SEGURANÇA DA INFORMAÇÃO

Criptografia Assimétrica

ROTEIRO

- Limitações da criptografia simétrica
- Criptografia assimétrica
- Algoritmos de criptografia assimétrica
- Vantagens e desvantagens

LIMITAÇÕES DA CRIPTOGRAFIA SIMÉTRICA

- Na criptografia de chave simétrica, a mesma chave é usada pelo remetente (para criptografia) e pelo receptor (para descriptografia).

- A chave é compartilhada.

  - Exemplos de algoritmo: DES, 3DES

LIMITAÇÕES DA CRIPTOGRAFIA ASSIMÉTRICA

Vantagens

- Simples e rápida

Desvantagem

- as chaves precisam ser trocadas em um canal seguro
- Um atacante pode facilmente interceptar e obter a chave

CRIPTOGRAFIA ASSIMÉTRICA

- **Usa um par de chaves para criptografia**
  - Chave pública para criptografia
  - Chave privada para descriptografia
- **As mensagens codificadas usando a chave pública só podem ser decodificadas pela chave privada**
- **A transmissão secreta da chave para descriptografia não é necessária**
- **Cada entidade pode gerar um par de chaves e liberar sua chave pública**
- **Usuários obtém a chave de uma autoridade certificadora**

CRIPTOGRAFIA ASSIMÉTRICA

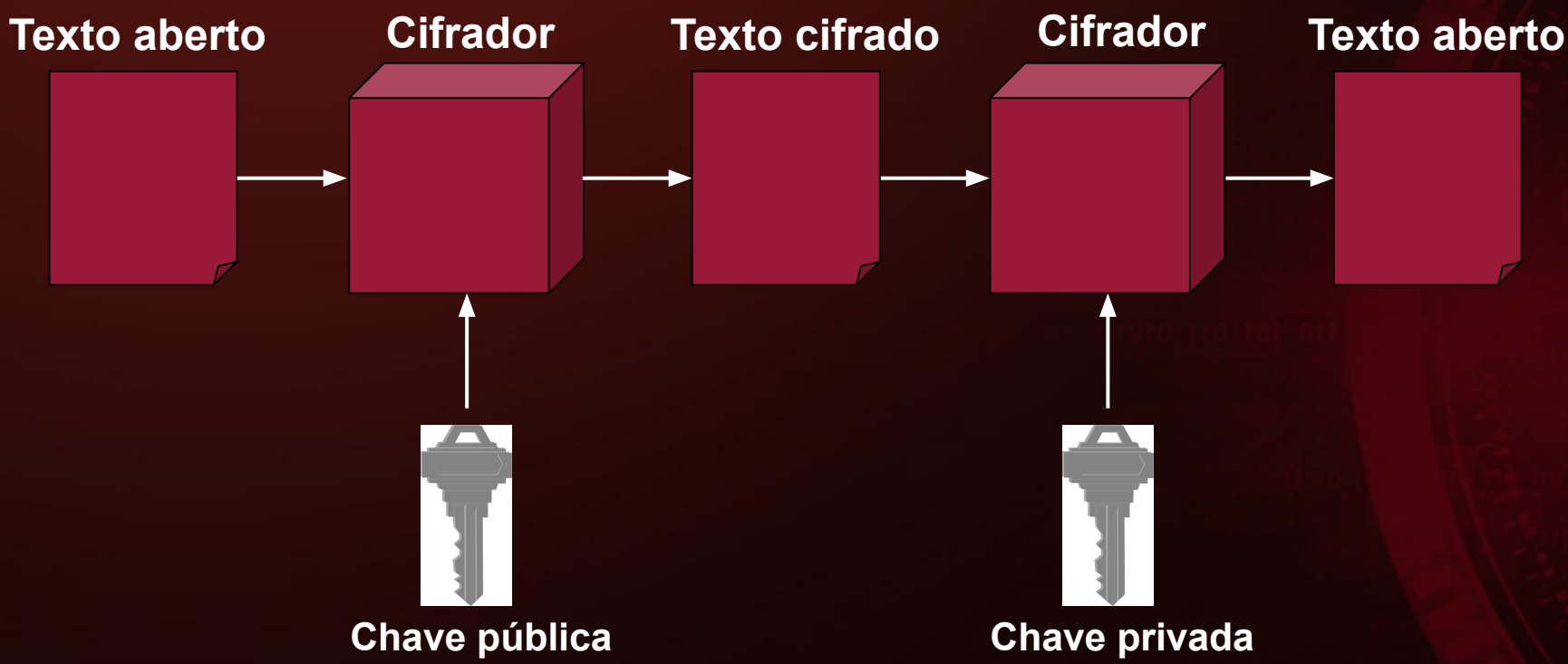
- **Essas chaves são geradas juntas**

- **A chave pública é distribuída gratuitamente.**
  - Ela encripta/descriptografa o dado

- **A chave privada é mantida em segredo**
  - Ela decripta/descriptogra o dado

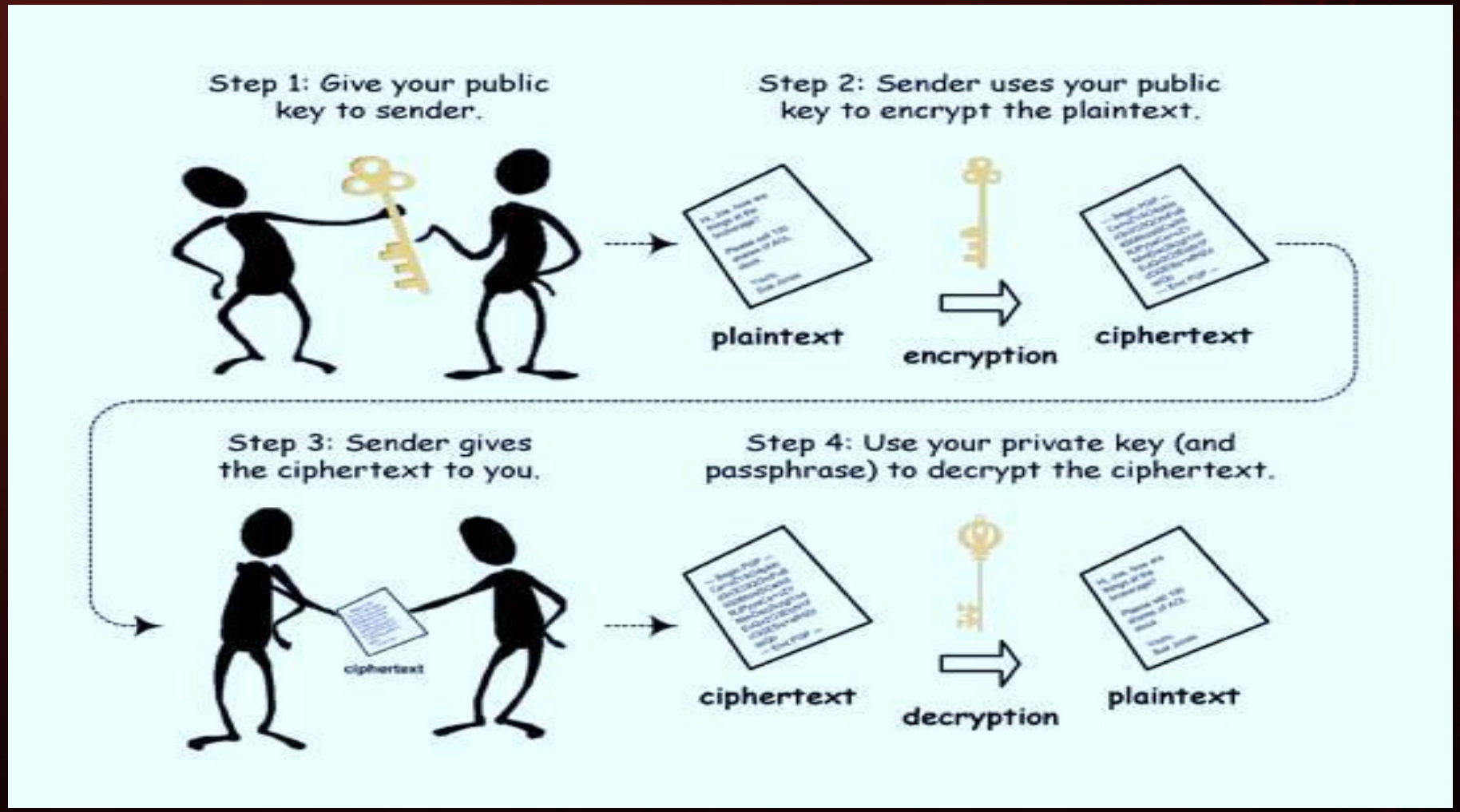
- **Tanto o emissor quanto o receptor devem compartilhar suas chaves públicas para criptografar e devem usar suas chaves privadas para descriptografar**

CRIPTOGRAFIA ASSIMÉTRICA



Fonte: 2

CRIPTOGRAFIA ASSIMÉTRICA



Fonte: 3

ALGORITMOS DE CRIPTOGRAFIA ASSIMÉTRICA

- **RSA e El Gamal são dois dos algoritmos mais populares**

RSA

- Desenvolvido por Ron Rivest, Adi Shamir e Len Adelman
- As chaves pública e privada são intercambiáveis
- Tamanho variável da chave (512, 1024 ou 2048 bits)
- Algoritmo de chave pública mais popular

El Gamal

- Desenvolvido por Taher ElGamal
- Tamanho de chave variável (512 ou 1024 bits)
- Menos comum que RSA, usado em protocolos como PGP

ALGORITMOS DE CRIPTOGRAFIA ASSIMÉTRICA

- **Funcionamento do RSA**

- Escolha dois números primos grandes p & q
- Calcule n=pq e z=(p-1)(q-1)
- Escolha o número e, menor que n, que não tem fator comum (além de 1) com z
- Encontre o número d, tal que ed – 1 seja exatamente divisível por z

ALGORITMOS DE CRIPTOGRAFIA ASSIMÉTRICA

- **Continua...**

- As chaves são geradas usando n, d, e
  - A chave pública é (n,e)
  - A chave privada é (n, d)
    - Criptografia: c = me mod n
      - m é texto simples
      - c é texto cifrado
    - Descriptografia: m = cd mod n

A chave pública é compartilhada e a chave privada está oculta

ALGORITMOS DE CRIPTOGRAFIA ASSIMÉTRICA

- **Exemplo com RSA**

- p=5 & q=7
- n=5*7=35 e z=(4)*(6) = 24
- e = 5
- d = 29 , (29x5 –1) é exatamente divisível por 24
- As chaves geradas são:
  - Chave pública: (35,5)
  - A chave privada é (35, 29)

ALGORITMOS DE CRIPTOGRAFIA ASSIMÉTRICA

- **Exemplo com RSA**

Encriptar a palavra *love* usando: $(c = m^e \bmod n)$

Texto Plano	Representação Numérica (Alfabeto)	m^e	Texto Crifrado ($c = m^e \bmod n$)
l	12	248832	17
o	15	759375	15
v	22	5153632	22
e	5	3125	10

ALGORITMOS DE CRIPTOGRAFIA ASSIMÉTRICA

- **Exemplo com RSA**

Encriptar a palavra *love* usando: $(c = m^e \bmod n)$

Texto Cifrado	c^d	$(m = m^e \bmod n)$	Texto Aberto
17	48196857210675091509141182522307200	17	l
15	12783403948858939111232757568359400	15	o
22	852643319086537701956194499721110000000	22	v
10	100000000000000000000000000000	10	e

ALGORITMOS DE CRIPTOGRAFIA ASSIMÉTRICA

- **Autenticação e não-repúdio são possíveis.**
  - Autenticação significa que você pode criptografar a mensagem com minha chave pública e somente eu posso descriptografá-la com minha chave privada.
  - Não-repúdio significa que você pode "assinar" a mensagem com sua chave privada e posso verificar se ela veio de você com sua chave pública.

ALGORITMOS DE CRIPTOGRAFIA ASSIMÉTRICA

Vantagens

- Mais segurança
- Autenticação

Desvantagens

- É mais complexa
- Processo demorado para criptografia e descriptografia

REFERÊNCIAS

1. https://www.albany.edu/~goel/classes/spring2002/msi604/
2. Criptografia e Segurança de Redes: Princípios e Práticas - Willian Stallings
3. https://www.pcpolytechnic.com/

SEGURANÇA DA INFORMAÇÃO

Criptografia Assimétrica