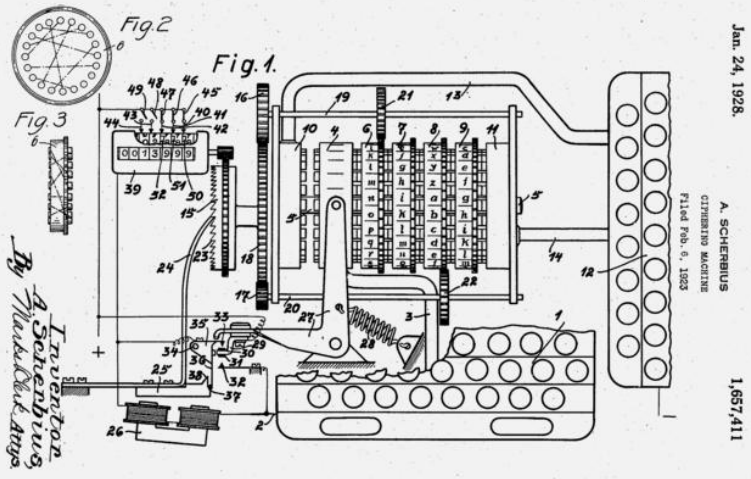
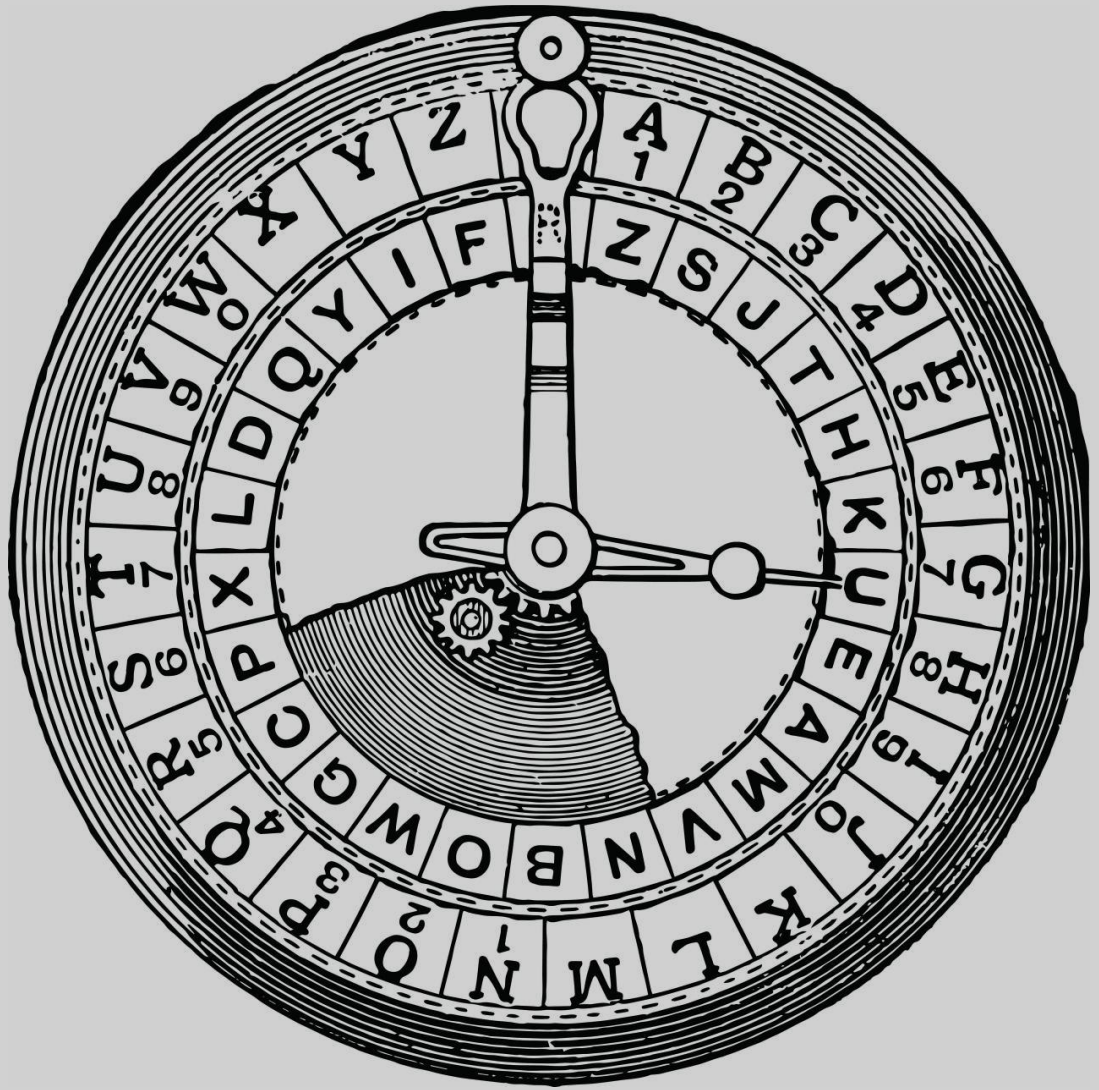
Reduções

Fundamentos da Criptografia

Nicollas Mocelin Sdroievski



Na última aula



Experimentos

- Duas partes para definição de segurança
  - Um modelo de ameaça (essencialmente, o poder do adversário)
  - Um objetivo de segurança (o que significa quebrar a segurança do protocolo)
- Por enquanto, adversários $\mathcal{A}$ que apenas interceptam o texto cifrado

O experimento $\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}$

Desafiante

Adversário $\mathcal{A}$



$m_0, m_1 \in \mathcal{M}$

$k \leftarrow \mathrm{Gen}$

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

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

$b' =$ chute para b



- Para cifras perfeitamente secretas, o adversário acerta com probabilidade $1/2$
- Vamos relaxar para $\leq \frac{1}{2} + \mathrm{negl}(n)$

Funções negligenciáveis

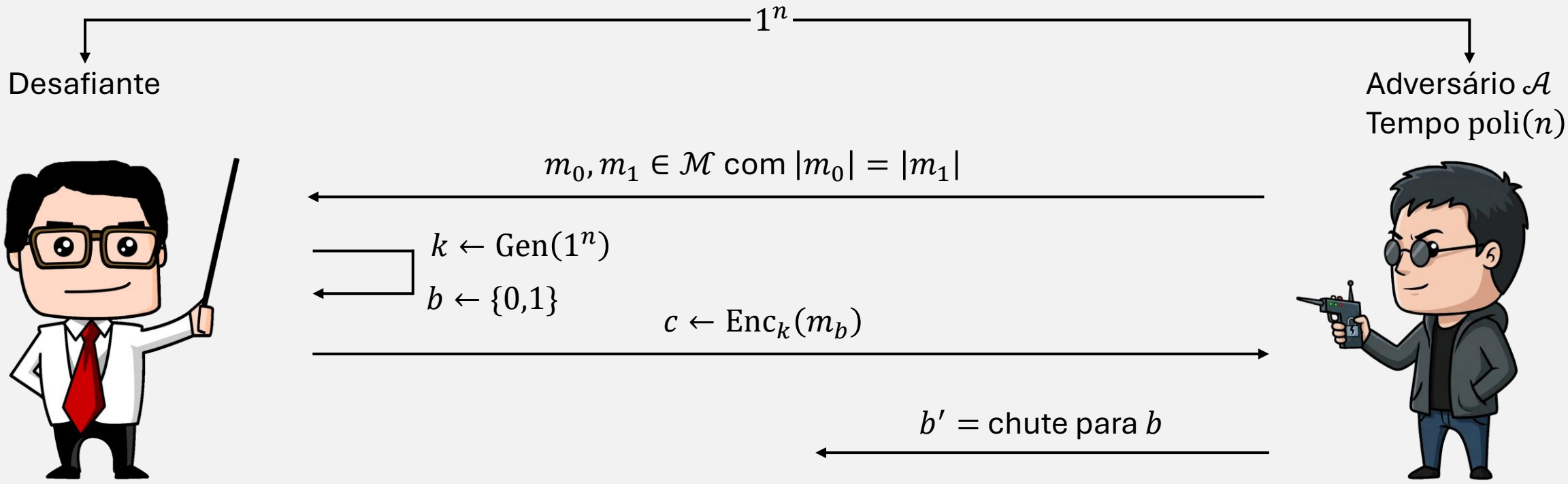
- **Definição 3.4.** Uma função f dos números naturais para números reais não-negativos é **negligenciável** se para todo polinômio positivo p existe um N tal que para todos os inteiros $n > N$, vale que

$$f(n) < \frac{1}{p(n)}$$

- Definições alternativas:
  - Para todo polinômio p e todo valor de n suficientemente grande, $f(n) < \frac{1}{p(n)}$
  - Para toda constante c existe N tal que para todo $n > N$, $f(n) < n^{-c}$

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

- Mesmo experimento, mas ambos desafiante e adversário recebem o parâmetro de segurança n como entrada
- E o adversário é limitado a tempo polinomial em n



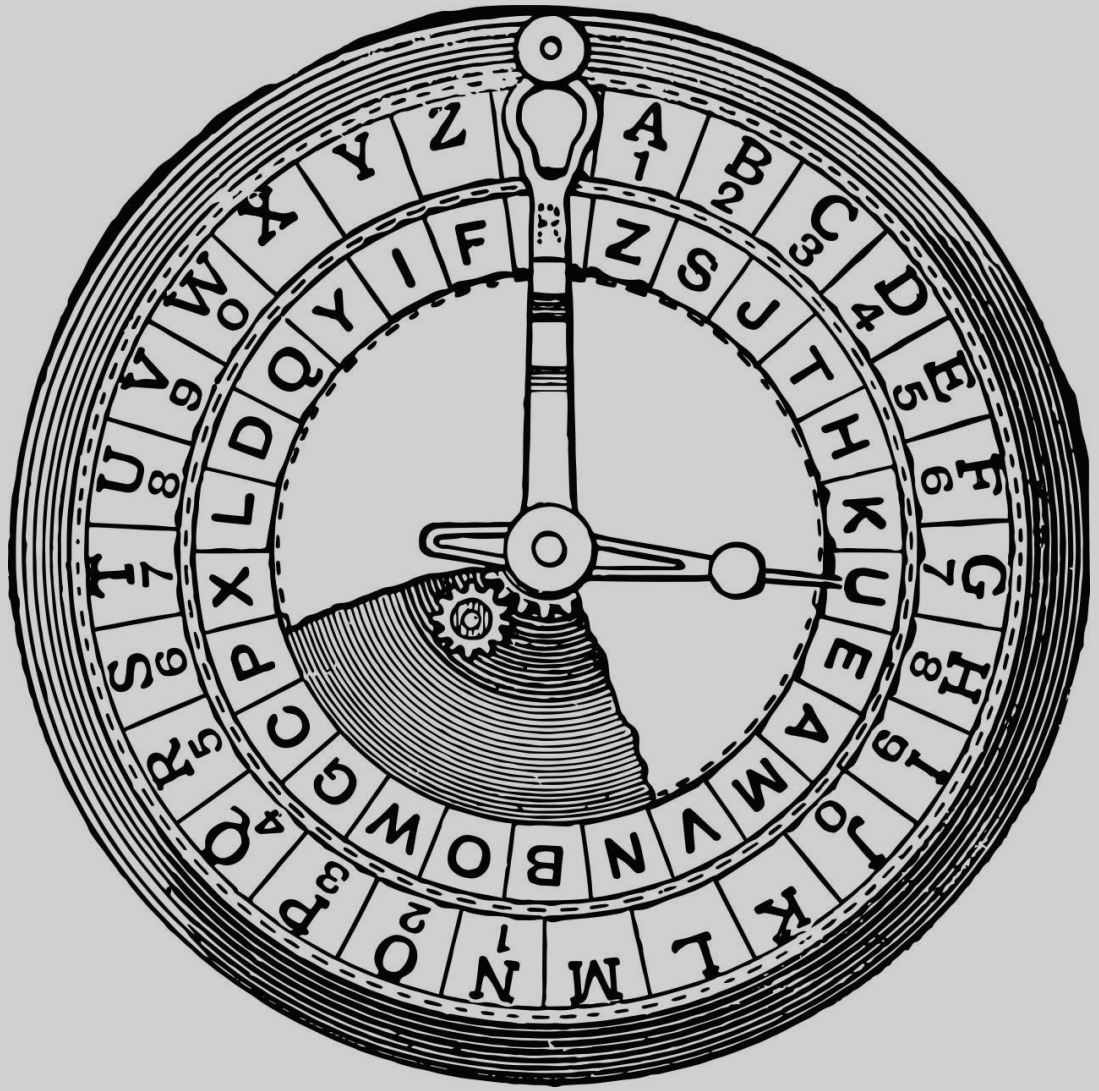
Definição de segurança

- Quando o adversário acerta o valor de $b' = b$, o experimento obtém sucesso e dizemos que $\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n) = 1$
- **Definição 3.8.** Uma cifra de chave privada $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ 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, para todo n,

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

onde as probabilidades são sobre a aleatoriedade de $\mathcal{A}$ e do Desafiante (para escolher a chave, o bit b, e de Enc , caso necessário)

Provas de segurança



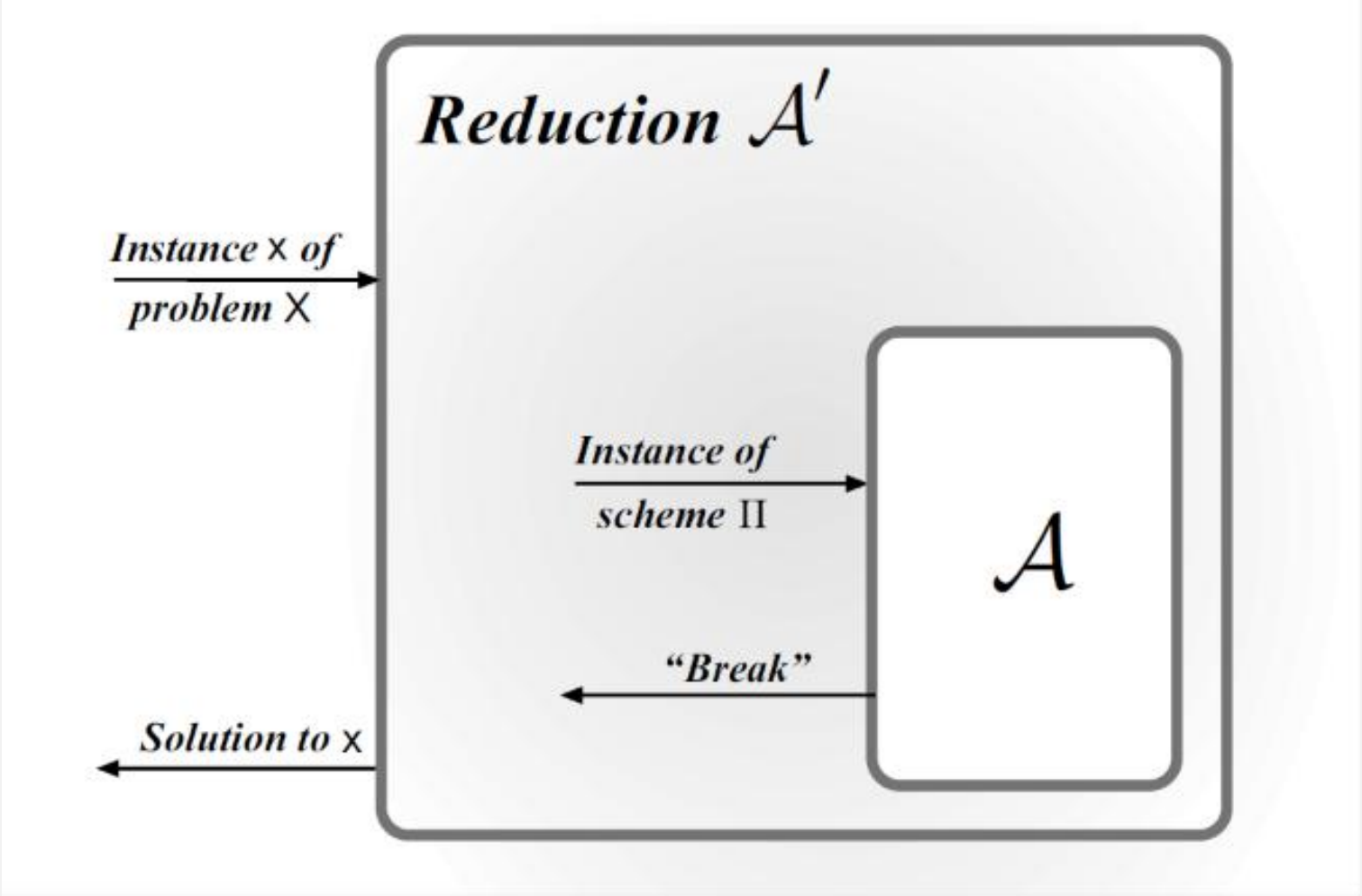
Suposições/Hipóteses

- Construções incondicionalmente seguras (como one-time pad) possuem várias limitações
- Vamos contornar essas limitações, porém, com uma desvantagem
  - A partir de agora, resultados **condicionais**
- Em particular, quase tudo em cripto necessita que P ≠ NP

Reduções

- Queremos provar a segurança de um protocolo Π
  - De acordo com uma definição precisa
- Vamos assumir, por exemplo, que é difícil resolver determinado problema computacional X
  - De novo de acordo com uma definição precisa
- Vamos provar que a dificuldade de X implica na segurança de Π
- Como?
  - Vamos mostrar como transformar um adversário eficiente $\mathcal{A}$ que quebra a segurança de Π em um algoritmo eficiente $\mathcal{A}'$ que resolve X

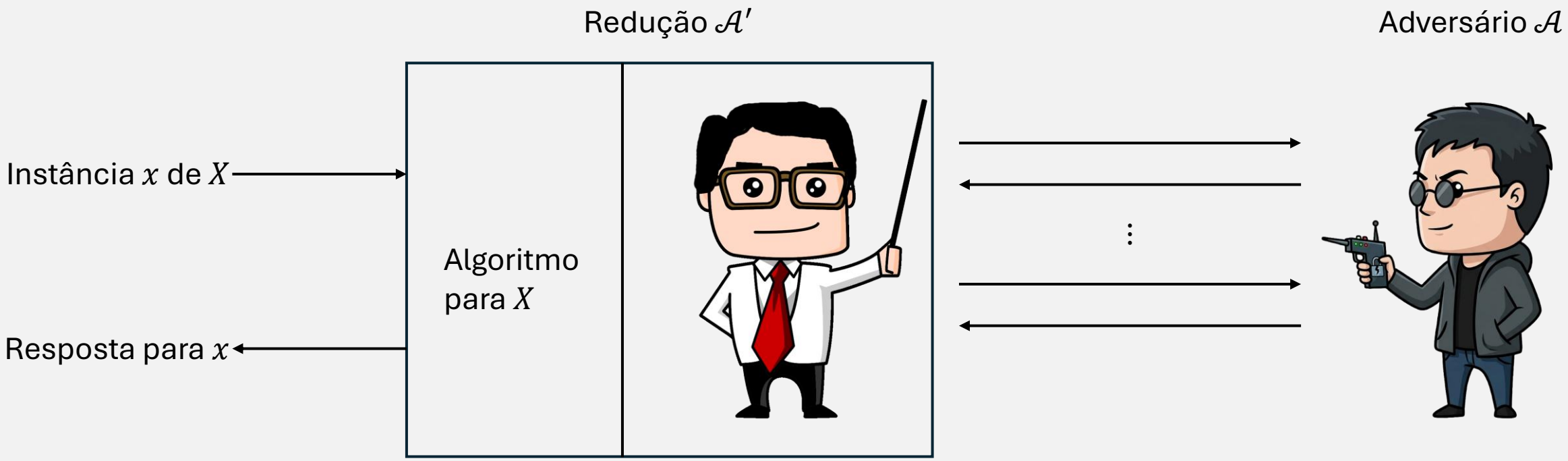
Visão geral


Reduction $\mathcal{A}'$
Instance x of
problem X
Instance of
scheme II
$\mathcal{A}$
"Break"
Solution to x

Sequência de passos

- Fixe um adversário eficiente $\mathcal{A}$ que ataca Π e denote sua probabilidade de sucesso por $\varepsilon(n)$
- Construa um algoritmo eficiente $\mathcal{A}'$ (a redução) que tenta resolver uma instância x de X usando $\mathcal{A}$ como uma sub-rotina
  - $\mathcal{A}'$ simula o Desafiante no experimento para Π ao interagir com $\mathcal{A}$
  - $\mathcal{A}$ não consegue perceber a diferença entre a simulação de $\mathcal{A}'$ e o Desafiante real, então age como no experimento
  - Caso $\mathcal{A}$ consiga quebrar a segurança de Π, então $\mathcal{A}'$ deve conseguir resolver x com probabilidade pelo menos $1/p(n)$, para um polinômio p
  - Assim, $\mathcal{A}'$ resolve X com probabilidade $\varepsilon(n)/p(n)$

Esquema visual



Concluindo

- Assumindo que $\mathcal{A}$ quebra Π com probabilidade $\varepsilon(n)$, construímos $\mathcal{A}'$ que resolve X com probabilidade $\varepsilon(n)/p(n)$
- **Ponto importante:** Se $\mathcal{A}$ é eficiente (polinomial), então $\mathcal{A}'$ deve ser também
- Assumindo que X é difícil
  - Não pode ser resolvido por um algoritmo eficiente com probabilidade não-negligenciável
- Segue que $\varepsilon(n)$ deve ser negligenciável
- E então que Π é seguro
  - Pois a probabilidade de sucesso de **qualquer** algoritmo $\mathcal{A}$ deve ser negligenciável

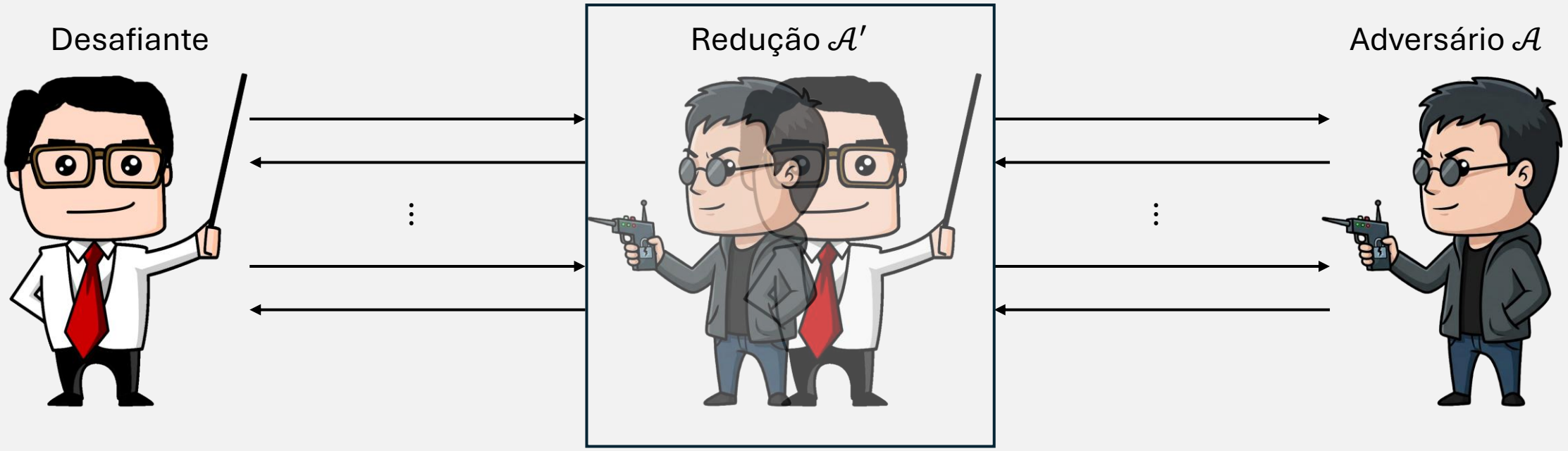
Observações

- $\mathcal{A}'$ utiliza $\mathcal{A}$ como uma **caixa-preta**
  - $\mathcal{A}'$ não sabe nada sobre o funcionamento interno de $\mathcal{A}$
  - $\mathcal{A}'$ sabe apenas que $\mathcal{A}$ foi feito para atacar Π
- $\mathcal{A}'$ deve conseguir simular a **visão** de $\mathcal{A}$ no experimento para Π
  - Do ponto de vista de $\mathcal{A}$, ele está interagindo com o Desafiante

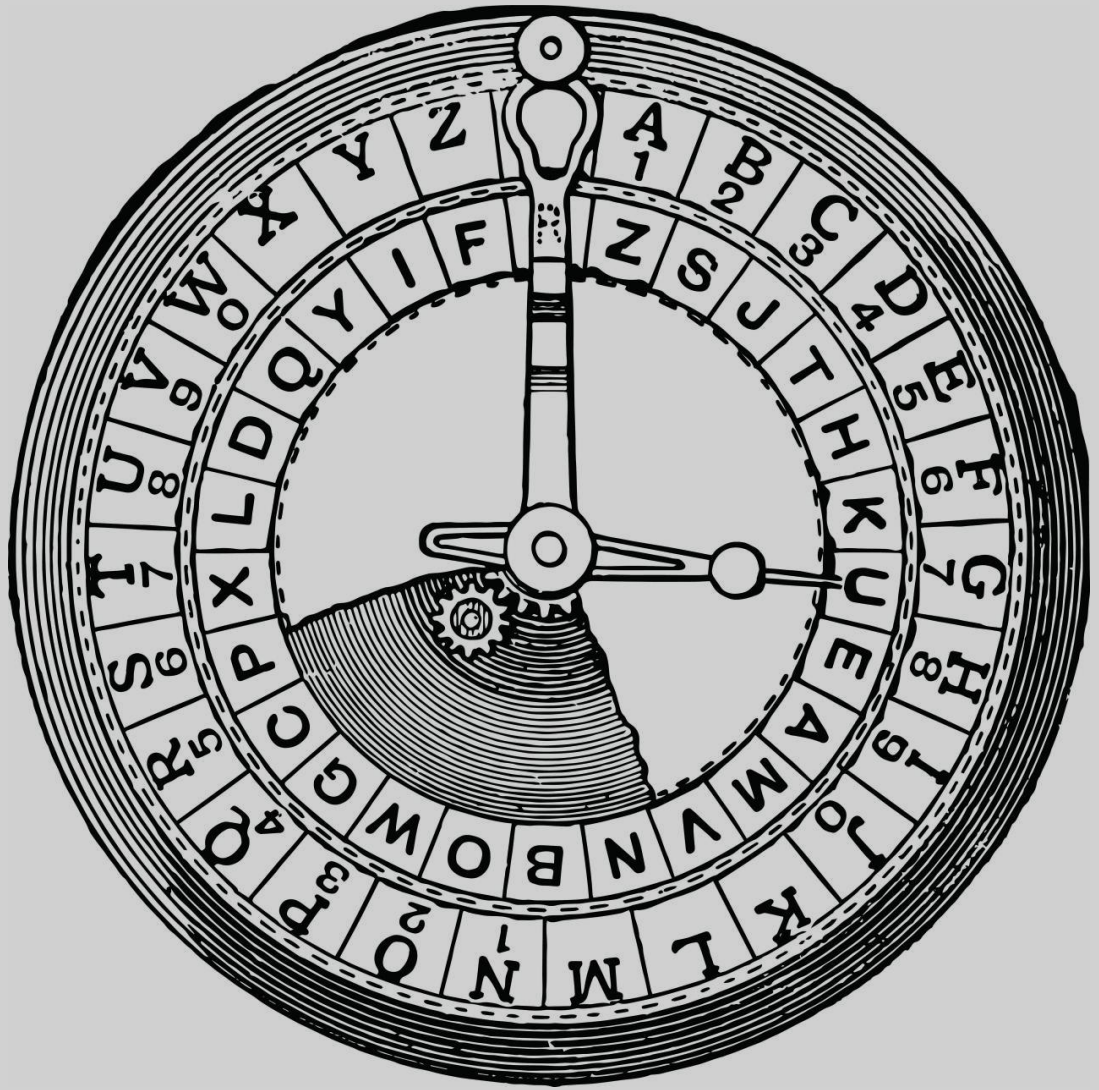
Reduções entre protocolos

- Também podemos provar a segurança de um protocolo Π através da segurança de outro protocolo Γ
- A redução $\mathcal{A}'$ serve dois papéis novamente
  - Desafiante para Π
  - Adversário para Γ
- Ideia semelhante
  - Assumimos que existe um adversário $\mathcal{A}$ para Π com probabilidade de sucesso $\varepsilon(n)$
  - Construímos a redução $\mathcal{A}'$, que tem probabilidade de sucesso $\varepsilon(n)/p(n)$ para Γ, onde p é um polinômio
  - Assumindo que Γ é segura, segue que $\varepsilon(n)$ deve ser negligenciável

A redução “engana” os dois!



Uma redução



É possível recuperar somente um bit?

- Considere uma cifra de chave simétrica EAV segura
- Será que um adversário conseguiria recuperar apenas um bit de uma mensagem cifrada escolhida de maneira aleatória?
  - Com vantagem não negligenciável, isto é, com probabilidade $\frac{1}{2} + \frac{1}{q(n)}$ para algum polinômio q
- Provaremos que isso não é possível (Teorema 3.10 no livro, com uma prova um pouco diferente)
- Primeiro passo?
  - Vamos definir um novo experimento!

O experimento $\mathrm{PrivK}^{\mathrm{eav-bit}}_{\mathcal{A},\Pi}(n,i)$

1^n

Desafiante

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



$k \leftarrow \mathrm{Gen}(1^n)$

$m \leftarrow \{0,1\}^{\ell}$ (escolhida aleatoriamente)

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

$b_i =$ chute para o i-ésimo bit de m



- A saída do experimento é 1 se $b_i = m[i]$, para $b_i \leftarrow \mathcal{A}(c)$
- Escrevemos $\mathrm{PrivK}^{\mathrm{eav-bit}}_{\mathcal{A},\Pi}(n,i) = 1$ se a saída do experimento é 1
  - e dizemos que $\mathcal{A}$ obtém sucesso neste caso

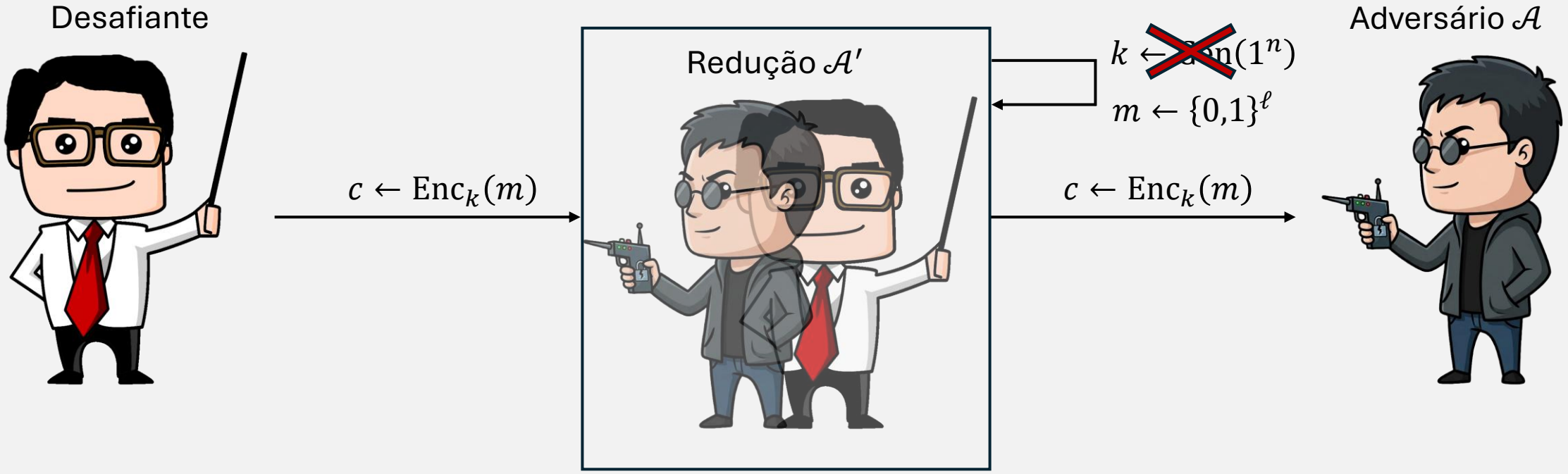
Definindo a segurança que queremos

- Qual a segurança que esperamos através do experimento que construímos?
  - Queremos que o adversário só consiga adivinhar o i-ésimo bit da mensagem com probabilidade negligenciavelmente maior que $1/2$
  - Queremos que, para qualquer algoritmo probabilístico polinomial $\mathcal{A}$ e qualquer $i \in \{1,2,\ldots,n\}$:

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

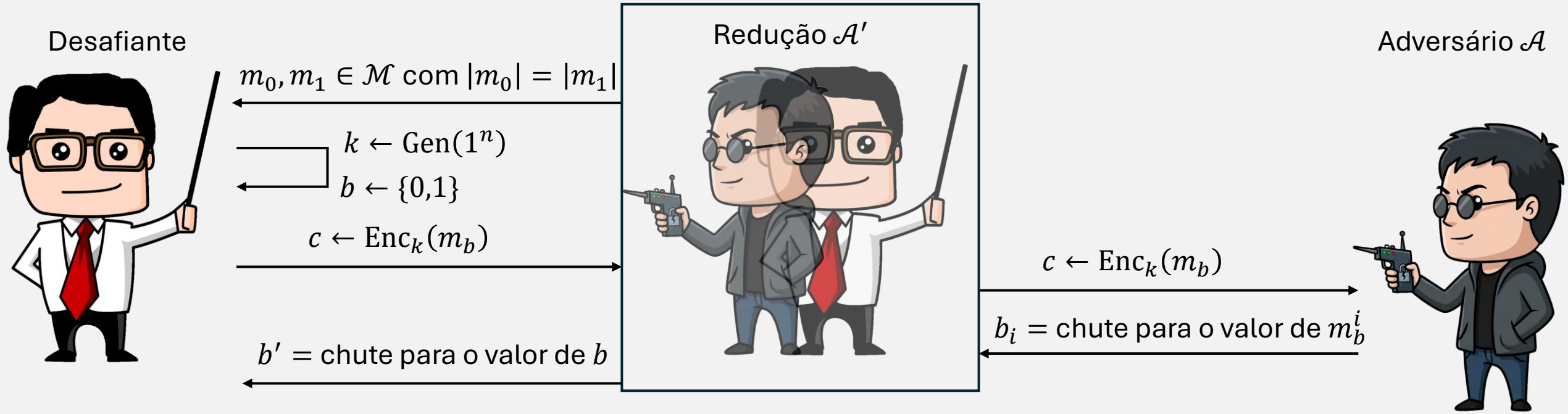
onde $\mathrm{negl}(n)$ é uma função negligenciável e a probabilidade é sobre a escolha de k usando Gen, escolha uniforme de $m \in \{0,1\}^{\ell}$, a aleatoriedade de Enc e a aleatoriedade de $\mathcal{A}$

Construindo a redução



- O que $\mathcal{A}$ espera receber?
  - $c \leftarrow \mathrm{Enc}_k(m)$ para escolha aleatória de m e $k \leftarrow \mathrm{Gen}(1^n)$
- Mas a redução não conhece o k do Desafiante!
- Não tem problema, basta pedir pro Desafiante produzir c!

Construindo a redução



- Como definir as mensagens m_0 e m_1?
  - m_0 deve ter $m_0^i = 0$ e m_1 deve ter $m_1^i = 1$
- E o valor de b'?
  - Pode ser igual a b_i

Descrição da redução

- A redução $\mathcal{A}'$ faz o seguinte
  1. Sorteia m_0 dentre as mensagens que possuem o i-ésimo bit igual a 0
  2. E m_1 de maneira similar mas com o i-ésimo bit igual a 1
  3. Envia m_0 e m_1 para o Desafiante e recebe c de volta
  4. Envia c para o Adversário $\mathcal{A}$ e recebe b_i de volta
  5. Tem como saída $b' = b_i$
- **Ponto importante.** O texto cifrado $c \leftarrow \mathrm{Enc}_k(m_b)$ que $\mathcal{A}'$ envia para $\mathcal{A}$ é distribuído como se m_b fosse apenas uma mensagem uniforme

Demonstração do ponto importante

- **Ponto importante.** O texto cifrado $c \leftarrow \mathrm{Enc}_k(m_b)$ que $\mathcal{A}'$ envia para $\mathcal{A}$ é distribuído como se m_b fosse apenas uma mensagem uniforme
- **Demonstração:** sejam I_0, I_1 os conjuntos de mensagens com o i-ésimo bit igual a 0 e 1, respectivamente, e seja m uma mensagem qualquer

$$\begin{aligned}
&\Pr[\mathrm{Enc}_k(m_b) = \mathrm{Enc}_k(m)] \\
&= \frac{1}{2} \cdot \Pr_{m_0 \leftarrow I_0}[\mathrm{Enc}_k(m_0) = \mathrm{Enc}_k(m)] + \frac{1}{2} \cdot \Pr_{m_1 \leftarrow I_1}[\mathrm{Enc}_k(m_1) = \mathrm{Enc}_k(m)] \\
&= \frac{1}{2} \cdot 2^{-\ell+1} \\
&= 2^{-\ell}
\end{aligned}$$

Onde a segunda igualdade segue pois uma das probabilidades é obrigatoriamente zero e a outra igual a $2^{-\ell+1}$, dependendo do i-ésimo bit de m

Finalizando o argumento

- Queremos mostrar que $\Pr\left[\mathrm{PrivK}^{\mathrm{eav-bit}}_{\mathcal{A},\Pi}(n,i)=1\right] \leq 1/2 + \mathrm{negl}(n)$
- Para isso, analisamos a probabilidade de sucesso de $\mathcal{A}'$ no experimento $\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A}',\Pi}(n)$
- Perceba que $\mathcal{A}'$ obtém sucesso exatamente quando $\mathcal{A}$ consegue adivinhar o i-ésimo bit de m_b, então

$$\Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A}',\Pi}(n)=1\right] = \Pr\left[\mathrm{PrivK}^{\mathrm{eav-bit}}_{\mathcal{A},\Pi}(n,i)=1\right]$$

Como assumimos que a cifra Π é IND-EAV segura, existe uma função negligenciável negl tal que

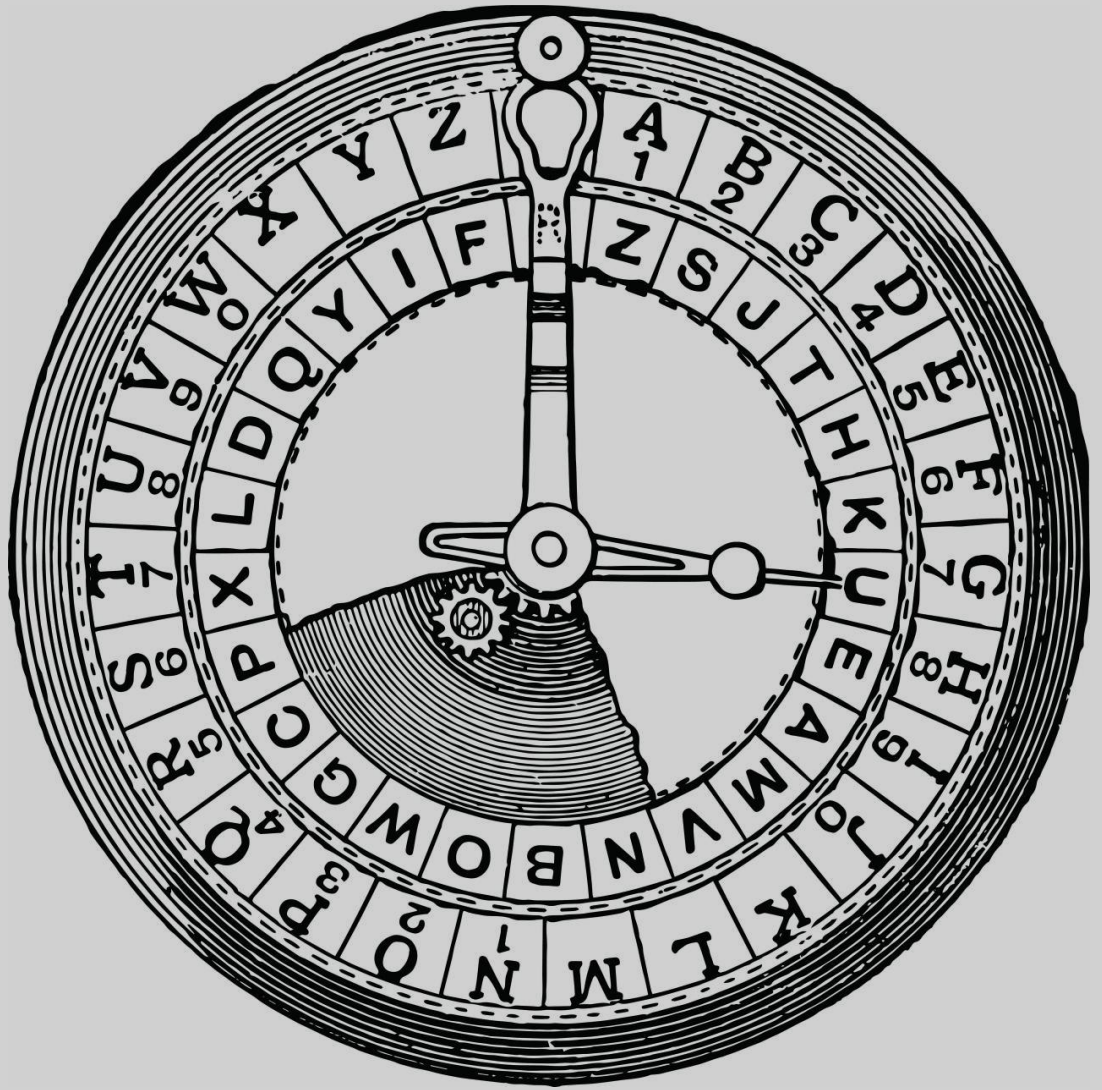
$$\Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A}',\Pi}(n)=1\right] \leq \frac{1}{2} + \mathrm{negl}(n).$$

Segue que

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

como desejado

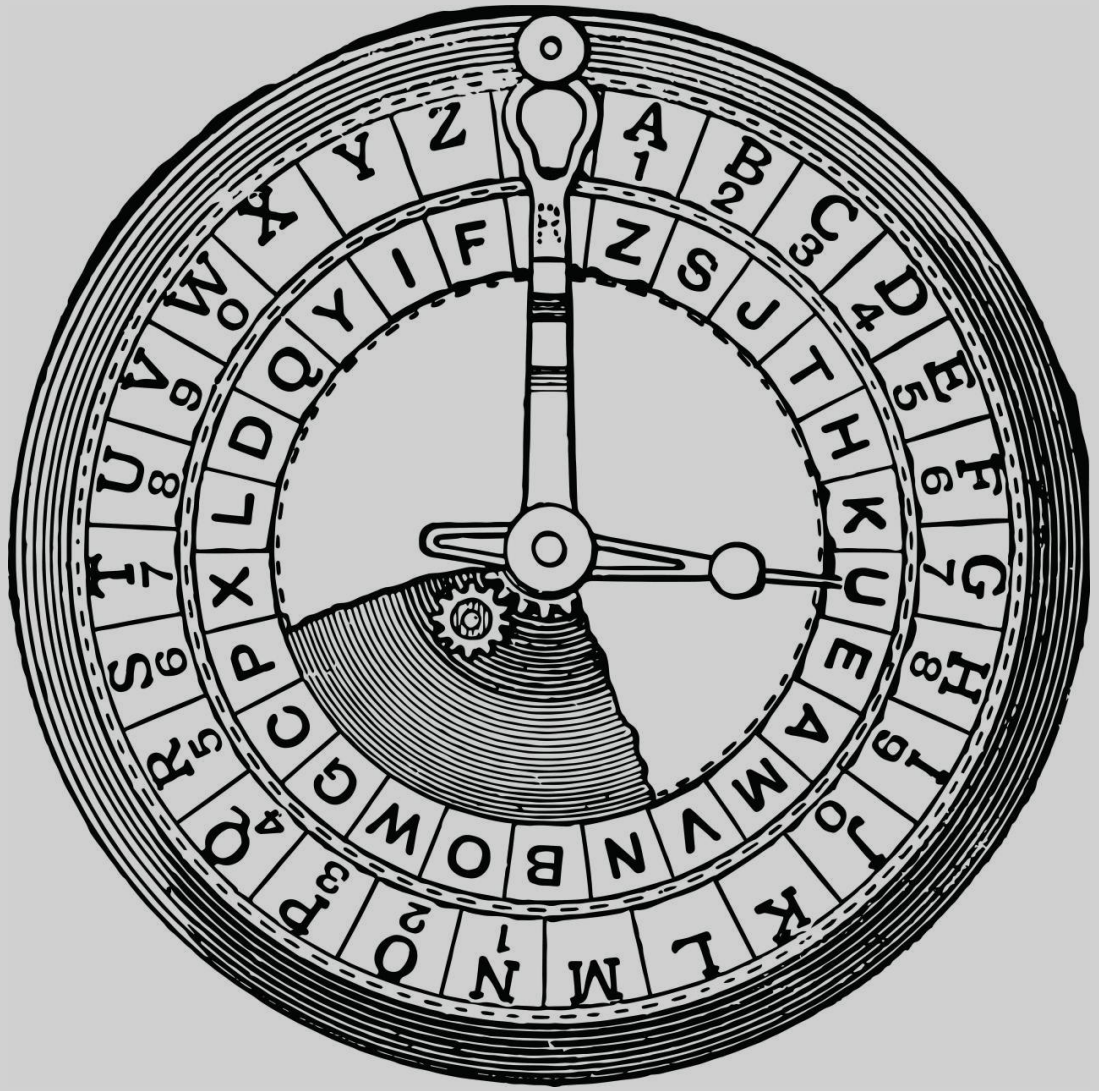
Primitivas Criptográficas



Onde terminam as reduções?

- Quero provar que Π é seguro
- Assumindo que Γ_1 é seguro, provo que Π é seguro
- Quero provar que Γ_1 é seguro
- Assumindo que Γ_2 é seguro, provo que Γ_1 é seguro
- $\vdots$
- Assumindo uma **primitiva criptográfica**, provo que Γ_i é seguro

Para fechar



Para fechar

- Hoje
  - Provas de segurança
  - Reduções
    - Exemplo de redução entre protocolos criptográficos
- Próximas aulas
  - Primitivas Criptográficas
  - Construindo uma cifra a partir de primitivas criptográficas