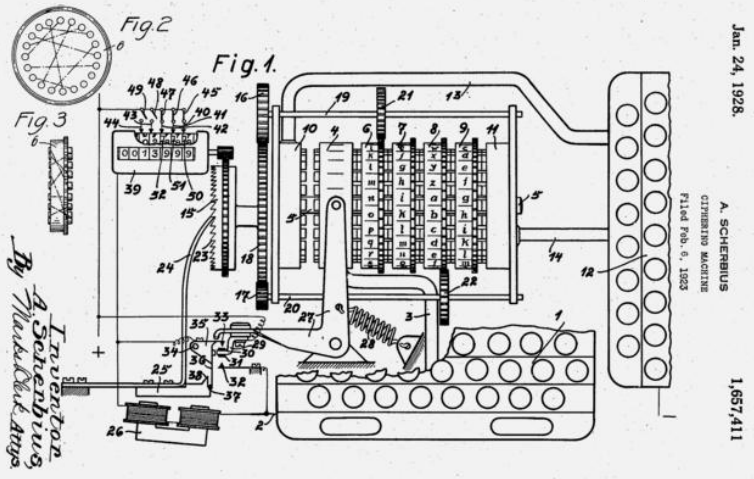
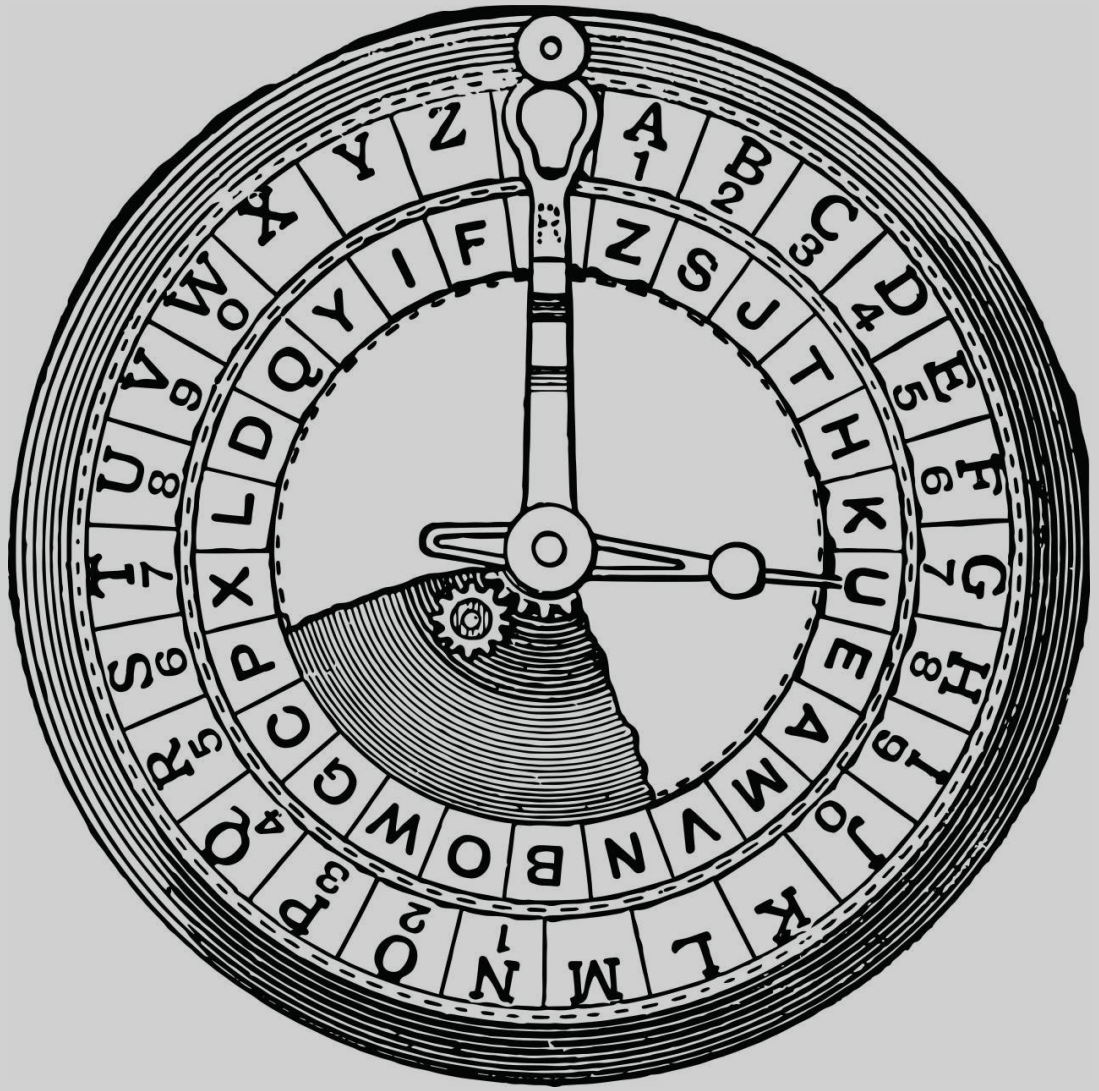
Criptografia Híbrida

Fundamentos da Criptografia

Nicollas Mocelin Sdroievski



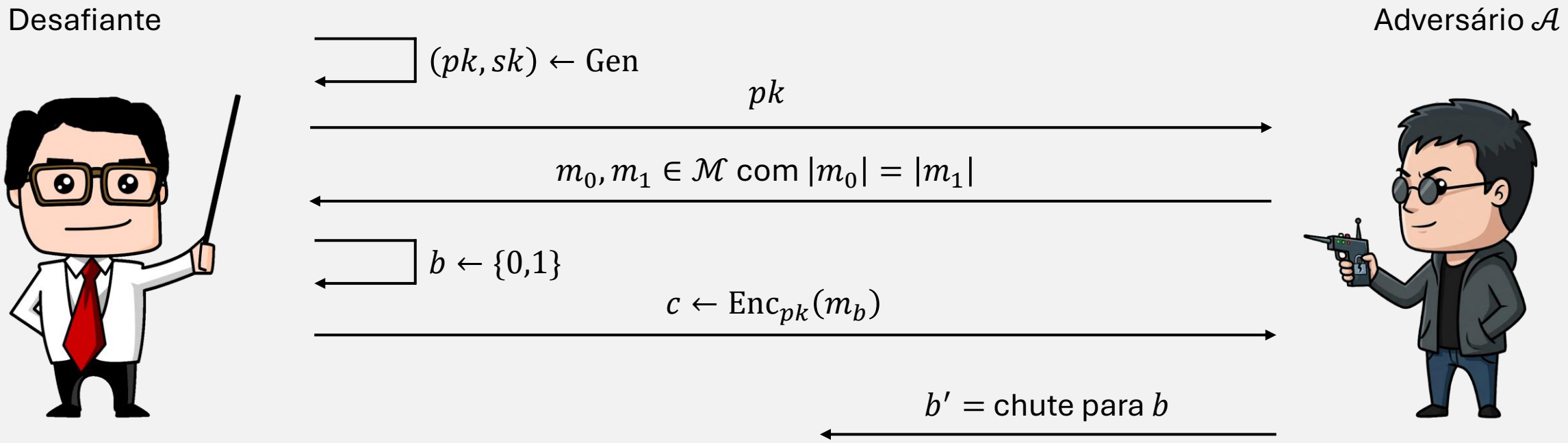
Nas últimas aulas



Criptografia de chave pública

- 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*)
  - A chave pública é utilizada para cifrar as mensagens
  - E a chave privada para decifrar

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

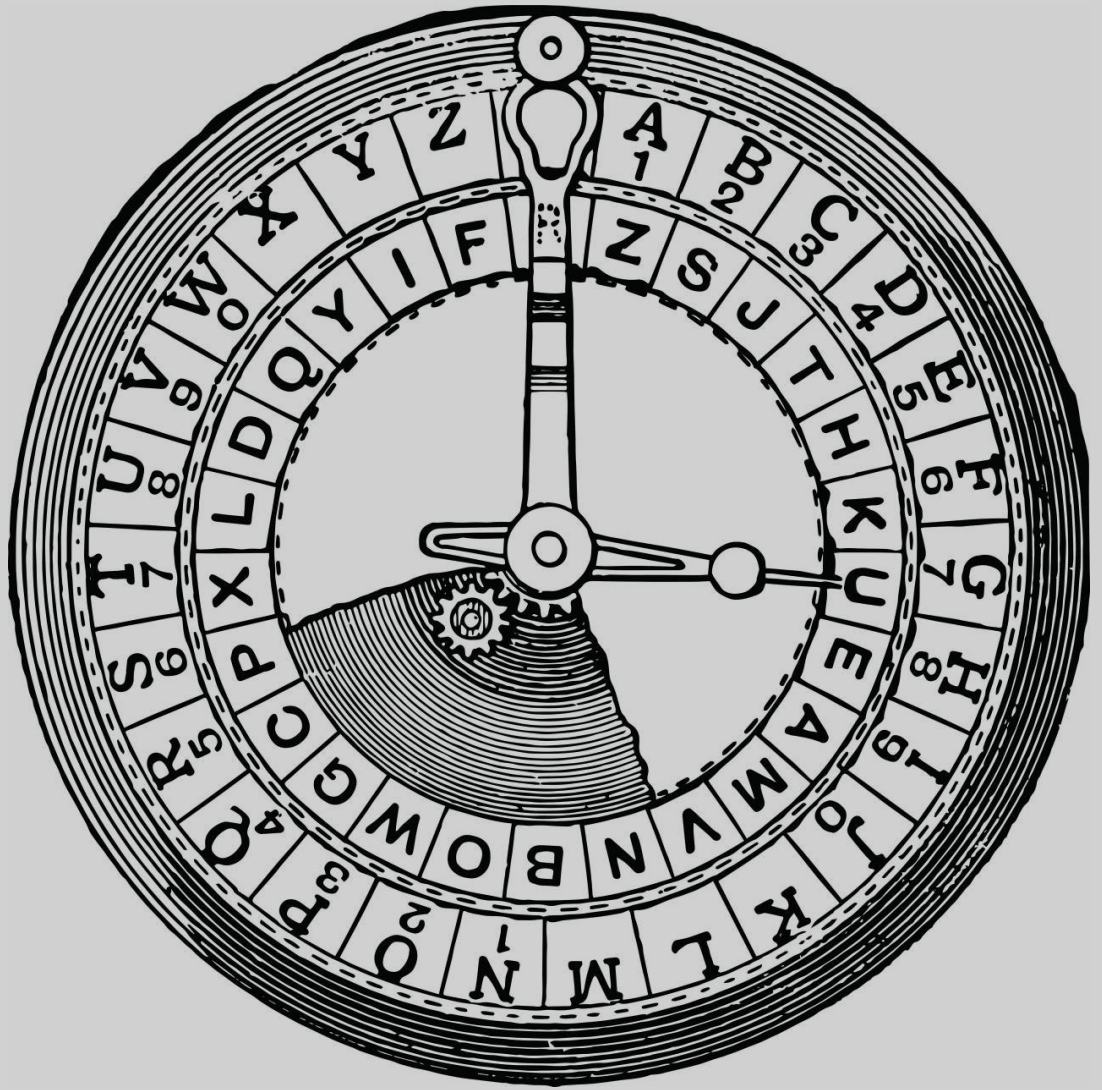
Segurança EAV

- **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

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

- **Proposição 11.3.** Se uma cifra de chave pública é EAV-segura, então também é CPA-segura.

Criptografia híbrida



Cifras para mensagens de tam. arbritrário

- **Afirmação 11.7.** Sejam $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ uma cifra de chave pública CPA segura para mensagens de tamanho fixo, então $\Pi' = (\mathrm{Gen}, \mathrm{Enc}', \mathrm{Dec}')$ onde
  - $\mathrm{Enc}'_{pk}(m_1, \dots, m_t) = \mathrm{Enc}_{pk}(m_1) \dots \mathrm{Enc}_{pk}(m_t)$
  - $\mathrm{Dec}'_{sk}(c_1, \dots, c_t) = \mathrm{Dec}_{sk}(c_1) \dots \mathrm{Dec}_{sk}(c_t)$

  é uma cifra CPA-segura para mensagens de tamanho arbitrário
- Ideia da prova na lista de exercícios

Na prática

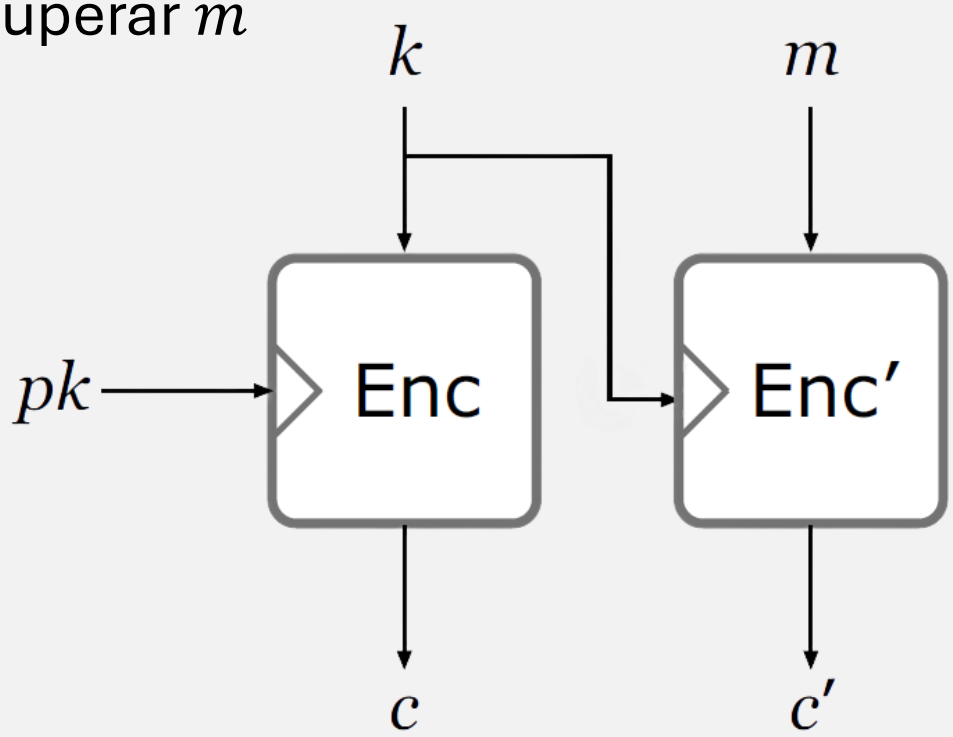
- Pela afirmação e uma cifra para mensagens de tamanho ℓ', quantas invocações da cifra original para cifrar uma mensagem de tamanho ℓ?

$$\gamma \doteq \left\lceil \frac{\ell}{\ell'} \right\rceil$$

- Ou seja, esforço computacional e tamanho do texto cifrado γ vezes maiores que na cifra original
- Podemos fazer melhor combinando cifras de chave privada e pública
  - Criptografia híbrida
  - Vale a pena pois cifras simétricas são mais rápidas e possuem textos cifrados menores

Ideia geral

- Usar uma cifra de chave pública para obter uma chave simétrica k
  - E então cifrar m usando k e uma cifra de chave privada
- Destinatário usa sua chave privada para recuperar k
  - E então usa k para recuperar m



KEM (*Key Encapsulation Mechanism*)

- Para compartilhar a chave, 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
- Três algoritmos
  - Geração de chaves
  - Encapsulamento (produz a chave simétrica e um texto cifrado)
  - Desencapsulamento (recupera a chave do texto cifrado)

Definição

- **Definição 11.9.** Um mecanism de encapsulamento de chaves (KEM) é uma tripla $(\mathrm{Gen}, \mathrm{Encaps}, \mathrm{Decaps})$ de algoritmos probabilísticos polinomiais tal que:
  - Gen recebe um parâmetro de segurança 1^n e produz um par de chaves pública e privada (pk, sk).
    - Assumimos que cada chave tem tamanho pelo menos n e que n pode ser determinado a partir de pk
  - $\backslash\mathrm{Encaps}$ recebe uma chave pública pk e um parâmetro de segurança 1^n, e produz uma chave $k \in \{0,1\}^{\ell(n)}$ e um texto cifrado c, onde ℓ é o tamanho da chave.
    - $(c, k) \leftarrow \mathrm{Encaps}_{pk}(1^n)$
  - $\backslash\mathrm{Decaps}$ é um algoritmo determinístico que recebe uma chave privada sk e um texto cifradado c, e produz uma chave k ou um símbolo especial $\perp$ indicando falha
    - $k := \mathrm{Decaps}_{sk}(c)$

Continuação da definição

- É necessário que
  - Com probabilidade $1 - \mathrm{negl}(n)$ sobre a escolha de (pk, sk), se

$$(c, k) \leftarrow \mathrm{Encaps}_{pk}(1^n)$$

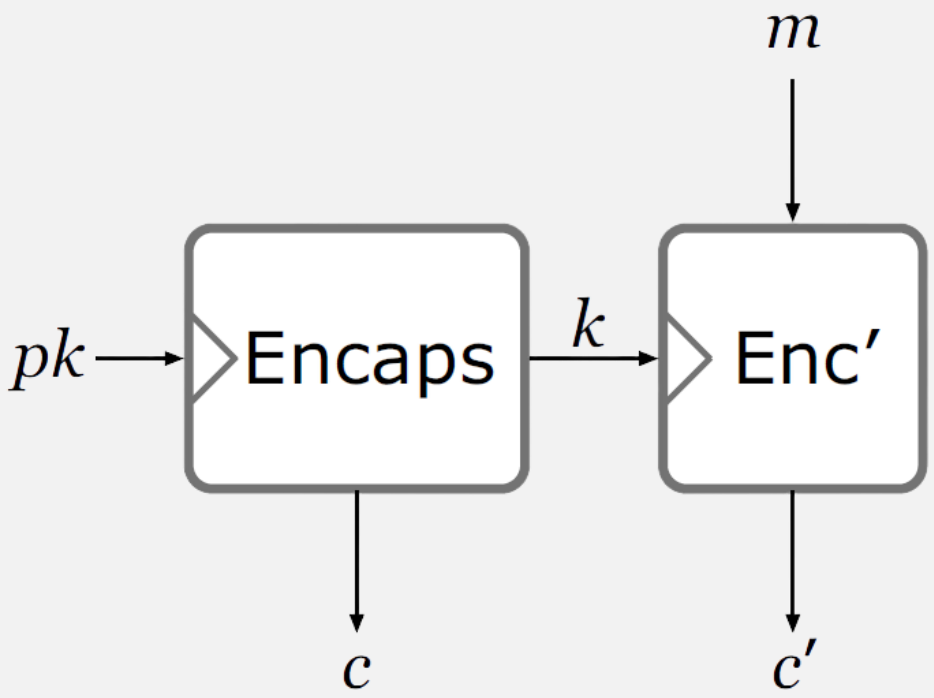
  Então

$$k := \mathrm{Decaps}_{sk}(c)$$

- Por simplicidade, assumimos que Encaps sempre produz um texto cifrado e uma chave de tamanho fixo $\ell(n)$

Esquema visual

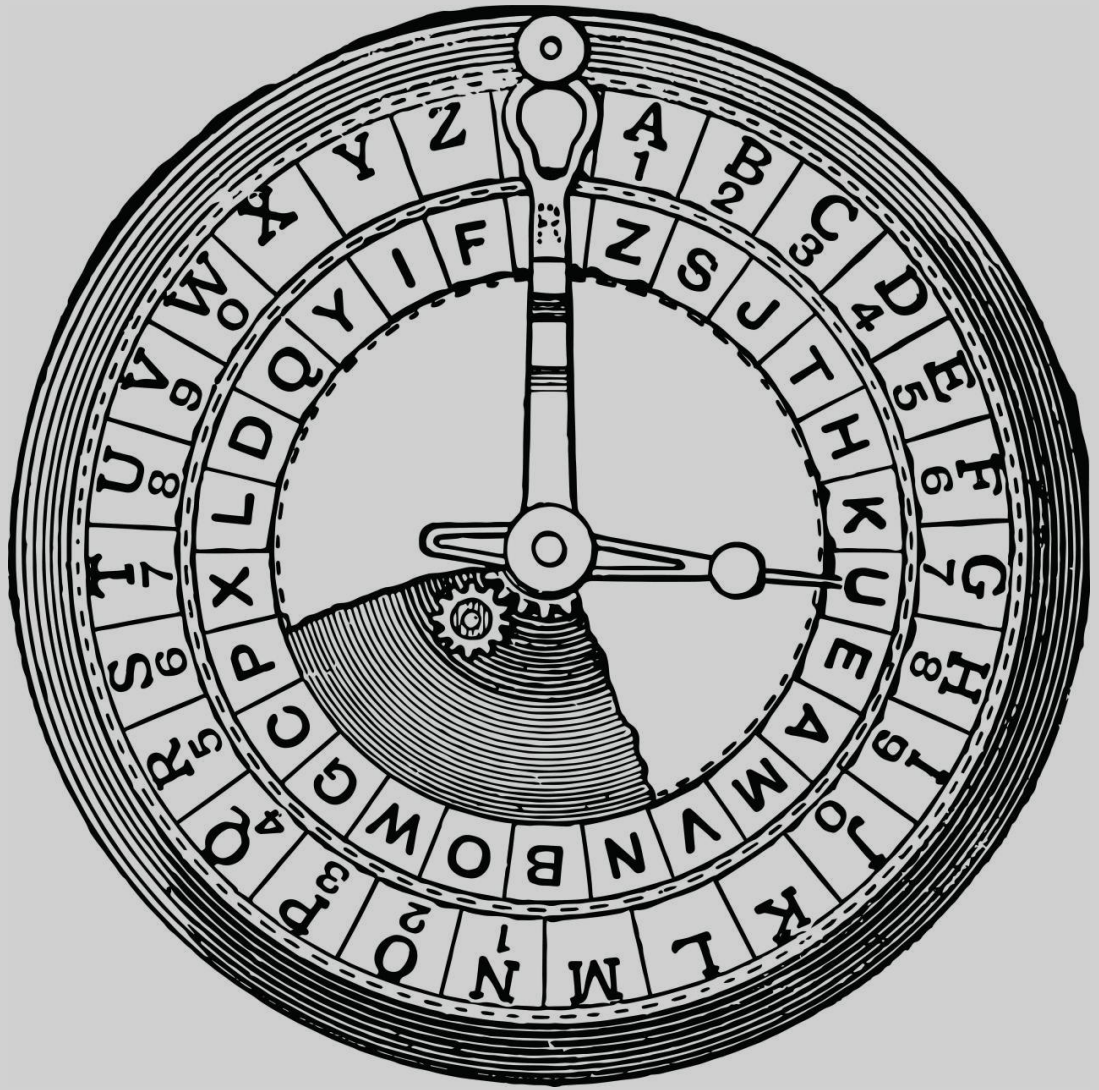
- Um KEM pode ser usado em criptografia híbrida como ao lado
- A cifra de chave privada utilizada é chamada de DEM (*Data Encapsulation Mechanism*)
- Daí o nome KEM/DEM



Construção 11.10

- Seja $\Pi = (\mathrm{Gen}, \mathrm{Encaps}, \mathrm{Decaps})$ um KEM com tamanho de chave n, e $\Pi' = (\mathrm{Gen}', \mathrm{Enc}', \mathrm{Dec}')$ uma cifra de chave privada. Construímos uma cifra de chave pública $\Pi^{\mathrm{hy}} = (\mathrm{Gen}^{\mathrm{hy}}, \mathrm{Enc}^{\mathrm{hy}}, \mathrm{Dec}^{\mathrm{hy}})$ a seguir:
  - $\mathrm{Gen}^{\mathrm{hy}}$: na entrada 1^n, execute $\mathrm{Gen}(1^n)$ e use as chaves pública e privadas (pk, sk) que são retornadas.
  - $\mathrm{Enc}^{\mathrm{hy}}$: ao receber como entrada a chave pública pk e a mensagem $m \in \{0,1\}^*$:
    1. Compute $(c, k) \leftarrow \mathrm{Encaps}_{pk}(1^n)$
    2. Compute $c' \leftarrow \mathrm{Enc}'_k(m)$
    3. Retorne o texto cifrado $\langle c, c' \rangle$
  - $\mathrm{Dec}^{\mathrm{hy}}$: ao receber como entrada a chave privada sk e um texto cifrado $\langle c, c' \rangle$:
    1. Compute $k := \mathrm{Decaps}_{sk}(c)$
    2. Retorne a mensagem $m := \mathrm{Dec}'_k(c')$

Eficiência



Tempo

- Fixamos um valor de n e seja
  - α o custo de encapsular uma chave privada de n bits
  - β o custo por bit de cifragem da cifra de chave privada
  - m a mensagem a ser cifrada, com $|m| > n$
- Custo por bit para cifrar m

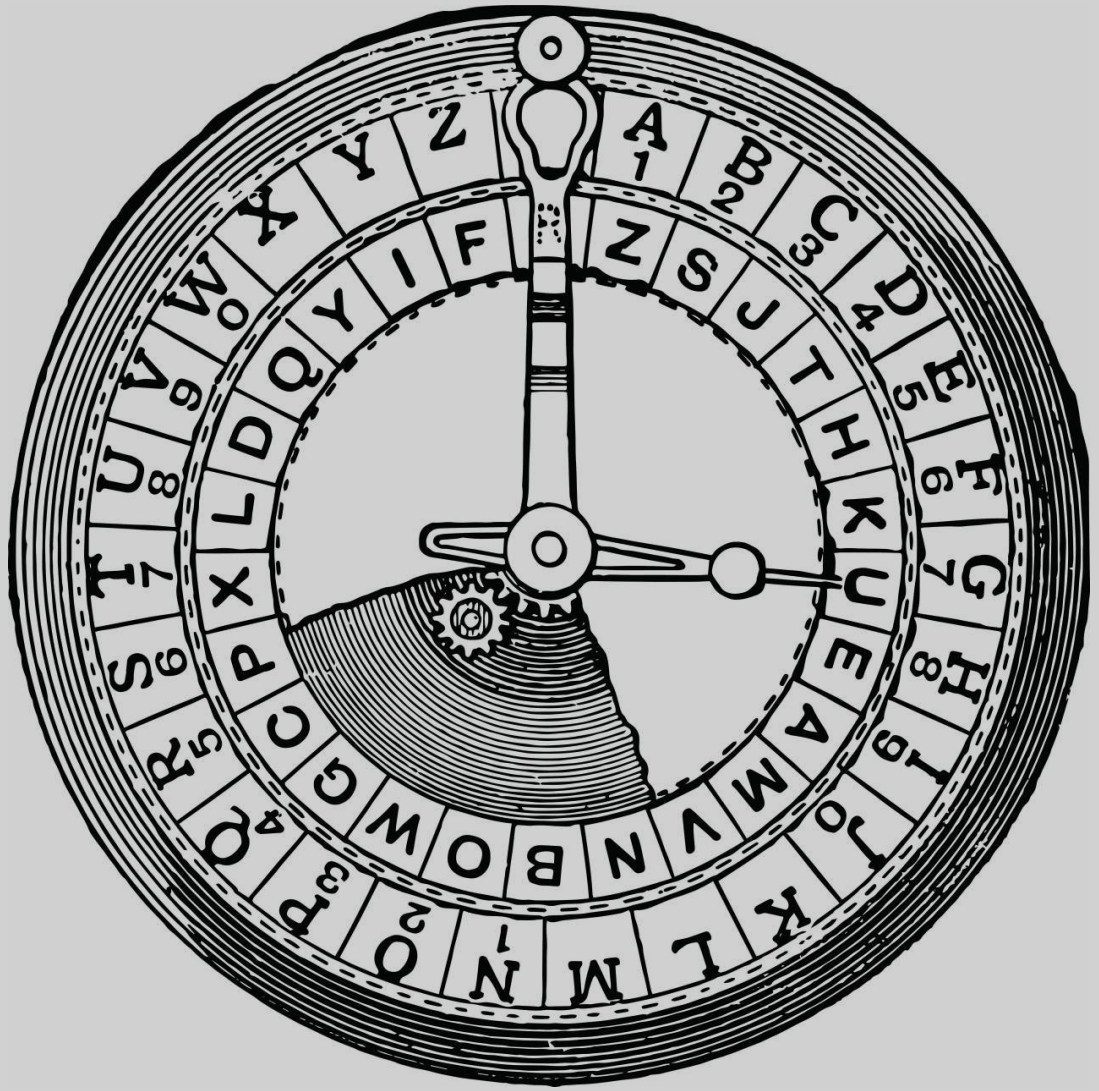
$$\frac{\alpha + \beta \cdot |m|}{|m|} = \frac{\alpha}{|m|} + \beta$$

Que tende a β para m suficientemente grande

Tamanho do texto cifrado

- $L =$ tamanho do texto cifrado produzido por Encaps
- Assumindo que a cifra simétrica produz textos cifrados de tamanho $|m| + n$ a partir da mensagem m
  - Até $|m|$ é possível, a cifra só precisa ser EAV-segura
- Tamanho do texto cifrado
  - $L + n + |m|$
- Usando uma cifra assimétrica bloco por bloco, com cada bloco de tamanho L, temos tamanho
  - $L \cdot \frac{|m|}{n}$
- KEM/DEM muito melhor para valores grandes de $|m|$

Segurança CPA



Ideia geral

- Queremos definir quando um KEM é CPA-seguro
- Vamos adotar uma estratégia similar à usada nos protocolos de troca de chaves
  - O protocolo é seguro se adversários eficientes não conseguem distinguir a chave real que foi enviada de uma chave aleatória
  - Neste caso, podemos usar a chave, sem medo, em uma cifra de chave simétrica

Experimento $\mathrm{KEM}_{\mathcal{A},\Pi}^{\mathrm{cpa}}(n)$

Desafiante

Adversário $\mathcal{A}$



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

$(c, k) \leftarrow \mathrm{Encaps}_{pk}(1^n)$

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

$(pk, c, \hat{k})$

$b' =$ chute para b



- Se $b = 0, \hat{k} = k$
- Se $b = 1, \hat{k} \leftarrow \{0,1\}^n$
- Dizemos que $\mathcal{A}$ vence e que $\mathrm{KEM}_{\mathcal{A},\Pi}^{\mathrm{cpa}}(n) = 1$ se $b' = b$

Segurança

- **Definição 11.11.** Um KEM Π é CPA-seguro se para todo algoritmo probabilístico polinomial $\mathcal{A}$ existe uma função negligenciável negl tal que

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

- **Teorema 11.12.** Se Π é um KEM CPA-seguro e Π' uma cifra simétrica que é EAV-segura, então o esquema da Construção 11.10 é uma cifra de chave pública CPA-segura.

Intuição da demonstração

- Notação $X \overset{c}{\equiv} Y$ se nenhum adversário probabilístico polinomial consegue distinguir (com vantagem não negligenciável) dentre as duas distribuições
- Seja $(c, k) \leftarrow \mathrm{Encaps}_{pk}(1^n)$
- Como o KEM é CPA seguro, segue que

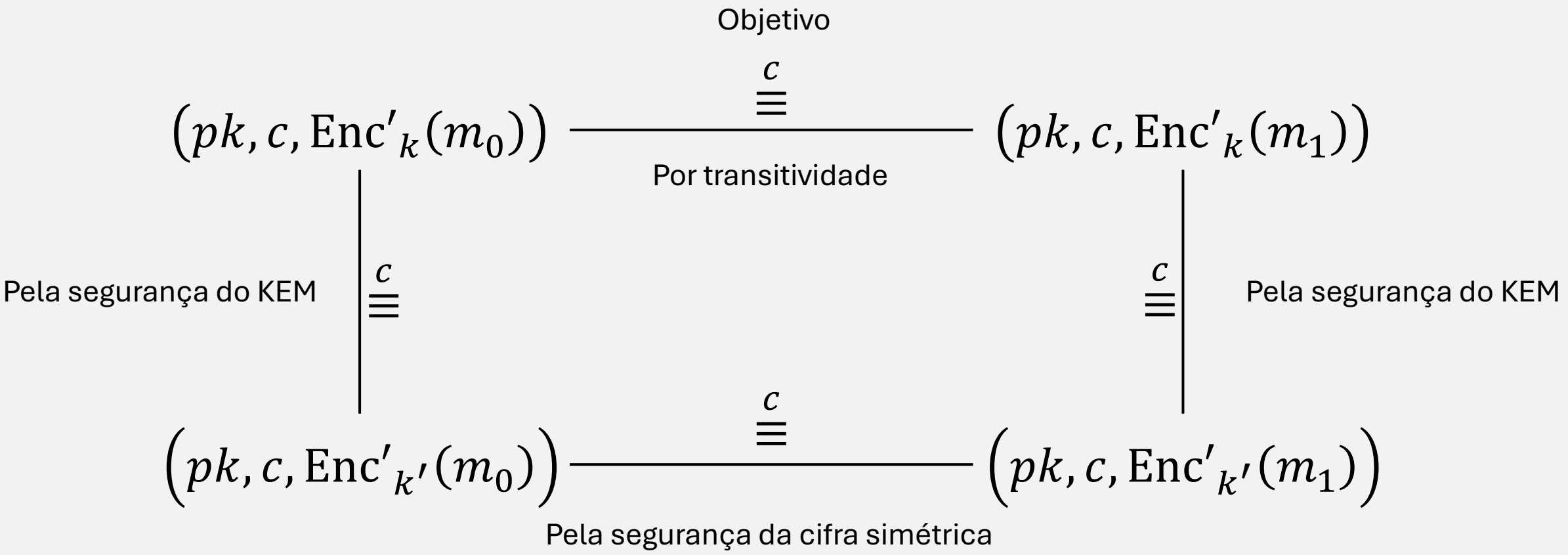
$$(pk, c, k) \overset{c}{\equiv} (pk, c, k')$$

Onde k' é uma chave aleatória.

- Queremos mostrar que a cifra resultante é CPA segura, ou seja, que, para o desafio m_0, m_1 produzido pelo adversário

$$\left(pk, c, \mathrm{Enc'}_k(m_0)\right) \overset{c}{\equiv} \left(pk, c, \mathrm{Enc}'_k(m_1)\right)$$

Mais intuição da demonstração



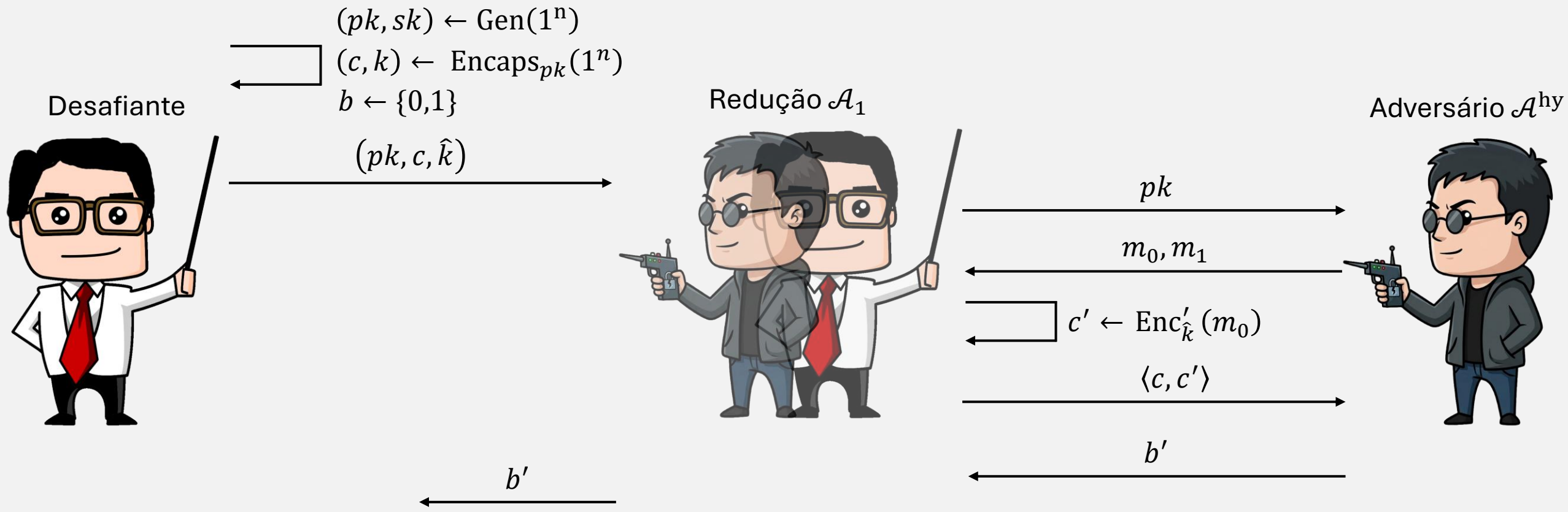
Primeira parte da demonstração

- Vamos focar na primeira parte da prova
  - As outras são similares (todas reduções)

$$\left(pk, c, \mathrm{Enc'}_k(m_0)\right) \overset{c}{\equiv} \left(pk, c, \mathrm{Enc'}_{k'}(m_0)\right)$$

- Seja $\mathcal{A}^{\mathrm{hy}}$ um adversário para a cifra da Construção 11.10
- Vamos construir um adversário/redução $\mathcal{A}_1$ para o KEM subjacente

Redução



- A redução sempre cifra m_0!
- Lembrando que queremos mostrar que $\left(pk, c, \mathrm{Enc}'_k(m_0)\right) \approx \left(pk, c, \mathrm{Enc}'_{k'}(m_0)\right)$

Análise da redução

- Quando $b = 0$, $\mathcal{A}_1$ recebe (pk, c, k), onde k é a chave real correspondente ao texto cifrado c
  - Então $\mathcal{A}^{\text{hy}}$ recebe $\langle c, c' \rangle = \langle c, \text{Enc}'_k(m_0) \rangle$
  - Logo

$$\Pr\left[\mathcal{A}_1\left(pk, c, \hat{k}\right) = 0 \mid b = 0\right] = \Pr\left[\mathcal{A}^{\text{hy}}\left(pk, c, \text{Enc}'_k(m_0)\right) = 0\right]$$

- Quando $b = 1$, $\mathcal{A}_1$ recebe (pk, c, k'), onde k' é uma chave aleatória
  - Então $\mathcal{A}^{\text{hy}}$ recebe $\langle c, c' \rangle = \langle c, \text{Enc}'_{k'}(m_0) \rangle$
  - Logo

$$\Pr\left[\mathcal{A}_1\left(pk, c, \hat{k}\right) = 1 \mid b = 1\right] = \Pr\left[\mathcal{A}^{\text{hy}}\left(pk, c, \text{Enc}'_{k'}(m_0)\right) = 1\right]$$

Mais análise

- Segue que

$$
\begin{aligned}
&\Pr\left[\mathrm{KEM}^{\mathrm{cpa}}_{\mathcal{A}_1,\Pi}(n) = 1\right] \\
&= \frac{1}{2} \cdot \Pr\left[\mathcal{A}_1\left(pk, c, \hat{k}\right) = 0 \mid b = 0\right] + \frac{1}{2} \cdot \Pr\left[\mathcal{A}_1\left(pk, c, \hat{k}\right) = 1 \mid b = 1\right] \\
&= \frac{1}{2} \cdot \Pr\left[\mathcal{A}^{\mathrm{hy}}\left(pk, c, \mathrm{Enc}'_k(m_0)\right) = 0\right] + \frac{1}{2} \cdot \Pr\left[\mathcal{A}^{\mathrm{hy}}\left(pk, c, \mathrm{Enc}'_{k'}(m_0)\right) = 1\right]
\end{aligned}
$$

- Como nosso KEM é CPA-seguro, existe uma função negligenciável negl tal que

$$\Pr\left[\mathrm{KEM}^{\mathrm{cpa}}_{\mathcal{A}_1,\Pi}(n) = 1\right] \leq \frac{1}{2} + \mathrm{negl}(n)$$

Finalizando

- Multiplicando ambos os lados por 2

$$\Pr\left[\mathcal{A}^{\text{hy}}\left(pk, c, \text{Enc}'_k(m_0)\right) = 0\right] + \Pr\left[\mathcal{A}^{\text{hy}}\left(pk, c, \text{Enc}'_{k'}(m_0)\right) = 1\right] \leq 1 + 2 \cdot \text{negl}(n)$$

- Fazendo

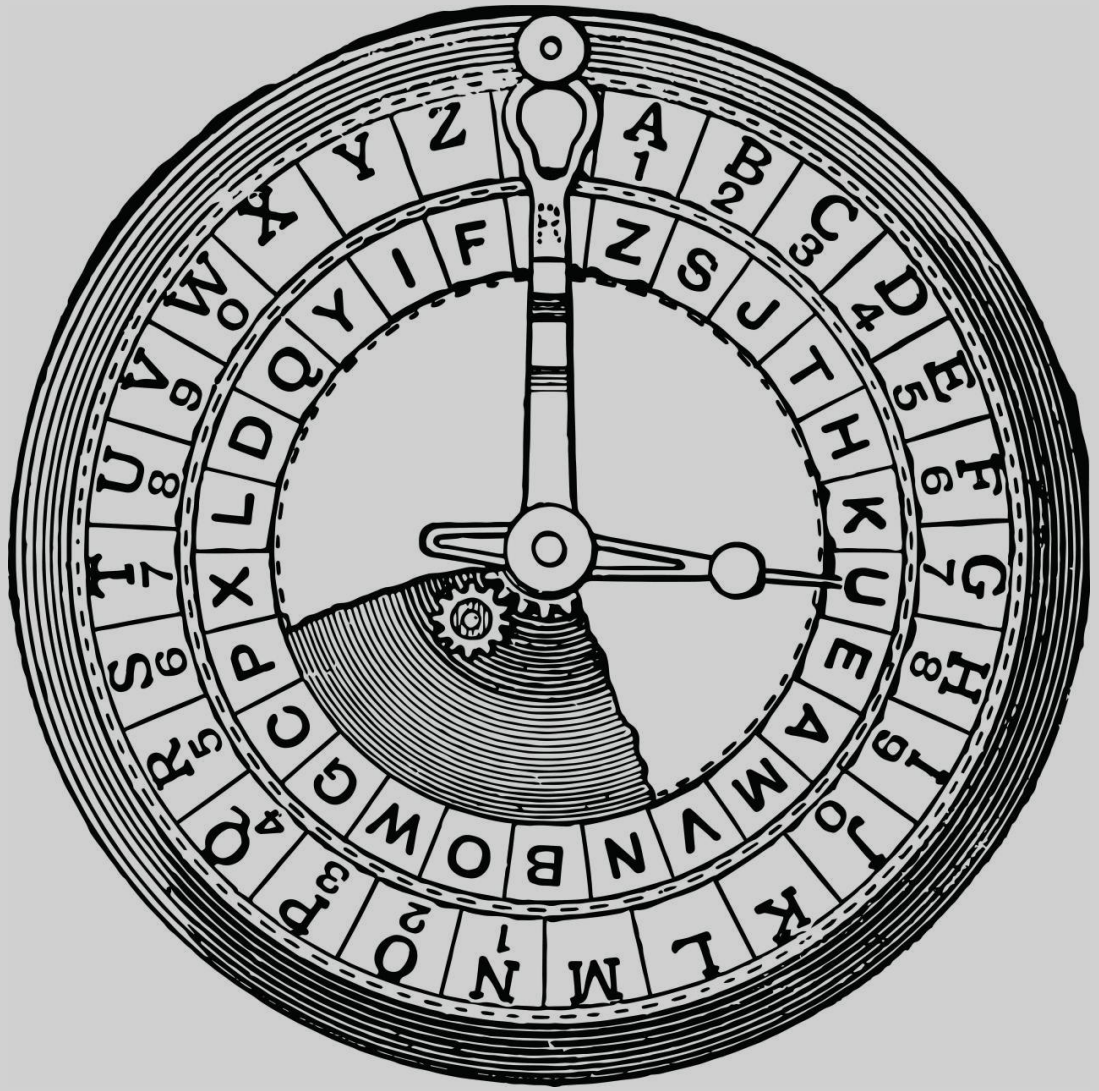
$$\Pr\left[\mathcal{A}^{\text{hy}}\left(pk, c, \text{Enc}'_k(m_0)\right) = 0\right] = 1 - \Pr\left[\mathcal{A}^{\text{hy}}\left(pk, c, \text{Enc}'_k(m_0)\right) = 1\right]$$

e simplificando

$$\Pr\left[\mathcal{A}^{\text{hy}}\left(pk, c, \text{Enc}'_{k'}(m_0)\right) = 1\right] - \Pr\left[\mathcal{A}^{\text{hy}}\left(pk, c, \text{Enc}'_k(m_0)\right) = 1\right] \leq 2 \cdot \text{negl}(n)$$

- Ou seja, $\mathcal{A}^{\text{hy}}$ não consegue distinguir dentre $\left(pk, c, \text{Enc}'_k(m_0)\right)$ e $\left(pk, c, \text{Enc}'_{k'}(m_0)\right)$

Para fechar



Para fechar

- Hoje
  - Criptografia híbrida
    - Combina cifras de chave privada e pública
    - Mais eficiente que construções puras de chave pública
  - KEM/DEM
    - Encapsula chaves privadas usando a chave pública
  - KEM CPA-seguro + cifra simétrica EAV-segura = cifra de chave pública CPA segura!
- Próxima aula
  - Cifra de El-Gamal
    - Baseada no problema (decisional) de Diffie-Hellman