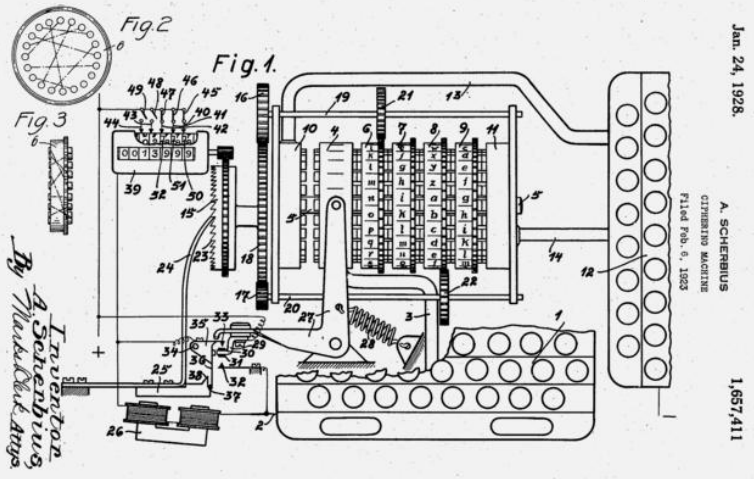
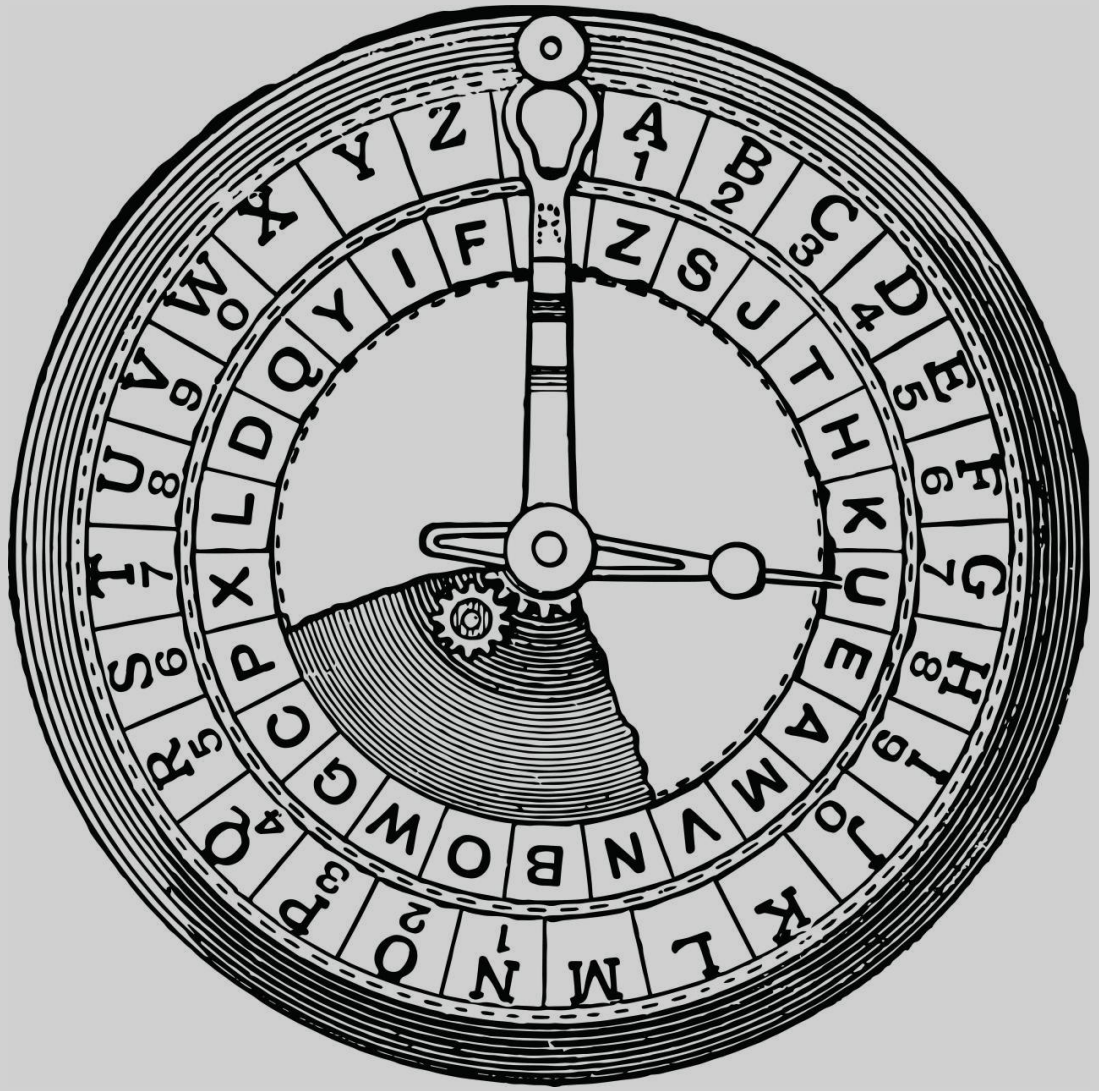
Criptografia de Chave Pública

Fundamentos da Criptografia

Nicollas Mocelin Sdroievski



Nas últimas aulas

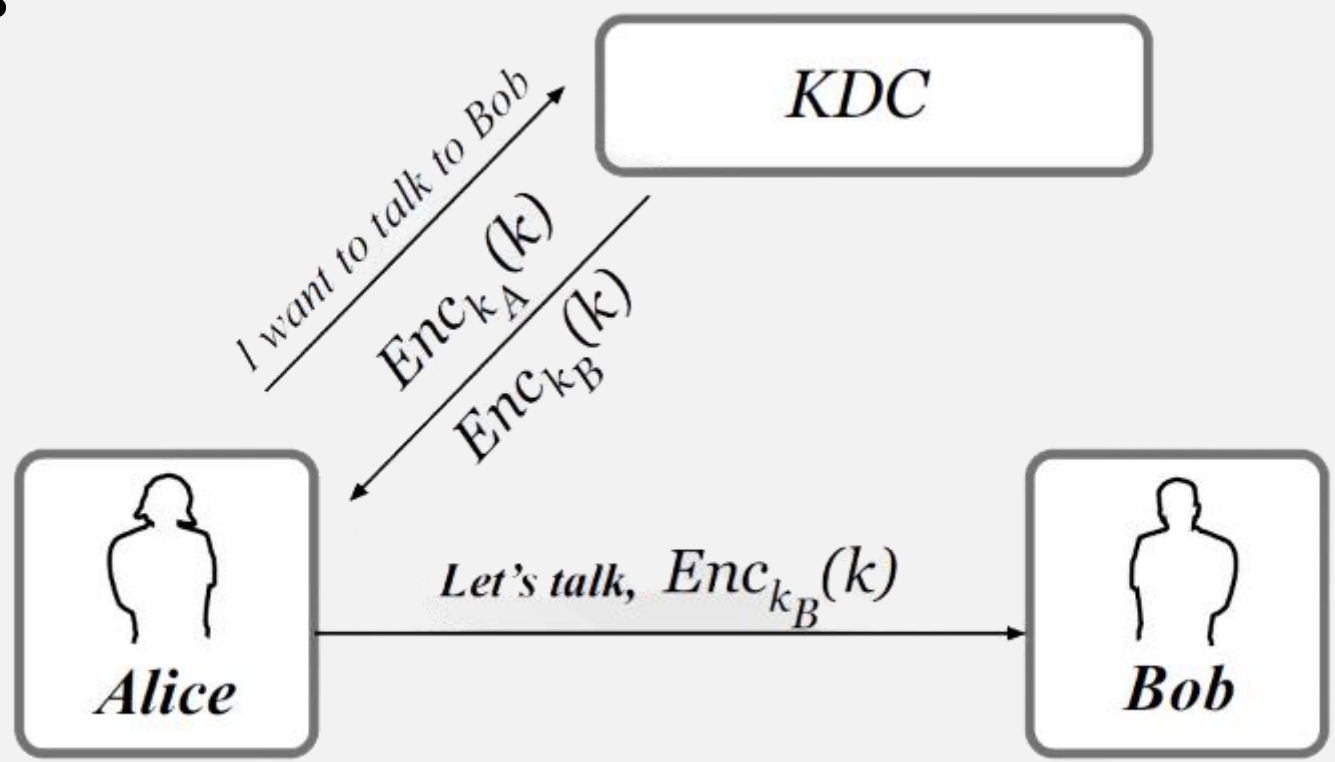


Construções de chave privada

- A maioria das construções que vimos até então são de chave privada
  - Cifras
  - MACs
- Na aula passada: focamos em um problema que essencialmente ignoramos até aqui
  - Como as partes honestas podem compartilhar uma chave secreta de maneira segura?
  - Certamente não podem apenas enviar a chave pelo canal público...

Esquema visual de um KDC

- KDC compartilha chaves
  - k_A com Alice
  - k_B com Bob



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

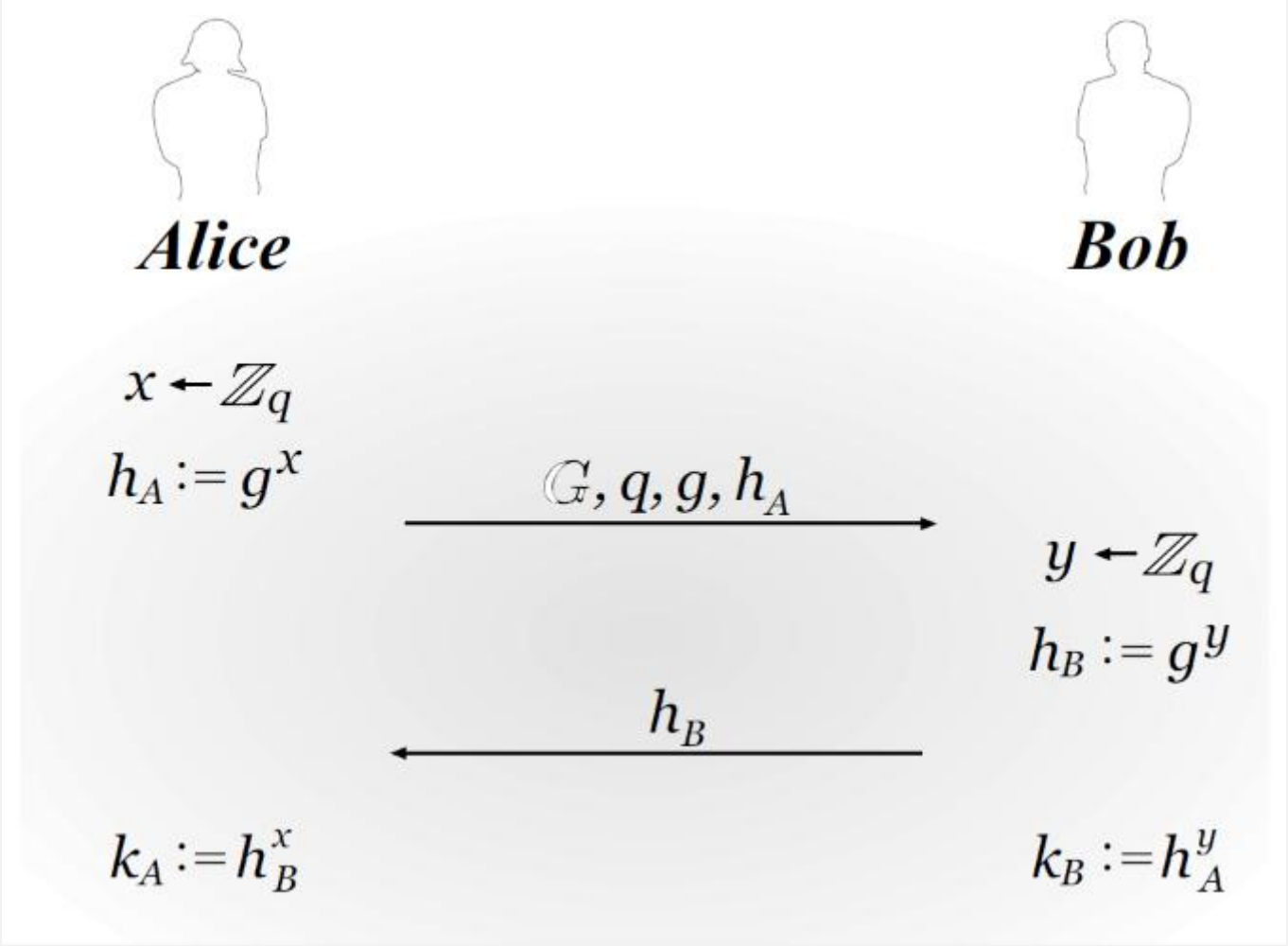
b' = chute para b

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

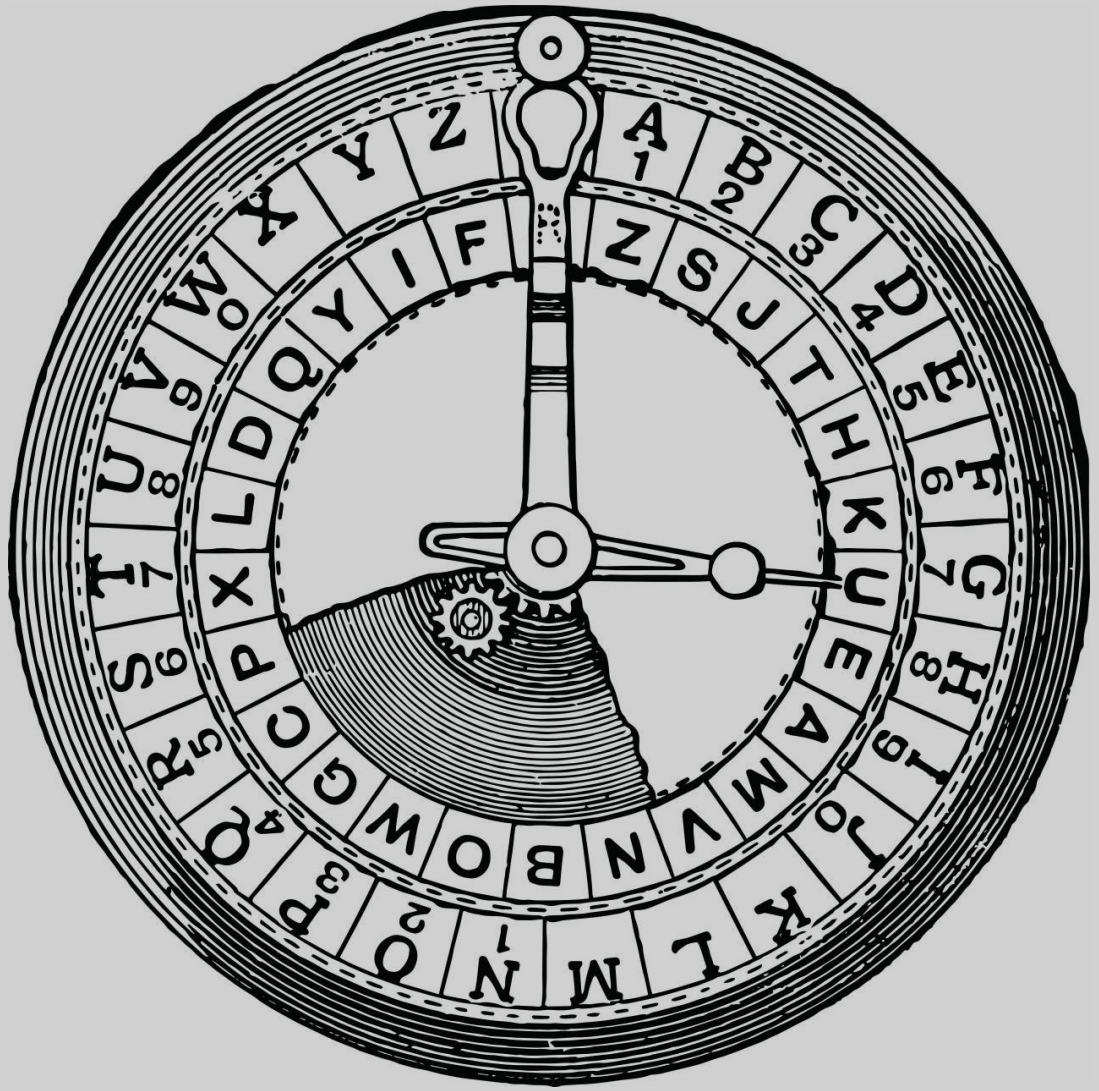
Esquema visual da troca de chaves DH



Corretude e segurança

- Alice e Bob computam a mesma chave
  - $k_B = h_A^y = (g^x)^y = g^{xy}$
  - $k_A = h_B^x = (g^y)^x = g^{xy}$
- Segurança segue quase que imediatamente da dificuldade da versão de decisão do problema de Diffie-Hellman
  - O adversário enxerga
    $$(\mathbb{G}, q, g, h_A, h_B, \hat{h})$$
  - Onde $h_A = g^x$ e $h_B = g^y$
  - Por fim, $\hat{h}$ é ou g^{xy} ou um elemento uniforme do grupo
    - Exatamente como no experimento $\mathrm{DDH}_{\mathcal{A},\mathcal{G}}(n)$

Introdução



Ideia geral

- Permite comunicação secreta sem compartilhar nenhum segredo anteriormente
- Criptografia de chave secreta é simétrica
  - Ambas as partes precisam conhecer a chave secreta k
- Criptografia de chave pública é assimétrica
  - Cada parte possui
    - Uma chave pública pk (de *public key*)
    - E uma chave privada sk (de *secret key*)
  - No geral, a chave pública é utilizada para cifrar as mensagens
  - E a chave privada para decifrar

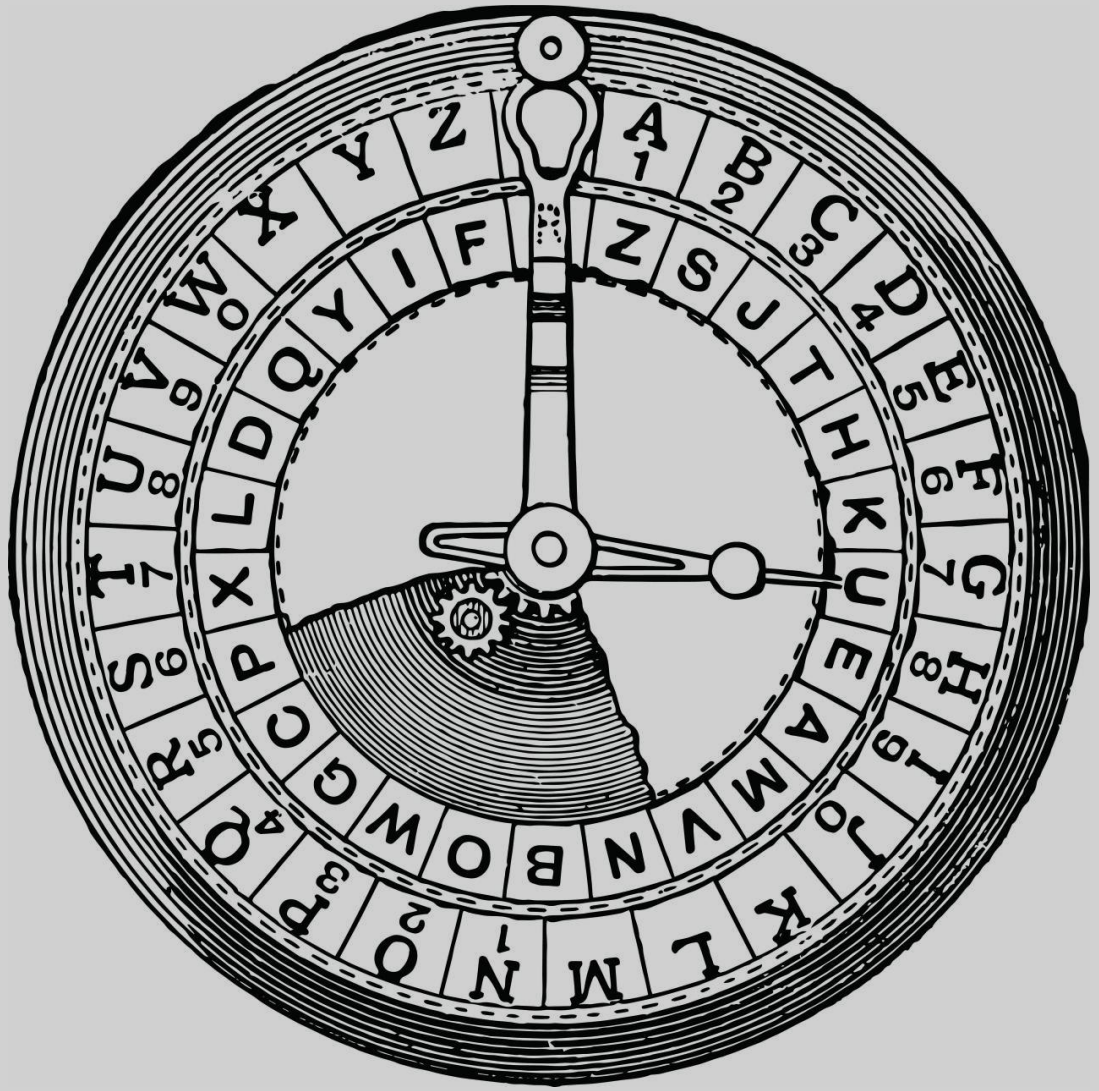
Chaves públicas

- Como um remetente Alice descobre a chave pública de um destinatário Bob?
- Duas maneiras (abstratas)
  - Alice descobre que Bob quer entrar em contato e envia pk para Bob, sem nenhuma criptografia
  - Alice já deixa sua chave visível em algum tipo de repositório publicamente acessível
- Assumem que o canal de comunicação é autenticado
  - Ninguém pode interceptar e modificar a chave no meio do caminho
  - Mais pra frente, veremos como lidar com essa situação também

Mais diferenças (cripto simétrica/assimétrica)

- Assimetria indica que remetente e destinatário não podem ser trocados
  - Um sabe pk e o outro sk
- Permite que múltiplos remetentes entrem em contato com o mesmo destinatário
  - De maneira secreta, com apenas a chave pública do destinatário
  - Mais fácil manter apenas uma chave privada (e conferir as chaves públicas dos outros quando necessário)
- Desvantagens principais
  - 2 a 3 ordens de magnitude mais lentas que cifras de chave privada
  - Mais difícil, em alguns casos, estabelecer a segurança necessária
    - Principalmente se queremos manter a eficiência

Definições e segurança



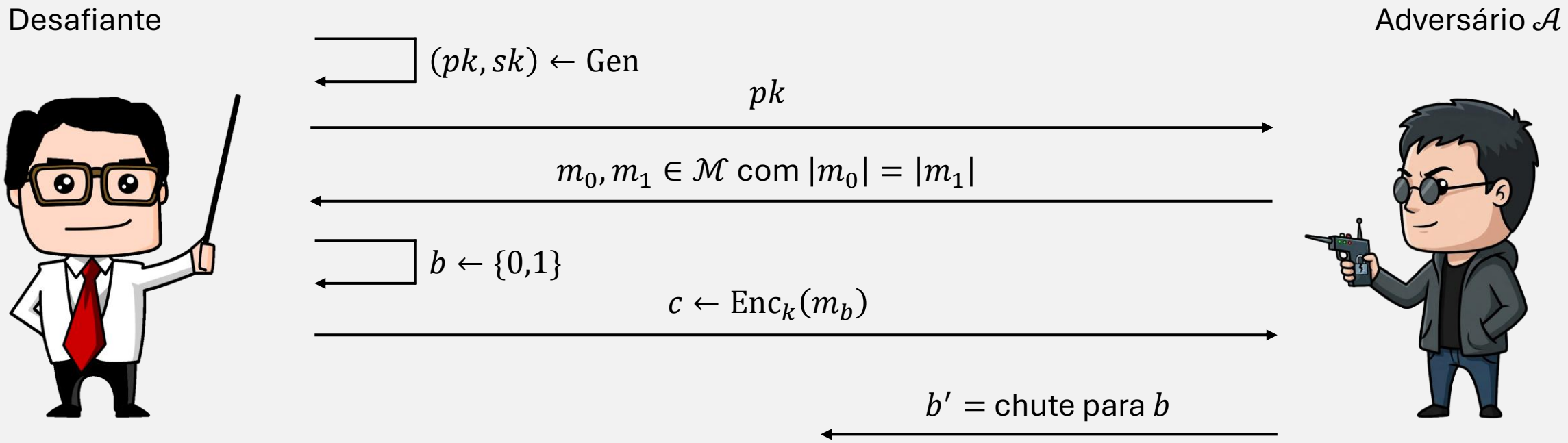
Definição 11.1

- Uma cifra de chave pública é uma tripla de algoritmos probabilísticos polinomiais $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ tal que:
  - Gen recebe um parâmetro de segurança 1^n e produz um par de chaves (pk, sk)
    - $pk =$ chave pública
    - $sk =$ chave privada
    - Assumimos que cada chave tem tamanho pelo menos n, e que n pode ser determinado a partir das chaves
  - Enc recebe uma chave pública pk e uma mensagem m, e produz um texto cifrado c
    - $c \leftarrow \mathrm{Enc}_{pk}(m)$ (no geral, Enc será probabilística)
  - Dec é um algoritmo determinístico que recebe uma chave privada sk e um texto cifrado c, e produz uma mensagem m ou um símbolo especial $\perp$, denotando que houve uma falha
    - $m := \mathrm{Dec}_{sk}(c)$

Alguns comentários

- Duas chaves (pk, sk) ao invés de uma
- É permitido que o algoritmo de decifragem falhe com probabilidade negligenciável
  - Mesmo para textos cifrados válidos
  - Exemplo: precisamos encontrar um número primo em um intervalo
  - No geral, vamos desconsiderar esse problema
- Na prática, queremos que o espaço de mensagens seja $\{0,1\}^n$ ou $\{0,1\}^*$
  - Comum que os esquemas usem números, elementos de grupo, etc. como mensagens
  - Nestes casos, existe um mapeamento eficiente entre os elementos e strings binárias

O experimento $\mathrm{PubK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n)$



- A saída do experimento é 1 se $b' = b$ e 0 caso contrário
- Escrevemos $\mathrm{PubK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n) = 1$ se a saída do experimento é 1
  - e dizemos que $\mathcal{A}$ obtém sucesso neste caso

Segurança EAV

- **Definição 11.2.** Uma cifra de chave pública $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ possui cifragens indistinguíveis na presença de um bisbilhoteiro, ou é EAV-segura, se para todos os algoritmos probabilísticos polinomiais $\mathcal{A}$ existe uma função negligenciável negl tal que

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

Diferenças

- $\mathcal{A}$ recebe a chave pública pk
  - Faz sentido, pois a ideia é que a chave seja pública e possa ser revelada sem problemas
- Isto dá algum poder adicional ao adversário?
  - O adversário pode usar pk para computar $\mathrm{Enc}_{pk}(m)$ para a mensagem que quiser
  - Ou seja, o adversário ganha um oráculo de cifragem “de graça”!

- **Proposição 11.3.** Se uma cifra de chave pública é EAV-segura, então também é CPA-segura (definida de maneira análoga à definição 3.22).

Segredo perfeito para cifras de chave pública

- Podemos definir uma noção de segredo perfeito para cifras de chave pública
  - Para todo adversário $\mathcal{A}$

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

  - Possível ou impossível?
    - Impossível!
    - Existe um adversário que é capaz de vencer no experimento com probabilidade 1
      - Independente dos tamanhos das chaves, mensagens, etc.

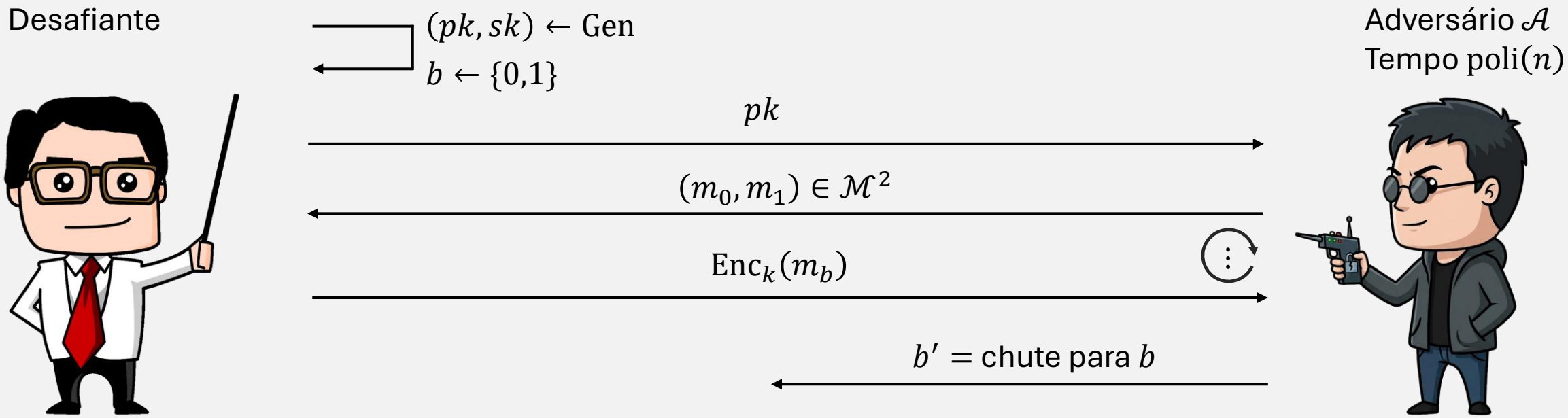
Cifras determinísticas

- **Teorema 11.4.** Nenhuma cifra de chave pública determinística pode ser CPA-segura
  - E portanto, nem EAV segura!
- Para cifras de chave pública, este é um problema ainda maior
  - Para cifras de chave privada, adversário consegue determinar se uma mensagem foi mandada duas vezes
  - Para cifras de chave pública, o adversário consegue recuperar a mensagem se existem poucas possibilidades!
    - Exemplo, notas de 0 a 100
    - Basta computar 101 textos cifrados e comparar com o observado

Segurança para múltiplas mensagens

- Definimos de maneira semelhante ao caso de cifras simétricas
  - O desafiante sorteia um bit b
  - O adversário envia pares de mensagens (m_0, m_1)
  - E (sempre) recebe a mensagem m_b cifrada
  - No fim, o adversário deve adivinhar o valor de b
- Única diferença?
  - Adversário recebe a chave privada também

O experimento $\mathrm{PubK}^{\text{LR-cpa}}_{\mathcal{A},\Pi}(n)$



- Definimos $\mathrm{PubK}^{\text{LR-cpa}}_{\mathcal{A},\Pi}(n) = 1$ se $b' = b$, caso em que $\mathcal{A}$ vence

Segurança CPA para múltiplas cifragens

- **Definição 11.5.** Uma cifra de chave pública $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ possui múltiplas cifragens indistinguíveis sob ataque de texto plano conhecido, ou é CPA-segura para múltiplas cifragens, se para todos os algoritmos probabilísticos polinomiais $\mathcal{A}$ existe uma função negligenciável negl tal que,

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

Teorema 11.6. Se uma cifra de chave pública é CPA-segura, então também é CPA-segura para múltiplas cifragens.

Mensagens de tamanho arbitrário

- **Terminologia:** segurança EAV, CPA, e CPA para múltiplas mensagens são todas equivalentes para cifras de chave pública
  - A partir de agora, falaremos apenas em cifras CPA-seguras
- Suponha que temos uma cifra de chave pública $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ que é CPA-segura para mensagens de tamanho n
- Como conseguir uma cifra para mensagens de tamanho arbitrário (por simplicidade, múltiplos de n)?
  - Seja $m = m_1 m_2 \ldots m_\ell$ onde $m_i \in \{0,1\}^n$
  - Basta fazer $\mathrm{Enc}'_{pk}(m) = \mathrm{Enc}_{pk}(m_1)\,\mathrm{Enc}_{pk}(m_2) \ldots \mathrm{Enc}_{pk}(m_\ell)$
  - E Dec' é definido de maneira similar
  - Segurança segue do Teorema 11.6
    - Prova mais direta para o caso $\ell = 2$ na lista de exercícios

Segurança CCA

- Ainda mais importante para cifras de chave pública
  - Agora, espera-se receber textos cifrados de múltiplos remetentes (qualquer um que saiba a sua chave pública)
- Imagine que $\mathcal{A}$ observa um texto cifrado c enviado de $\mathcal{S}$ para $\mathcal{R}$
- Essencialmente dois tipos de ataques no estilo CCA
  - $\mathcal{A}$ pode modificar c, obtendo c' e enviar c' no lugar de $\mathcal{S}$
    - Como em um sistema de e-mail, modificando o remetente
    - A resposta de $\mathcal{R}$ pode revelar algo sobre a mensagem original m' de c'
  - $\mathcal{A}$ pode modificar c, obtendo c' e enviar c' no seu próprio nome
    - Novamente, a reposta de $\mathcal{R}$ pode revelar informações sobre a mensagem original

Alguns cenários

1. Um usuário envia sua senha pw cifrada com um *timestamp*. O banco retorna uma de duas possibilidades
   1. Senha incorreta
   2. *Timestamp* incorreto se a senha está correta mas não o *timestamp*
   - Pode permitir ataque no estilo Padding-Oracle
2. Um usuário $\mathcal{S}$ envia um e-mail cifrado c para $\mathcal{R}$, que é observado por $\mathcal{A}$
   - $\mathcal{A}$ então envia um e-mail c' cifrado para $\mathcal{R}$
   - Se $\mathcal{R}$ responder, pode incluir uma citação para a mensagem m' correspondente a c'
     - $\mathcal{R}$ agiu como um oráculo de decifragem!

O experimento $\mathrm{PubK}^{\mathrm{cca}}_{\mathcal{A},\Pi}(n)$

Desafiante



$(pk, sk) \leftarrow \mathrm{Gen}(1^n)$

pk

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



$c' \in \mathcal{C}$

$\mathrm{Dec}_{sk}(c')$

$m_0, m_1 \in \mathcal{M}$ com $|m_0| = |m_1|$

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

$c \leftarrow \mathrm{Enc}_k(m_b)$

$c' \in \mathcal{C}$ (não vale $c = c'$)

$\mathrm{Dec}_k(c)$

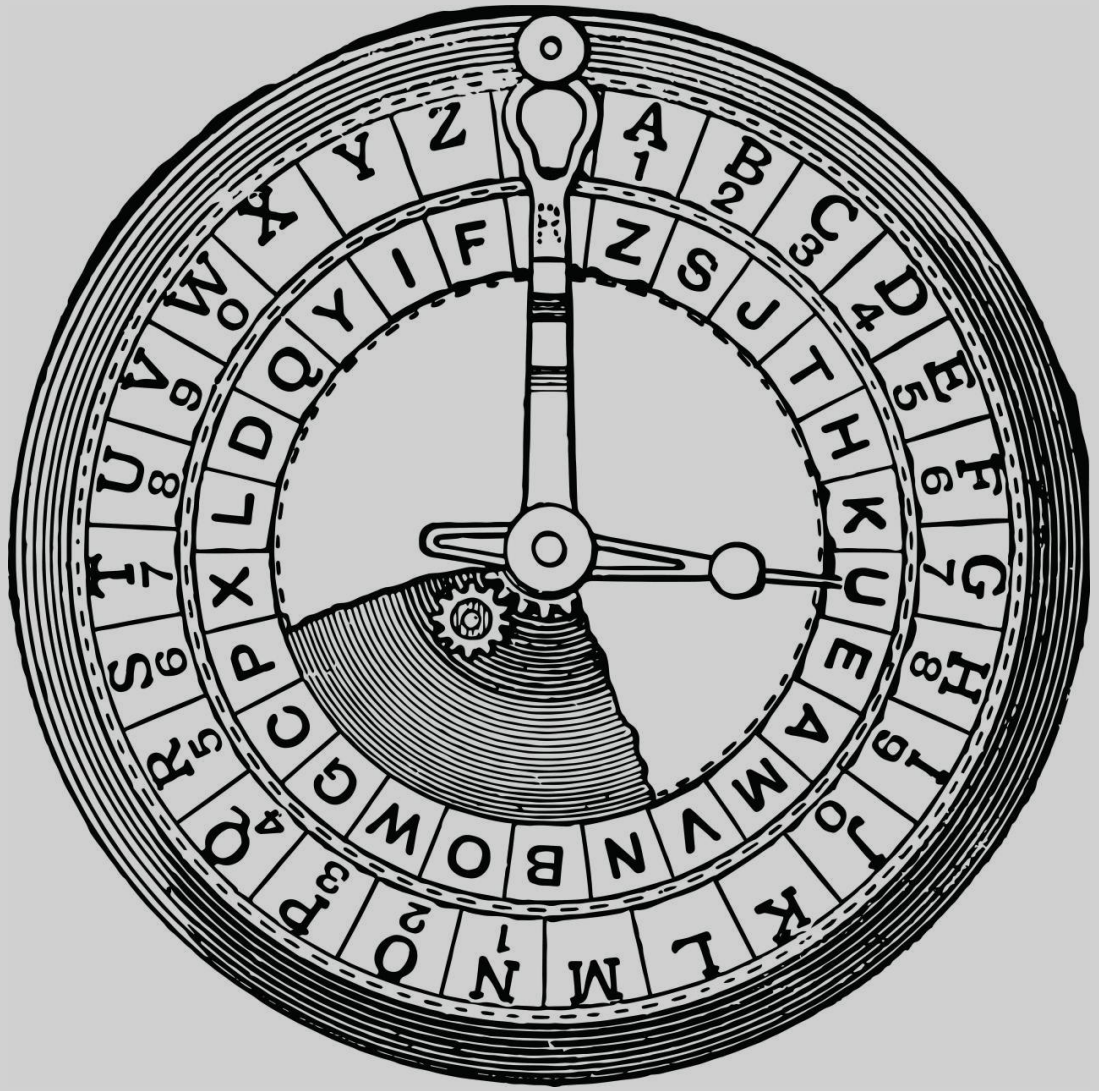
$b' =$ chute para b

Definição de segurança

- Como antes, a saída do experimento é 1 se $b' = b$ e 0 caso contrário
- Escrevemos $\mathrm{PubK}^{\mathrm{cca}}_{\mathcal{A},\Pi}(n) = 1$ se a saída do experimento é 1
- **Definição 11.8.** Uma cifra de chave pública $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ possui cifragens indistinguíveis sob ataque de texto cifrado conhecido, ou é CCA-segura, se para todos os algoritmos probabilísticos polinomiais $\mathcal{A}$ existe uma função negligenciável negl tal que,

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

Para fechar



Para fechar

- Hoje
  - Cifras de chave pública
    - Definição básica
    - Segurança EAV, CPA e CCA
- Próxima aula
  - Cifras híbridas
  - O esquema KEM/DEM