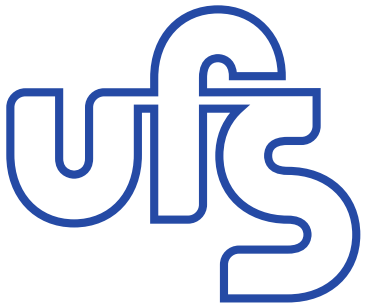
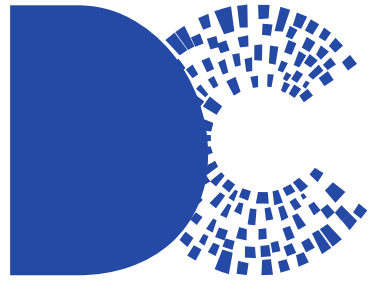




Criptografia assimétrica

Projeto e Análise de Algoritmos

Bruno Prado

Departamento de Computação / UFS

Introdução

- Contexto e história
  - A proteção de segredos de estratégicos e militares remonta à civilização egípcia a mais de 4.000 anos

Introdução

- Contexto e história
  - A proteção de segredos de estratégicos e militares remonta à civilização egípcia a mais de 4.000 anos
  - Na era da informação, com o uso massivo de sistemas computacionais e de redes de comunicação, é preciso ainda mais proteção das informações digitais

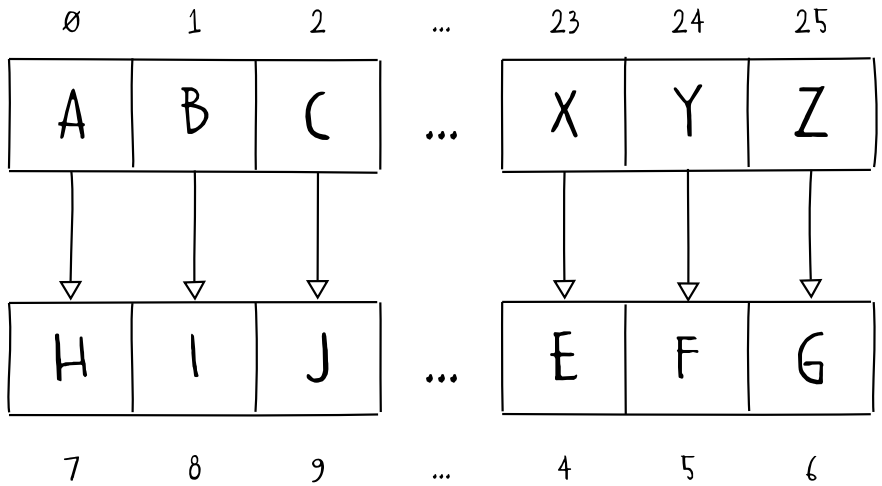
Introdução

- Contexto e história
  - A proteção de segredos de estratégicos e militares remonta à civilização egípcia a mais de 4.000 anos
  - Na era da informação, com o uso massivo de sistemas computacionais e de redes de comunicação, é preciso ainda mais proteção das informações digitais

$$\textit{Cripto} \longleftrightarrow \textit{Escondido}$$
$$\textit{Grafia} \longleftrightarrow \textit{Escrita}$$

Introdução

- Criptografia do imperador Júlio César

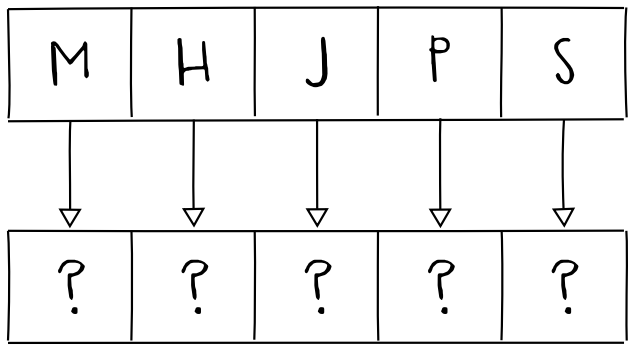


$$E_D(M) = (M_1 + D) \bmod 26 = C$$

$$D_D(C) = (C_1 - D) \bmod 26 = M$$

Introdução

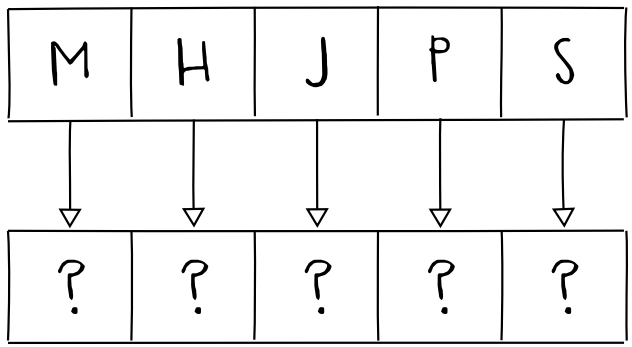
- Criptografia do imperador Júlio César



Quantos passos são necessários
para decifrar este código por força bruta?

Introdução

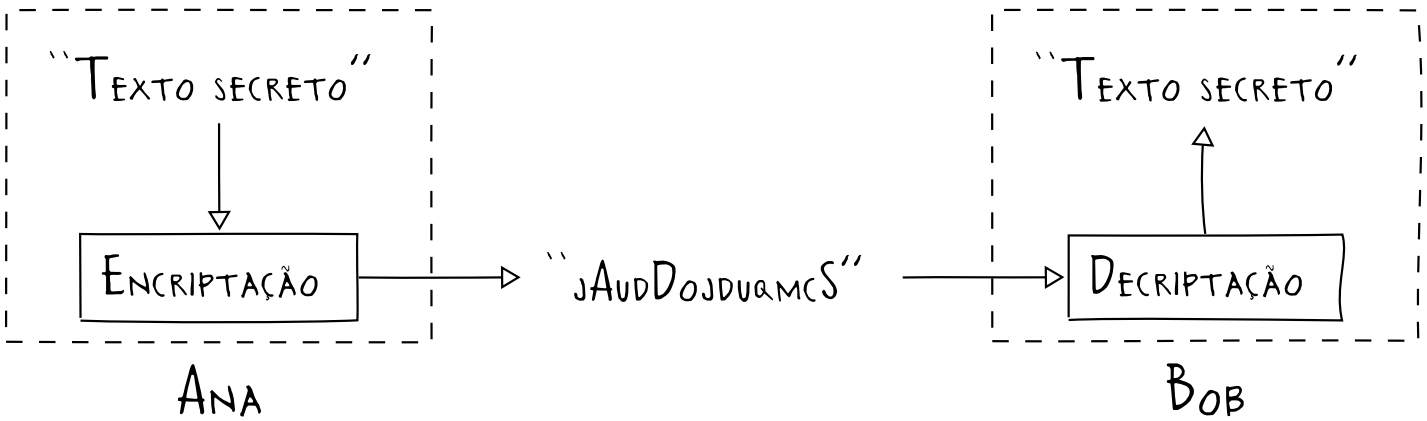
- Criptografia do imperador Júlio César



E se os mapeamentos fossem
gerados a partir de uma permutação?

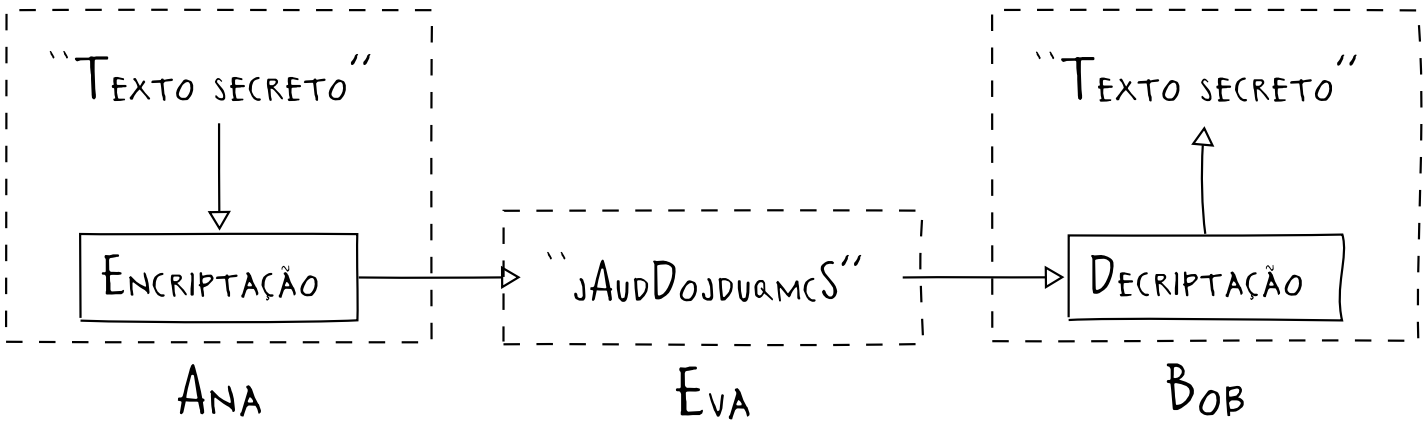
Introdução

- Cenário de funcionamento
  - Comunicação entre terceiros
  - Canal de comunicação inseguro



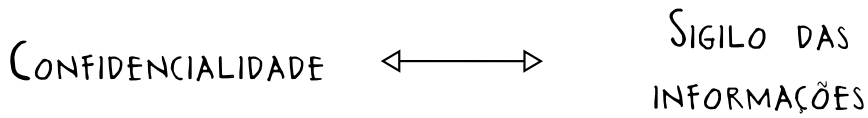
Introdução

- Cenário de funcionamento
  - Comunicação entre terceiros
  - Canal de comunicação inseguro



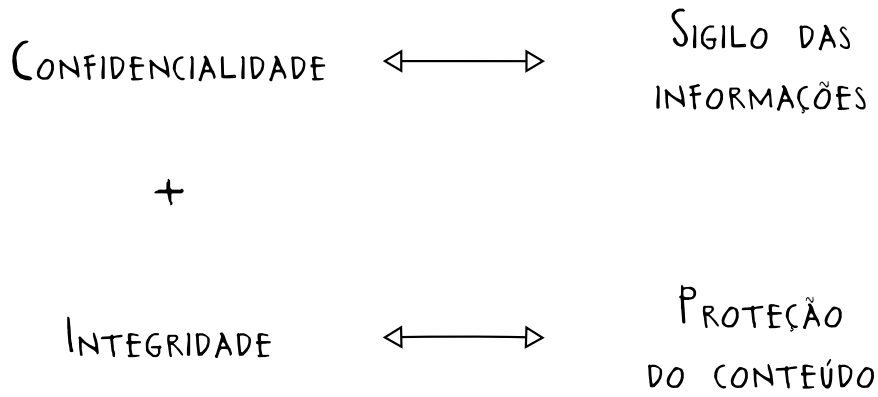
Introdução

- O que é criptografia em sistemas?
  - É a aplicação de técnicas matemáticas para proporcionar segurança da informação



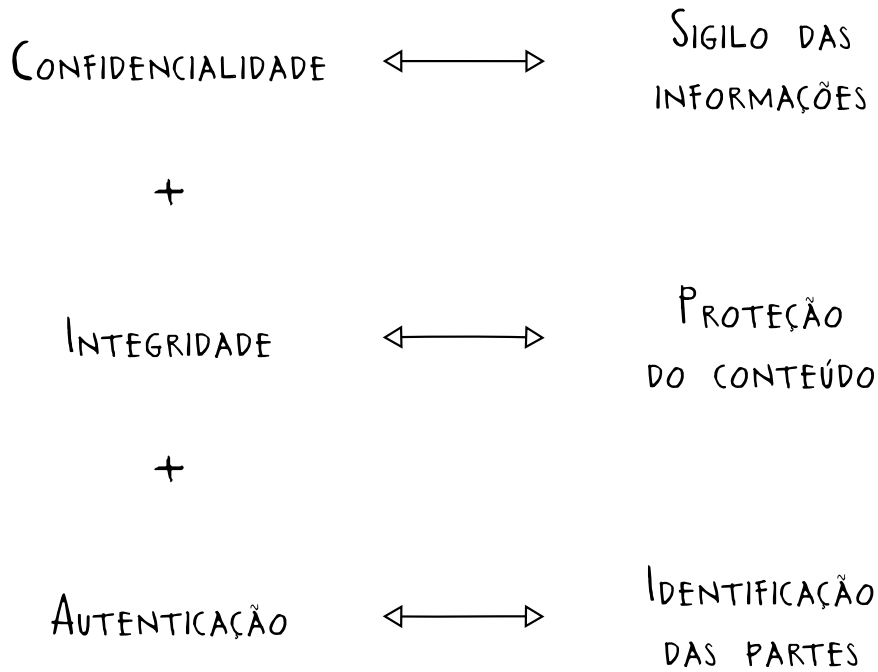
Introdução

- O que é criptografia em sistemas?
  - É a aplicação de técnicas matemáticas para proporcionar segurança da informação



Introdução

- O que é criptografia em sistemas?
  - É a aplicação de técnicas matemáticas para proporcionar segurança da informação



Introdução

- O que é criptografia em sistemas?
  - É a aplicação de técnicas matemáticas para proporcionar segurança da informação

Introdução

- Função de mão única: é uma função bijetora com baixo custo computacional para gerar os resultados, entretanto, é difícil reverter o resultado, com o objetivo de determinar quais foram as entradas utilizadas
  - Multiplicação dos números primos $z = x \times y$ é $O\left(n^2\right)$
  - Fatoração do número z para obter x e y é $O\left(2^n\right)$

Introdução

- Função de mão única: é uma função bijetora com baixo custo computacional para gerar os resultados, entretanto, é difícil reverter o resultado, com o objetivo de determinar quais foram as entradas utilizadas
  - Multiplicação dos números primos $z = x \times y$ é $O\left(n^2\right)$
  - Fatoração do número z para obter x e y é $O\left(2^n\right)$

$$\begin{aligned} f(x,y) &= Multiplicação(x,y) &= z \\ f^{-1}(z) &= Fatoração(z) &= x,y \end{aligned}$$

Introdução

- Função de mão única: é uma função bijetora com baixo custo computacional para gerar os resultados, entretanto, é difícil reverter o resultado, com o objetivo de determinar quais foram as entradas utilizadas
  - Multiplicação dos números primos $z = x \times y$ é $O\left(n^2\right)$
  - Fatoração do número z para obter x e y é $O\left(2^n\right)$

$$\begin{aligned} f(x,y) &= \mathit{Multiplicação}(x,y) &&= z \\ f^{-1}(z) &= \mathit{Fatoração}(z) &&= x, y \end{aligned}$$

$$\uparrow \mathit{Custo\ problema} \quad \longleftrightarrow \quad \uparrow \mathit{Segurança\ da\ criptografia}$$

Introdução

- Métricas de avaliação da criptografia
  - Nível de segurança: como é de difícil quantificação, uma boa estratégia é medir a quantidade de passos necessários para resolver o problema em questão

Introdução

- Métricas de avaliação da criptografia
  - Nível de segurança: como é de difícil quantificação, uma boa estratégia é medir a quantidade de passos necessários para resolver o problema em questão
  - Desempenho: avalia a eficiência de espaço e de tempo para encriptação dos dados originais, verificando o aumento do volume de dados e a taxa de processamento do algoritmo

Introdução

- Métricas de avaliação da criptografia
  - Nível de segurança: como é de difícil quantificação, uma boa estratégia é medir a quantidade de passos necessários para resolver o problema em questão
  - Desempenho: avalia a eficiência de espaço e de tempo para encriptação dos dados originais, verificando o aumento do volume de dados e a taxa de processamento do algoritmo
  - Implementação: consiste em verificar a viabilidade prática de implementação de uma solução, utilizando componentes de hardware ou software

Introdução

- Criptografia perfeita (*one-time pad*)
  - Durante a segunda guerra mundial, Claude E. Shannon formalizou o conceito de segredo perfeito, demonstrando que é impossível decifrar uma mensagem cifrada c que não oferece nenhuma informação sobre a mensagem original m

Introdução

- Criptografia perfeita (*one-time pad*)
  - Durante a segunda guerra mundial, Claude E. Shannon formalizou o conceito de segredo perfeito, demonstrando que é impossível decifrar uma mensagem cifrada c que não oferece nenhuma informação sobre a mensagem original m
  - Esta definição requer que para um conjunto de mensagens M, as probabilidades de se obterem a mesma mensagem cifrada c, utilizando um conjunto de chaves perfeitamente aleatórias K, sejam iguais

Introdução

- Criptografia perfeita (*one-time pad*)
  - Durante a segunda guerra mundial, Claude E. Shannon formalizou o conceito de segredo perfeito, demonstrando que é impossível decifrar uma mensagem cifrada c que não oferece nenhuma informação sobre a mensagem original m
  - Esta definição requer que para um conjunto de mensagens M, as probabilidades de se obterem a mesma mensagem cifrada c, utilizando um conjunto de chaves perfeitamente aleatórias K, sejam iguais

$$\begin{aligned} M &= \{0,1\}^n \\ K &= \{0,1\}^n \end{aligned}$$

Introdução

- Criptografia perfeita (*one-time pad*)
  - Durante a segunda guerra mundial, Claude E. Shannon formalizou o conceito de segredo perfeito, demonstrando que é impossível decifrar uma mensagem cifrada c que não oferece nenhuma informação sobre a mensagem original m
  - Esta definição requer que para um conjunto de mensagens M, as probabilidades de se obterem a mesma mensagem cifrada c, utilizando um conjunto de chaves perfeitamente aleatórias K, sejam iguais

$$\begin{aligned} M &= \{0,1\}^n \\ K &= \{0,1\}^n \\ E_k\left(m = m_0 m_1 \ldots m_{n-1}\right) &= c_0 c_1 \ldots c_{n-1}, \quad c_i = m_i \oplus k_i \\ D_k\left(c = c_0 c_1 \ldots c_{n-1}\right) &= m_0 m_1 \ldots m_{n-1}, \quad m_i = c_i \oplus k_i \end{aligned}$$

Introdução

- Criptografia perfeita (*one-time pad*)
  - Durante a segunda guerra mundial, Claude E. Shannon formalizou o conceito de segredo perfeito, demonstrando que é impossível decifrar uma mensagem cifrada c que não oferece nenhuma informação sobre a mensagem original m
  - Esta definição requer que para um conjunto de mensagens M, as probabilidades de se obterem a mesma mensagem cifrada c, utilizando um conjunto de chaves perfeitamente aleatórias K, sejam iguais

$$
\begin{aligned}
M &= \{0,1\}^n \\
K &= \{0,1\}^n \\
E_k\left(m = m_0 m_1 \ldots m_{n-1}\right) &= c_0 c_1 \ldots c_{n-1}, \quad c_i = m_i \oplus k_i \\
D_k\left(c = c_0 c_1 \ldots c_{n-1}\right) &= m_0 m_1 \ldots m_{n-1}, \quad m_i = c_i \oplus k_i \\
&\downarrow \\
|K| &\geq |M|
\end{aligned}
$$

Introdução

- Por que uma técnica de criptografia com segurança perfeita não é amplamente utilizada?

Introdução

- Por que uma técnica de criptografia com segurança perfeita não é amplamente utilizada?
  - É exigida a geração de chaves perfeitamente aleatórias, ou seja, sem padrões ou repetições para cada mensagem

Introdução

- Por que uma técnica de criptografia com segurança perfeita não é amplamente utilizada?
  - É exigida a geração de chaves perfeitamente aleatórias, ou seja, sem padrões ou repetições para cada mensagem
  - As chaves geradas precisam ter pelo menos o tamanho da mensagem original, para atender o requisito de não repetição da chave

Introdução

- Por que uma técnica de criptografia com segurança perfeita não é amplamente utilizada?
  - É exigida a geração de chaves perfeitamente aleatórias, ou seja, sem padrões ou repetições para cada mensagem
  - As chaves geradas precisam ter pelo menos o tamanho da mensagem original, para atender o requisito de não repetição da chave
  - Todas as informações precisam ser protegidas e previamente distribuídas entre as partes, evitando reuso parcial ou total das informações

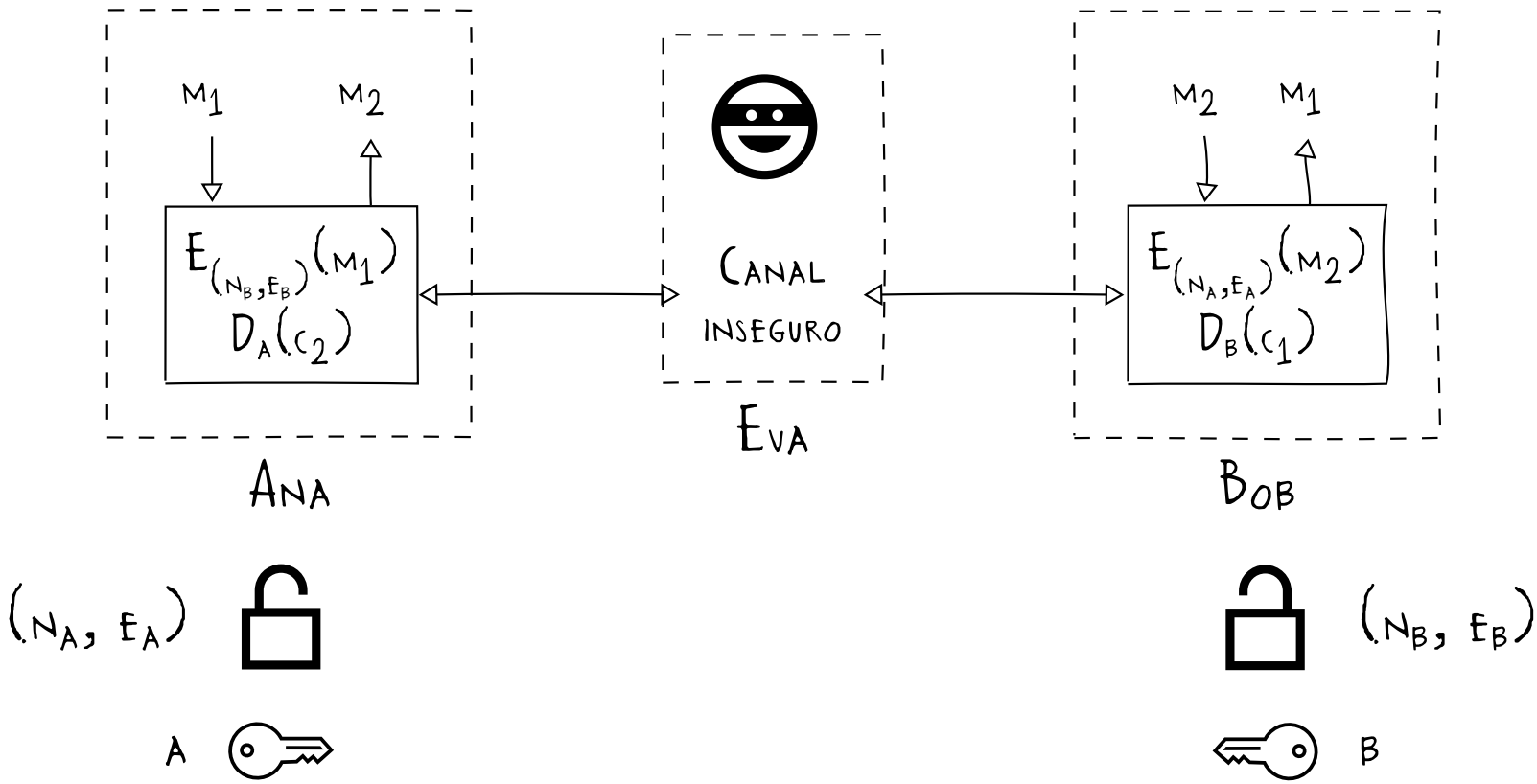
Introdução

- Por que uma técnica de criptografia com segurança perfeita não é amplamente utilizada?
  - É exigida a geração de chaves perfeitamente aleatórias, ou seja, sem padrões ou repetições para cada mensagem
  - As chaves geradas precisam ter pelo menos o tamanho da mensagem original, para atender o requisito de não repetição da chave
  - Todas as informações precisam ser protegidas e previamente distribuídas entre as partes, evitando reuso parcial ou total das informações

Só é utilizada em aplicações onde
a segurança da informação é muito crítica

Criptografia assimétrica

- Rivest-Shamir-Adleman (RSA)
  - Utiliza chaves privadas para decriptação e públicas para encriptação das mensagens



Criptografia assimétrica

- Rivest-Shamir-Adleman (RSA)
  - A criptografia de chave pública RSA é baseada no problema intratável de fatoração de números, gerando uma chave pública n através da multiplicação de dois números primos p e q, que precisam ser distintos e suficientemente grandes

Criptografia assimétrica

- Rivest-Shamir-Adleman (RSA)
  - A criptografia de chave pública RSA é baseada no problema intratável de fatoração de números, gerando uma chave pública n através da multiplicação de dois números primos p e q, que precisam ser distintos e suficientemente grandes
  - A chave pública (n, e) é obtida por $n = (p-1) \times (q-1)$ e pela geração de um número aleatório e ímpar e tal que $1 < e \leq n$ e $mdc\,(e, n) = 1$

Criptografia assimétrica

- Rivest-Shamir-Adleman (RSA)
  - A criptografia de chave pública RSA é baseada no problema intratável de fatoração de números, gerando uma chave pública n através da multiplicação de dois números primos p e q, que precisam ser distintos e suficientemente grandes
  - A chave pública (n, e) é obtida por $n = (p-1) \times (q-1)$ e pela geração de um número aleatório e ímpar e tal que $1 < e \leq n$ e $mdc\,(e, n) = 1$
  - Através da aplicação do inverso multiplicativo, chave privada d é gerada, onde $1 < d \leq n$ e $e \times d \equiv 1 \bmod n$

Criptografia assimétrica

- Rivest-Shamir-Adleman (RSA)
  - A encriptação utiliza a chave pública (n, e) e a mensagem m fornecidas, calculando $c = m^e \bmod n$
  - A mensagem c é decriptada aplicando a chave privada d em $m = c^d \bmod n$ para obter m

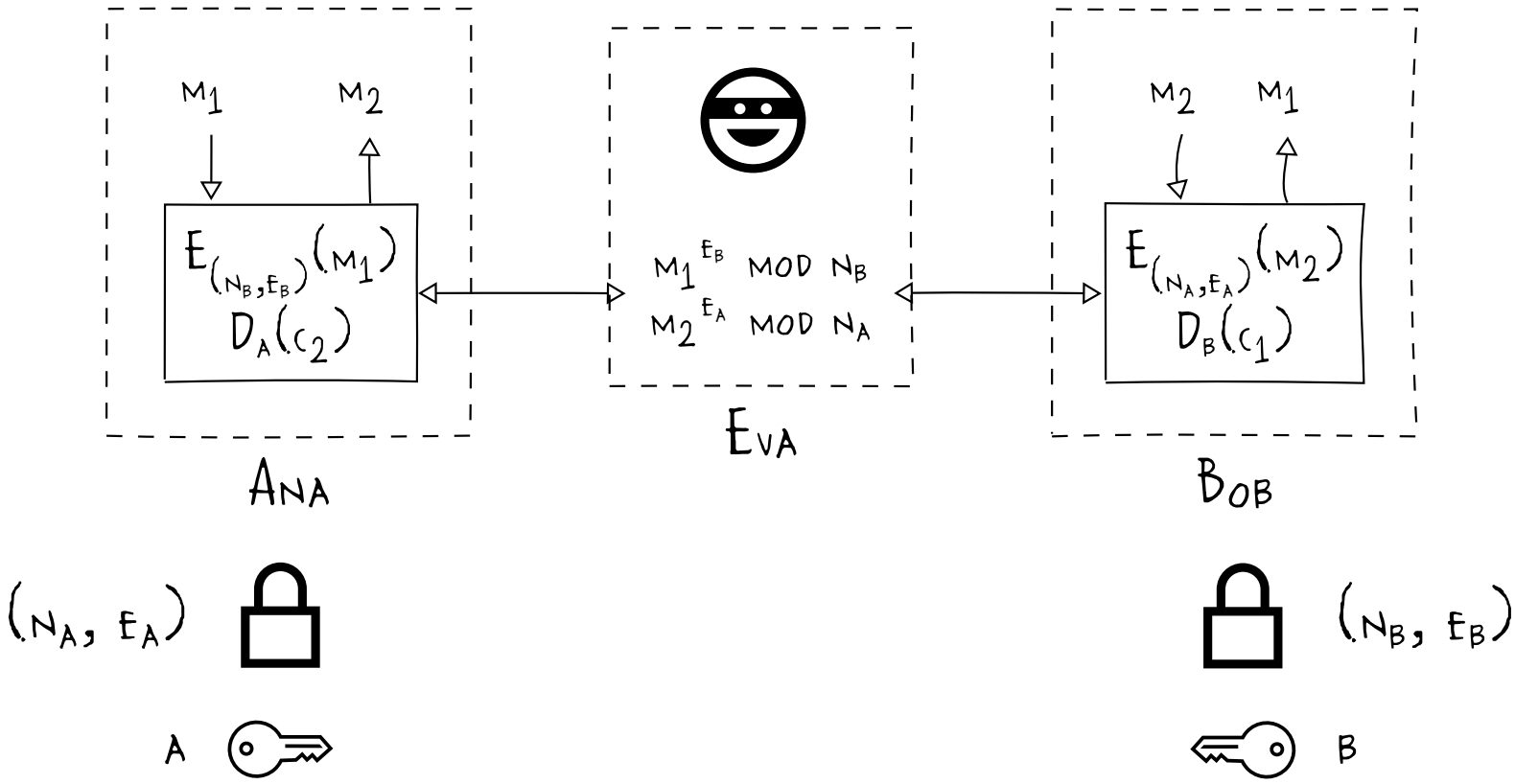
Criptografia assimétrica

- Rivest-Shamir-Adleman (RSA)
  - A encriptação utiliza a chave pública (n, e) e a mensagem m fornecidas, calculando $c = m^e \bmod n$
  - A mensagem c é decriptada aplicando a chave privada d em $m = c^d \bmod n$ para obter m

$$c^d \equiv \left(m^e\right)^d \equiv m \bmod n$$

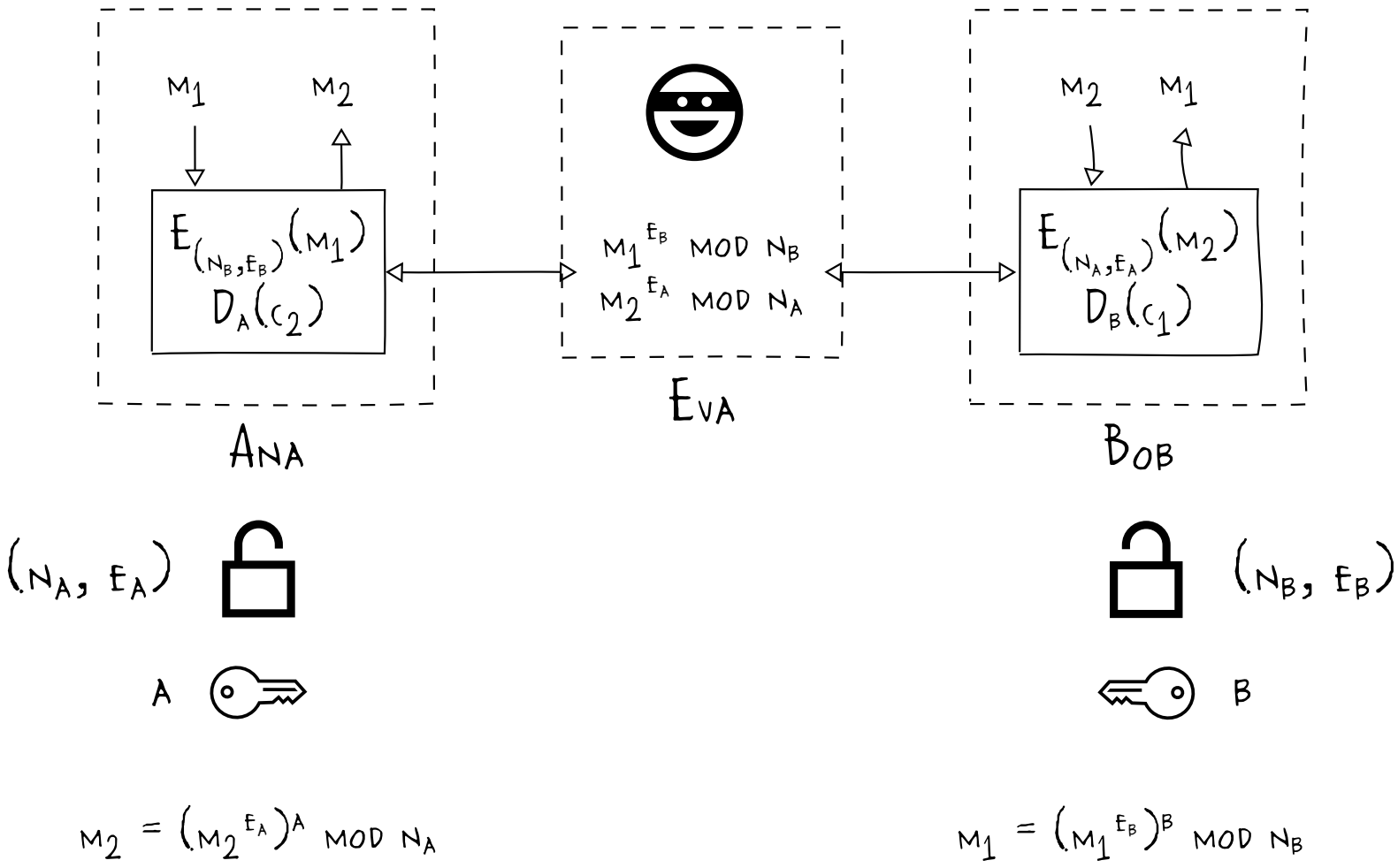
Criptografia assimétrica

- Rivest-Shamir-Adleman (RSA)



Criptografia assimétrica

- Rivest-Shamir-Adleman (RSA)



Criptografia assimétrica

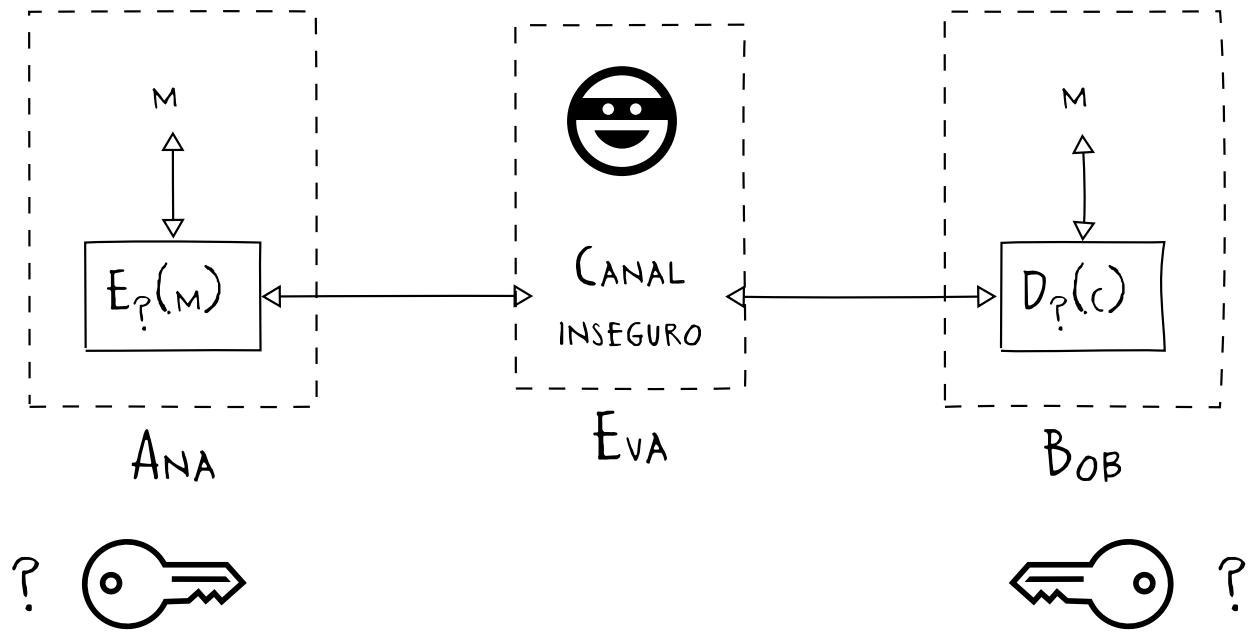
- Rivest-Shamir-Adleman (RSA)
  - Permite a autenticação das partes, uma vez que as chaves públicas são seguras e só podem ser decriptadas com a chave privada do proprietário

Criptografia assimétrica

- Rivest-Shamir-Adleman (RSA)
  - Permite a autenticação das partes, uma vez que as chaves públicas são seguras e só podem ser decriptadas com a chave privada do proprietário
  - Apresenta um custo computacional mais elevado, em comparação aos algoritmos de criptografia simétricos, por demandar chaves com pelo menos 2.048 bits para ser considerado seguro

Criptografia assimétrica

- Como compartilhar uma chave privada entre as partes quando não existe um canal seguro?



Criptografia assimétrica

- Compartilhamento de chaves com Diffie-Hellman
  - É baseado no problema intratável do logaritmo discreto, ou seja, ainda não existe nenhum algoritmo computacionalmente eficiente para sua resolução

Criptografia assimétrica

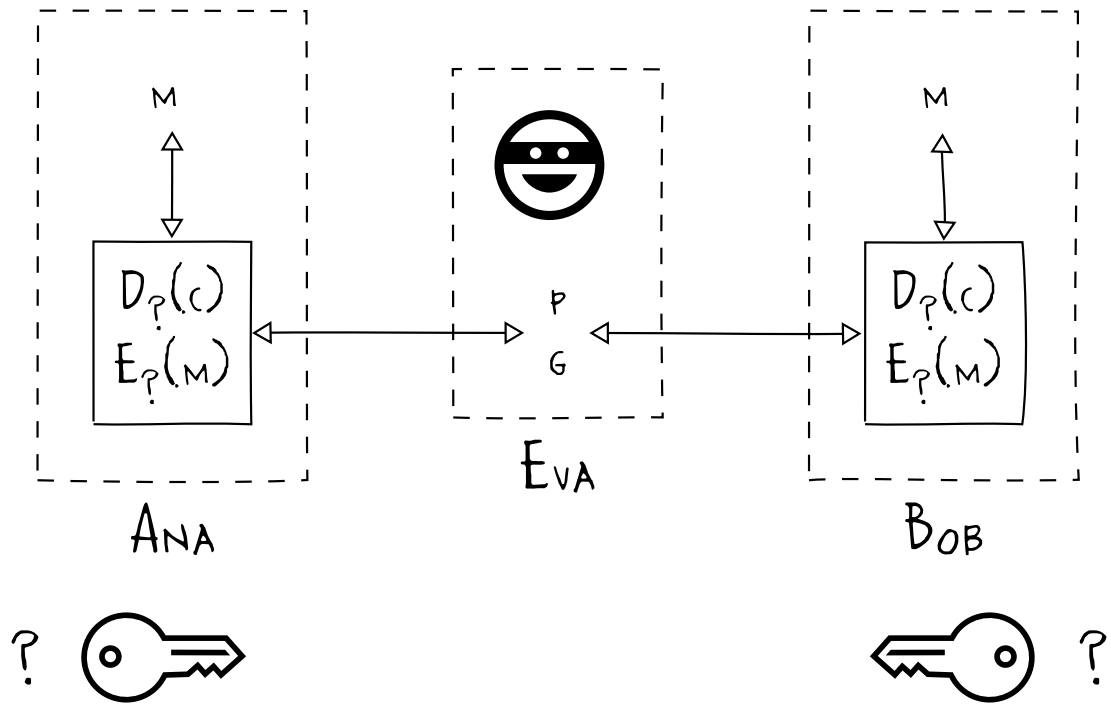
- Compartilhamento de chaves com Diffie-Hellman
  - É baseado no problema intratável do logaritmo discreto, ou seja, ainda não existe nenhum algoritmo computacionalmente eficiente para sua resolução
  - O cálculo da exponenciação b^n é rapidamente obtida com complexidade de $O\left(n^2 \log n\right)$

Criptografia assimétrica

- Compartilhamento de chaves com Diffie-Hellman
  - É baseado no problema intratável do logaritmo discreto, ou seja, ainda não existe nenhum algoritmo computacionalmente eficiente para sua resolução
  - O cálculo da exponenciação b^n é rapidamente obtida com complexidade de $O\left(n^2 \log n\right)$
  - Entretanto, para se obter o número n a partir de b^n, é preciso calcular o logaritmo discreto $\log_b b^n = n$ que possui complexidade exponencial $O\left(2^n\right)$

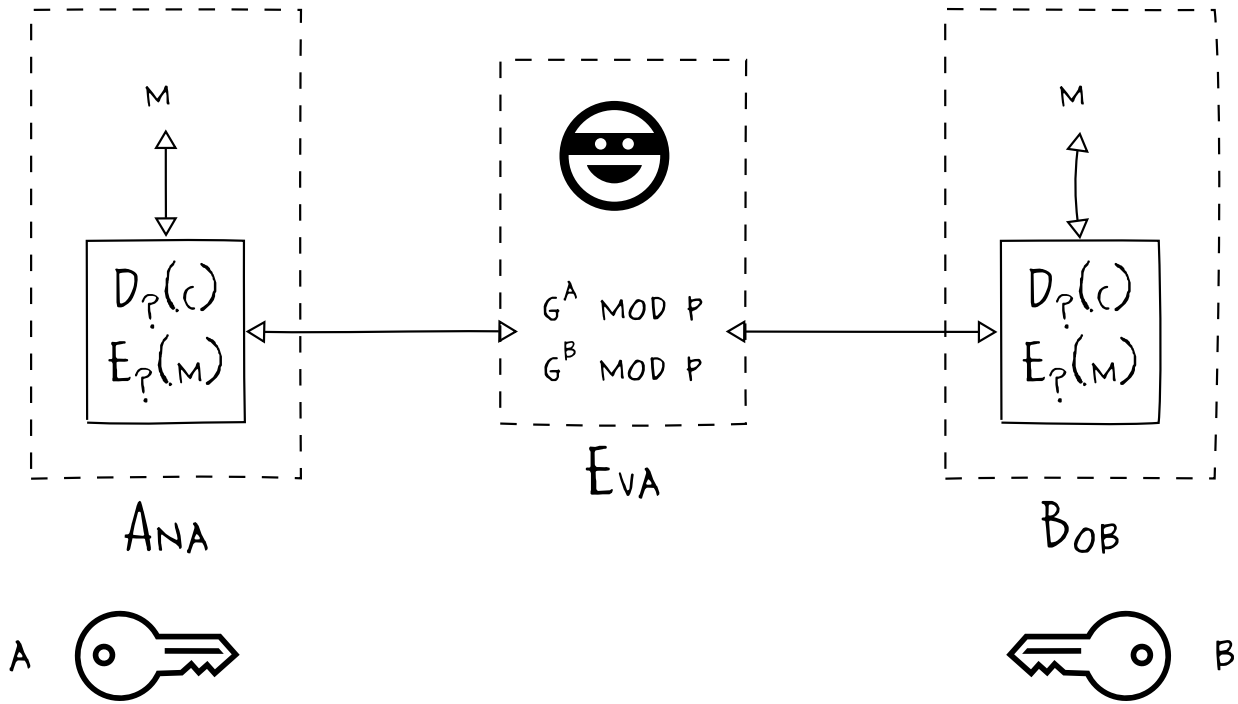
Criptografia assimétrica

- Compartilhamento de chaves com Diffie-Hellman
  - Ana e Bob não se conhecem, mas concordam em utilizar uma base *g* e o número primo *p*, ambos públicos e transmitidos pelo canal inseguro



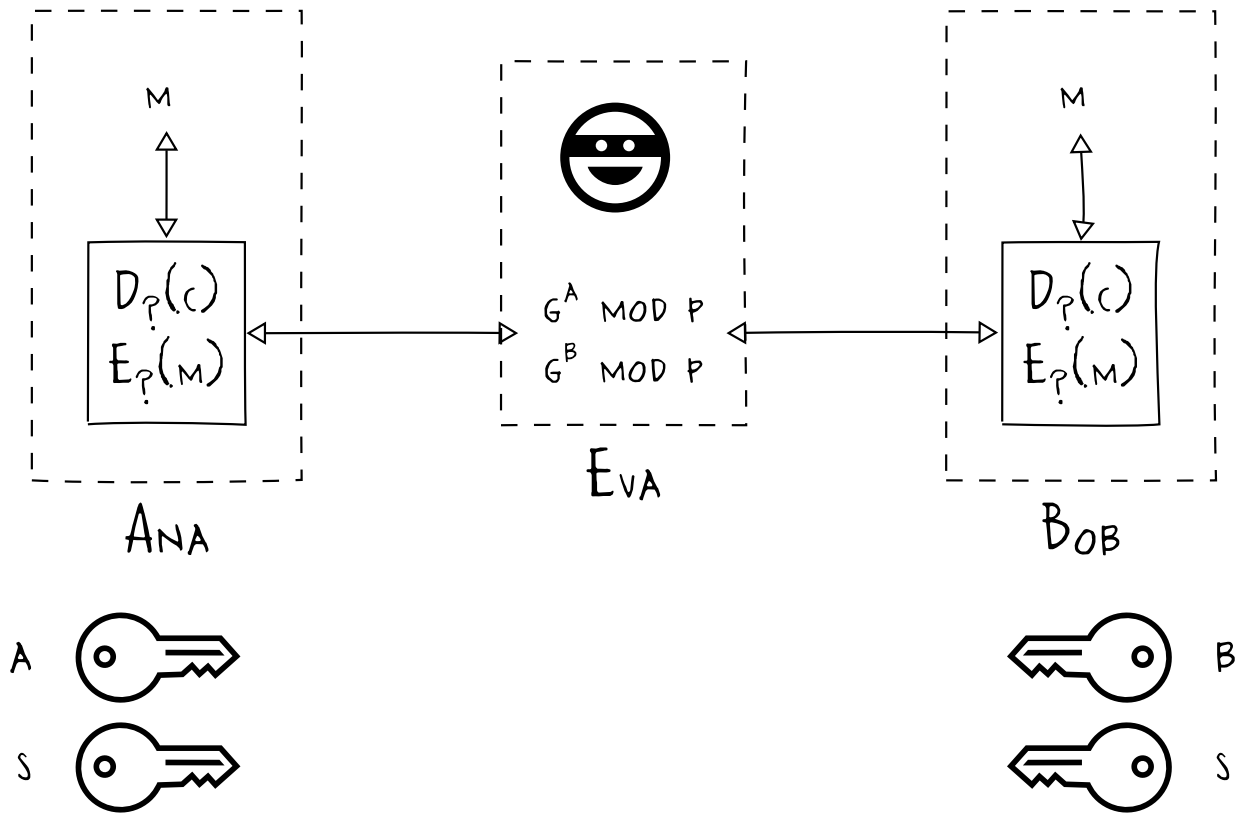
Criptografia assimétrica

- Compartilhamento de chaves com Diffie-Hellman
  - Utilizando suas próprias chaves privadas, Ana envia para Bob $g^a \bmod p$ e Bob envia para Ana $g^b \bmod p$



Criptografia assimétrica

- Compartilhamento de chaves com Diffie-Hellman
  - A chave compartilhada s é gerada por Ana $s = \left(g^b\right)^a \bmod p$ e por Bob $s = (g^a)^b \bmod p$



Criptografia assimétrica

- Compartilhamento de chaves com Diffie-Hellman
  - Para que a atacante Eva seja capaz de obter o valor da chave privada compartilhada s, é preciso resolver eficientemente o problema do logaritmo discreto

Criptografia assimétrica

- Compartilhamento de chaves com Diffie-Hellman
  - Para que a atacante Eva seja capaz de obter o valor da chave privada compartilhada *s*, é preciso resolver eficientemente o problema do logaritmo discreto
  - Devem ser utilizados números primos de tamanho grande, com pelo menos 2.048 bits, para dificultar a recuperação das chaves privadas *a* ou *b*

Criptografia assimétrica

- Compartilhamento de chaves com Diffie-Hellman
  - Para que a atacante Eva seja capaz de obter o valor da chave privada compartilhada *s*, é preciso resolver eficientemente o problema do logaritmo discreto
  - Devem ser utilizados números primos de tamanho grande, com pelo menos 2.048 bits, para dificultar a recuperação das chaves privadas *a* ou *b*
  - Esta técnica de troca de chave é vulnerável ao ataque do homem do meio e pode ser evitado com autenticação das partes envolvidas

Criptografia assimétrica

- Compartilhamento de chaves com Diffie-Hellman
  - Para que a atacante Eva seja capaz de obter o valor da chave privada compartilhada *s*, é preciso resolver eficientemente o problema do logaritmo discreto
  - Devem ser utilizados números primos de tamanho grande, com pelo menos 2.048 bits, para dificultar a recuperação das chaves privadas *a* ou *b*
  - Esta técnica de troca de chave é vulnerável ao ataque do homem do meio e pode ser evitado com autenticação das partes envolvidas

Pode ser utilizado no compartilhamento seguro de chaves privadas em algoritmos de criptografia simétricos