Data Encapsulation Mechanism*)
- Daí o nome KEM/DEM



Troca de chaves de Diffie-Hellman



Dificuldade do DDH

Desafiante

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



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

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

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

$(\mathbb{G}, q, g, g^x, g^y, \hat{h})$

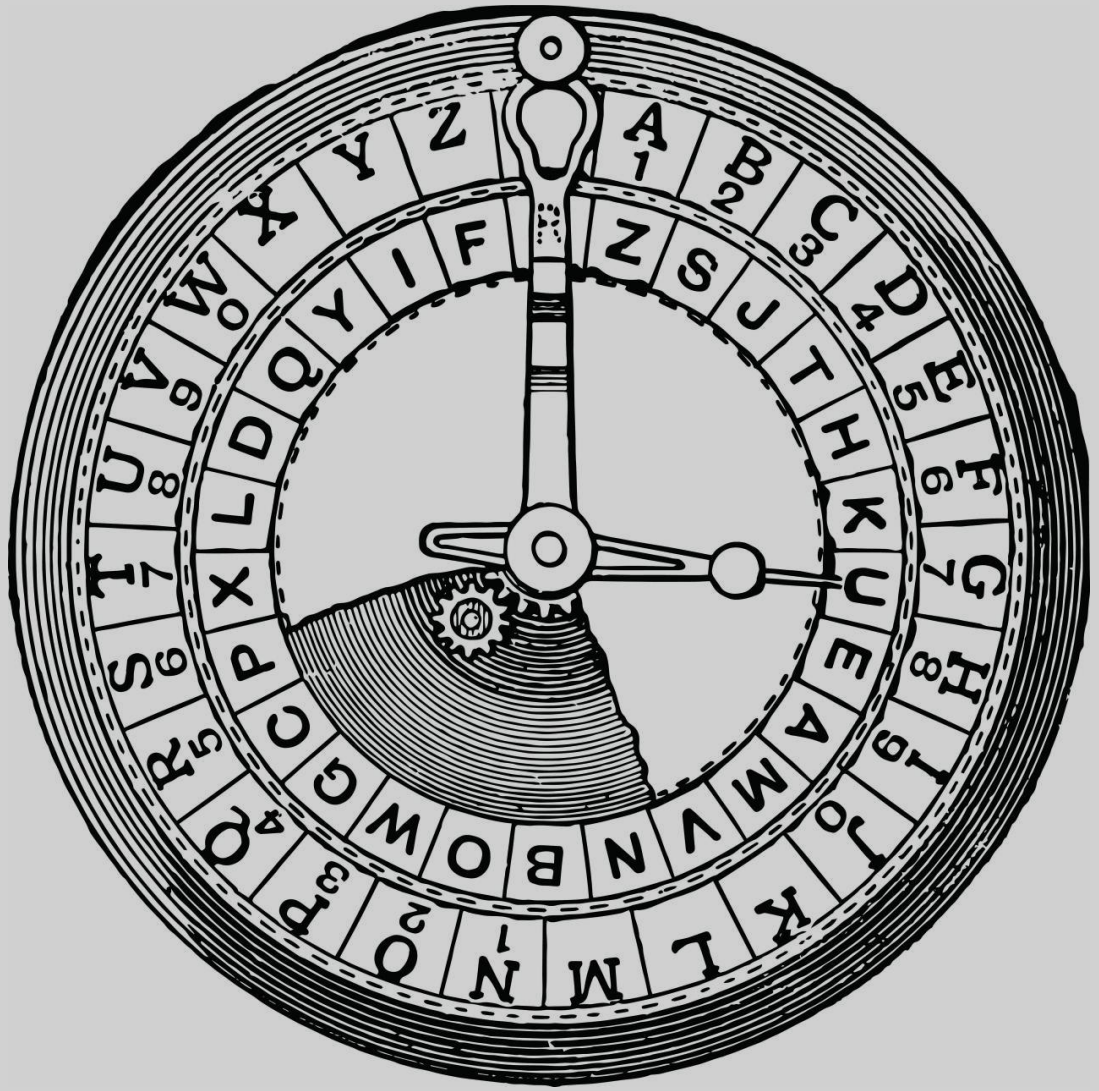
b' = chute para b



- Se $b = 0, \hat{h} = g^z$
  - $\hat{h}$ é aleatório, sem relação com g^x e g^y
- Se $b = 1, \hat{h} = g^{xy}$
- O problema é difícil quando, para todo $\mathcal{A}$ eficiente existe negl tal que

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

Cifra El Gamal



Ideia

- Essencialmente, uma mudança de perspectiva no protocolo de troca de chaves
- Imagine que Alice e Bob compartilharam uma chave k
  - Como k parece aleatória para qualquer adversário “bisbilhoteiro”, Bob poderia enviar uma mensagem cifrada como $k \cdot m$
    - $k \cdot m$ continua parecendo aleatória, como no one-time pad
- A primeira mensagem de Alice será sua chave pública
- E a resposta de Bob, tanto a parte para construir k como $k \cdot m$, será o texto cifrado

Um lema simples

- **Lema 11.15.** Seja $\mathbb{G}$ um grupo finito e $m \in \mathbb{G}$. Escolher um elemento aleatório e uniforme $k \leftarrow \mathbb{G}$ e fazer $k' := k \cdot m$ resulta na mesma distribuição que escolher $k' \leftarrow \mathbb{G}$ aleatoriamente. Em outras palavras, para qualquer $\hat{g} \in \mathbb{G}$:

$$\Pr[k \cdot m = \hat{g}] = \frac{1}{|\mathbb{G}|},$$

onde a probabilidade é sobre uma escolha aleatória de $k \leftarrow \mathbb{G}$

- **Demonstração:** Seja $\hat{g} \in \mathbb{G}$ um elemento arbitrário, então

$$\Pr[k \cdot m = \hat{g}] = \Pr[k = \hat{g} \cdot m^{-1}]$$

- Como k é uniforme, essa probabilidade é exatamente $1/|\mathbb{G}|$

Uma cifra perfeitamente secreta

- A chave secreta é um elemento $k \in \mathbb{G}$
- Para cifrar $m \in \mathbb{G}$
  - $c \coloneqq k \cdot g$
- Para decifrar c
  - $g = k^{-1}c$
- Na verdade, o one-time pad é esse exato esquema, com o grupo das strings binárias e a operação XOR
- Para a cifra de El Gamal, usamos essa ideia para obter um elemento k que "parece aleatório", e então construímos o texto cifrado
  - $\langle c_1, c_2 \rangle = \langle k, k \cdot m \rangle$

A cifra de El-Gamal

- **Construção 11.16.** Seja $\mathcal{G}$ como antes, defina uma cifra de chave pública como a seguir
  - Gen: na entrada 1^n, execute $\mathcal{G}(1^n)$ para obter $(\mathbb{G}, q, g)$. Então, escolha um elemento uniforme $x \leftarrow \mathbb{Z}_q$ e compute $h := g^x$. A chave pública é $\langle \mathbb{G}, q, g, h \rangle$, a chave privada é $\langle \mathbb{G}, q, g, x \rangle$. O espaço de mensagens é $\mathbb{G}$.

  - Enc: ao receber como entrada a chave pública $pk = \langle \mathbb{G}, q, g, h \rangle$ e uma mensagem $m \in \mathbb{G}$, escolha um elemento uniforme $y \leftarrow \mathbb{Z}_q$ e retorne o texto cifrado

$$\langle g^y, h^y \cdot m \rangle = \langle g^y, g^{xy} \cdot m \rangle$$

  - Dec: ao receber como entrada uma chave privada $sk = \langle \mathbb{G}, q, g, x \rangle$ e um texto cifrado $\langle c_1, c_2 \rangle$, retorne

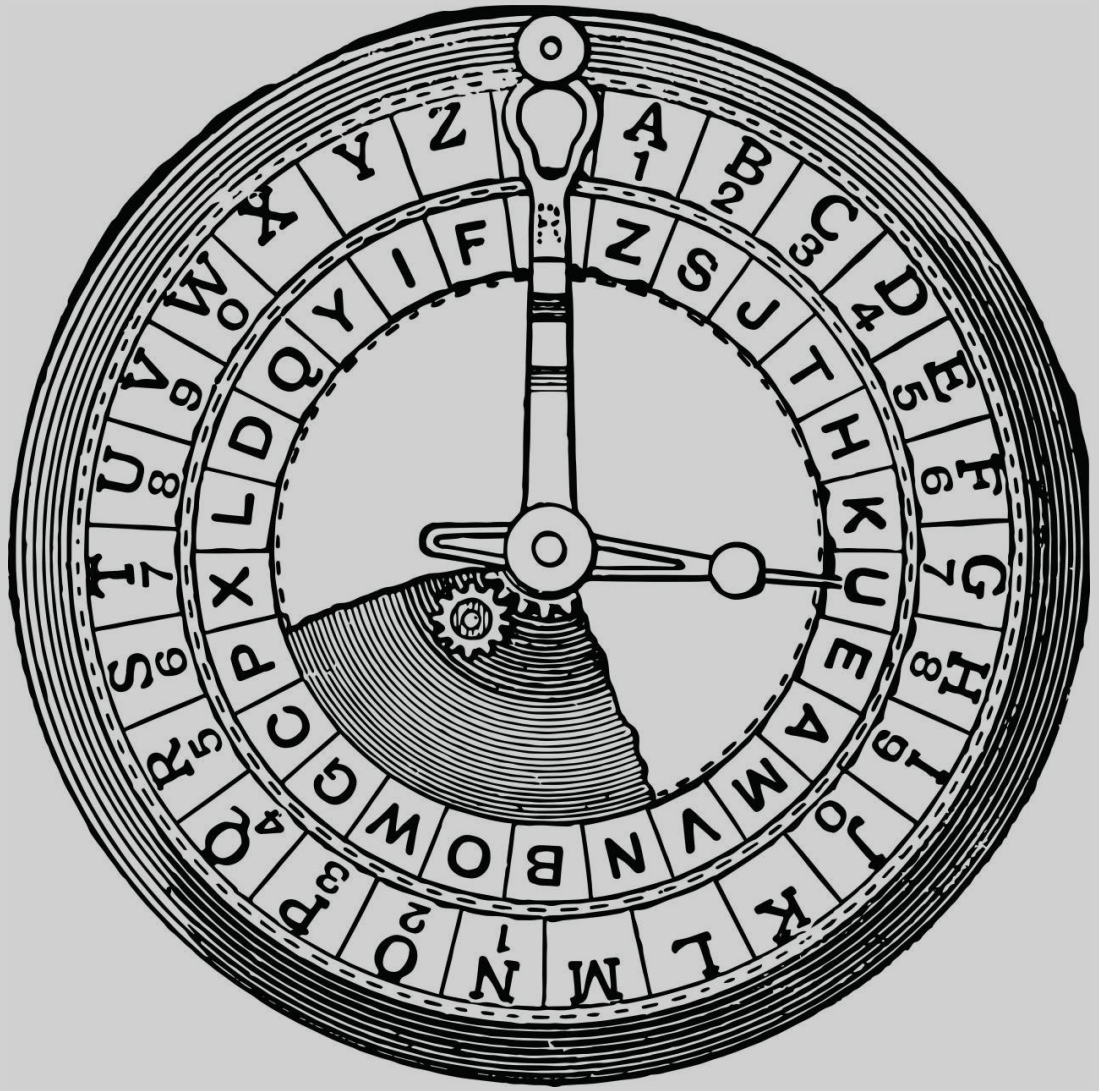
$$\hat{m} := c_2 / c_1^x = c_2 \cdot c_1^{-x}$$

Corretude

- Vamos verificar que decifrar um texto cifrado resulta na mensagem original
- Seja $\langle c_1, c_2 \rangle = \langle g^y, h^y \cdot m \rangle$ com $h = g^x$, então

$$\widehat{m} = \frac{c_2}{c_1^x} = \frac{h^y \cdot m}{(g^y)^x} = \frac{(g^x)^y \cdot m}{g^{xy}} = \frac{g^{xy} \cdot m}{g^{xy}} = m$$

Segurança



Segurança

- **Teorema 11.18.** Se o problema DDH é difícil em relação à $\mathcal{G}$, então a cifra de El Gamal é CPA-segura.
- **Demonstração:** Seja Π a cifra de El Gamal. Vamos provar que Π é EAV-segura, o que basta pela Proposição 11.3.
- Seja $\mathcal{A}$ um adversário probabilístico polinomial.
  - Vamos mostrar que existe uma função negligenciável negl tal que

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

  - Através de uma redução para o problema DDH

Lembrando, dificuldade do DDH

Desafiante

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



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

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

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

$(\mathbb{G}, q, g, g^x, g^y, \hat{h})$

b' = chute para b



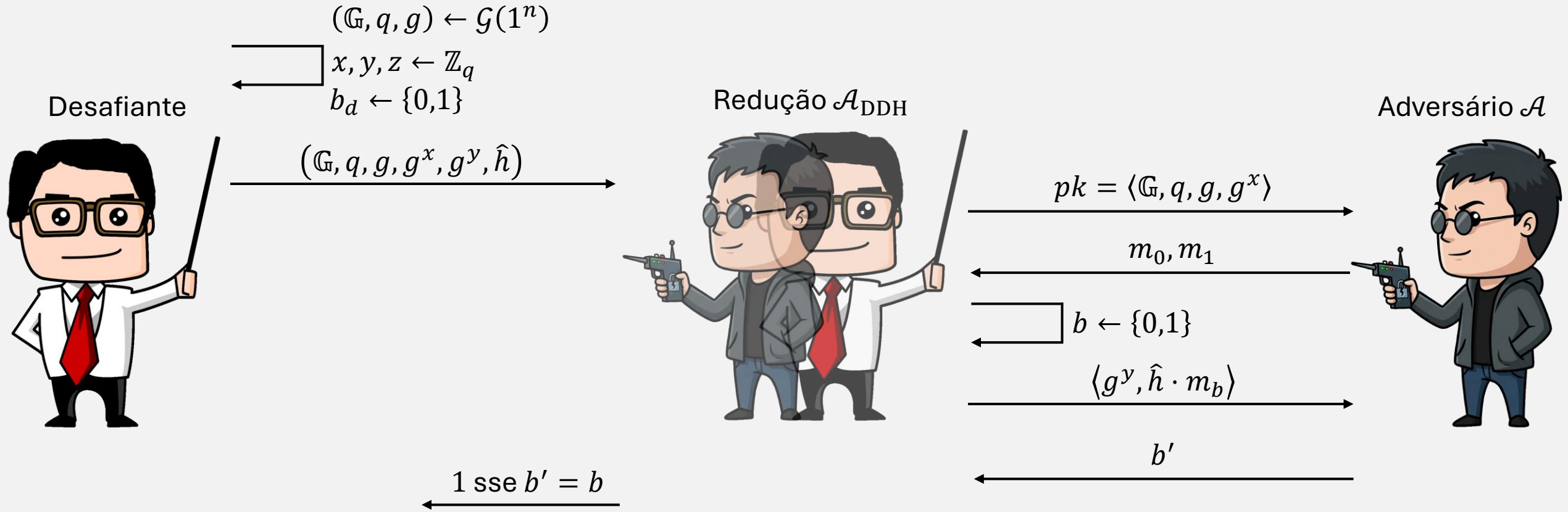
- Se $b = 0, \hat{h} = g^z$
  - $\hat{h}$ é aleatório, sem relação com g^x e g^y
- Se $b = 1, \hat{h} = g^{xy}$
- O problema é difícil quando, para todo $\mathcal{A}$ eficiente existe negl tal que

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

Um experimento “híbrido”

- Considere a “cifra” $\widetilde{\Pi}$ onde Gen é igual, porém o processo de cifragem é “mais aleatório”
  - Para cifrar m com $pk = \langle \mathbb{G}, q, g, h \rangle$, a cifra escolhe $y, z \leftarrow \mathbb{Z}_q$ uniformes e produz o texto cifrado
    $$\langle g^y, g^z \cdot m \rangle$$
  - Perceba que
    - $\widetilde{\Pi}$ não é uma cifra válida (é impossível decifrar)
      - Mas não tem problema!
    - Tanto g^y quanto $g^z \cdot m$ (pelo Lema 11.15) são uniformes e independentes de m
  - Segue que
    $$\Pr\left[\mathrm{PubK}^{\mathrm{eav}}_{\mathcal{A},\widetilde{\Pi}}(n) = 1\right] = \frac{1}{2}$$

Redução



- Lembrando, $\hat{h} = g^z$ se $b_d = 0$ e $\hat{h} = g^{xy}$ se $b_d = 1$
- Se o adversário $\mathcal{A}$ ganha, a redução imagina que $\hat{h}$ não é aleatória!

Análise

- $\mathcal{A}$ sempre recebe $pk = \langle \mathbb{G}, q, g, g^x \rangle$
- Para o texto cifrado de desafio, dois casos

1. $b_d = 0$ e $\hat{h} = g^z$ (independente de g^x e g^y)
   - O texto cifrado é $\langle g^y, g^z \cdot m_b \rangle$
   - A visão de $\mathcal{A}$ é idêntica à sua visão no experimento $\mathrm{PubK}^{\mathrm{eav}}_{\mathcal{A},\tilde{\Pi}}(n)$
   - Neste caso, $\mathcal{A}_{\mathrm{DDH}}$ vence com probabilidade exatamente $1/2$

2. $b_d = 1$ e $\hat{h} = g^{xy}$
   - O texto cifrado é $\langle g^y, g^{xy} \cdot m_b \rangle$
   - A visão de $\mathcal{A}$ é idêntica à sua visão no experimento $\mathrm{PubK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n)$
   - Neste caso, $\mathcal{A}_{\mathrm{DDH}}$ vence no experimento com probabilidade

$$\Pr\left[\mathrm{PubK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n) = 1\right]$$

Finalizando a análise

- A probabilidade de $\mathcal{A}_{\mathrm{DDH}}$ vencer é exatamente

$$\frac{1}{2}\cdot\frac{1}{2}+\frac{1}{2}\cdot\Pr\left[\mathrm{PubK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n)=1\right]=\frac{1}{4}+\frac{1}{2}\cdot\Pr\left[\mathrm{PubK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n)=1\right]$$

- Porque o problema DDH é difícil para $\mathcal{G}$, existe uma função negligenciável negl tal que

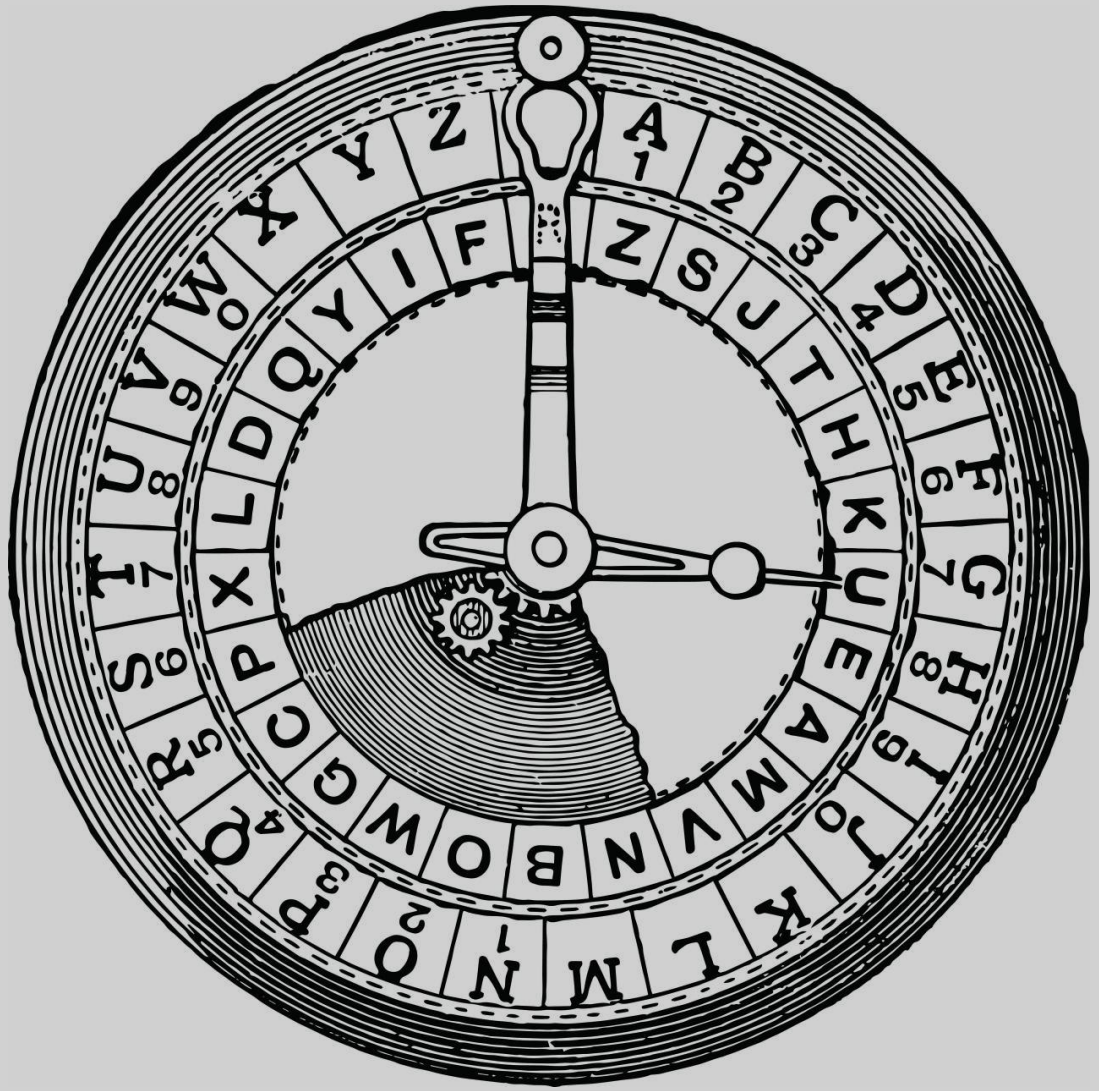
$$\frac{1}{4}+\frac{1}{2}\cdot\Pr\left[\mathrm{PubK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n)=1\right]\leq\frac{1}{2}+\mathrm{negl}(n)$$

- Reorganizando, temos que

$$\Pr\left[\mathrm{PubK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n)=1\right]\leq\frac{1}{2}+2\cdot\mathrm{negl}(n)$$

- Que basta pois $2\cdot\mathrm{negl}(n)$ é negligenciável também

Um KEM



Um KEM baseado no problema DDH

- Poderíamos usar a cifra de El Gamal para construir um KEM
  - Sorteia a chave k
  - Cifra k com a chave pública
  - E a mensagem com k
- Porém, considere o texto cifrado para k
  - $\langle g^y, g^{xy} \cdot k \rangle$
  - Se fizemos $(g^y)^x = (g^x)^y$, obtemos um elemento aleatório do grupo, então podemos usar só essa “primeira metade” do texto cifrado

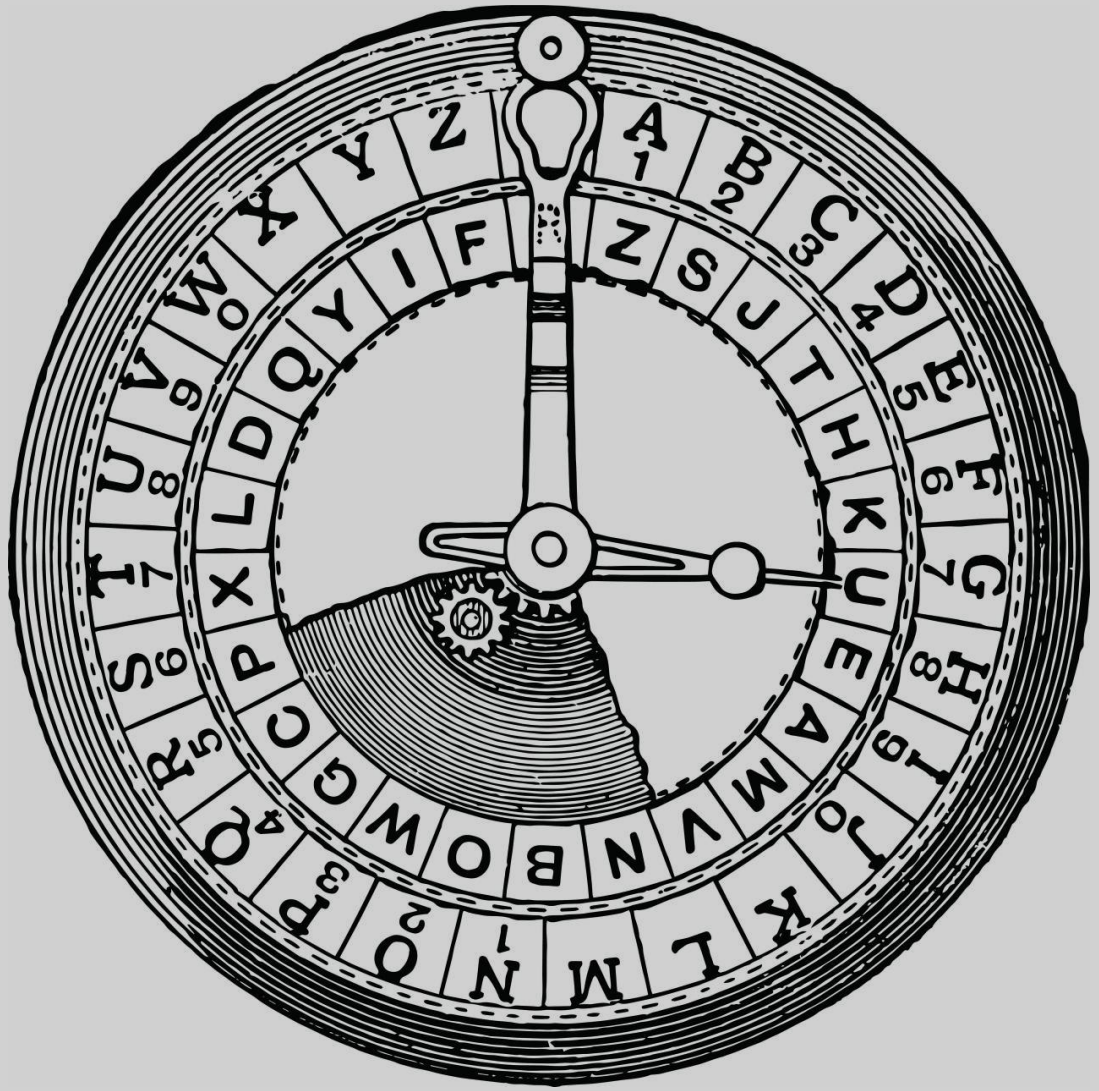
Construção 11.19

- Seja $\mathcal{G}$ como antes. Defina um KEM a seguir:
  - Gen: na entrada 1^n, execute $\mathcal{G}(1^n)$ para obter $(\mathbb{G}, q, g)$, escolha $x \leftarrow \mathbb{Z}_q$ e faça $h := g^x$. Defina também uma função $H : \mathbb{G} \to \{0,1\}^{\ell(n)}$ para alguma função ℓ. A chave pública é $\langle \mathbb{G}, q, g, h, H \rangle$ e a chave privada é $\langle \mathbb{G}, q, g, x \rangle$
  - Encaps: ao receber como entrada $pk = \langle \mathbb{G}, q, g, h, H \rangle$, escolha um elemento $y \leftarrow \mathbb{Z}_q$ e retorna o texto cifrado g^y e a chave $H(h^y)$
  - Decaps: ao receber como entrada $sk = \langle \mathbb{G}, q, g, x \rangle$ e um texto cifrado $c \in \mathbb{G}$, retorne a chave $H(c^x)$
- Na construção, H é um algoritmo de derivação de chaves
  - Uma função “bem distribuída”
  - Ou uma função hash criptográfica (com chave)
  - Ou um extrator de aleatoriedade

Segurança

- **Teorema 11.20.** Se o problema DDH é difícil em relação à $\mathcal{G}$, e H é escolhida corretamente, então a construção 11.19 é um KEM CPA-seguro.
- A demonstração é muito parecida com a demonstração da segurança do esquema de troca de chaves de Diffie-Hellman
- Se modelarmos H como um oráculo aleatório, então é possível provar que a construção é segura a partir da versão de busca/computacional do problema de Diffie-Hellman

Para fechar



Para fechar

- Hoje
  - Cifra El Gamal
    - Baseada no problema DDH
    - Possível construir um KEM também
      - Um pouco mais simples/eficiente
- Próxima aula
  - Cifra RSA
    - Baseada em um problema “parecido” com fatoração