Criptografia de Chave Pública

Gerência e Segurança de Redes

Objetivos de Aprendizagem

- Introduzir o conceito de chaves assimétricas
- Apresentar aplicações práticas

Agenda

- Objetivos dos algoritmos assimétricos
- Princípios e Elementos
- Aplicações
- Vulnerabilidades

Objetivos

- Atacar o problema de distribuição de chaves para criptografia simétrica
- Criar um método para garantir que ambas as partes de uma comunicação, Emissor e Receptor, tenham certeza das respectivas identidades

Criptossistemas de Chave Pública

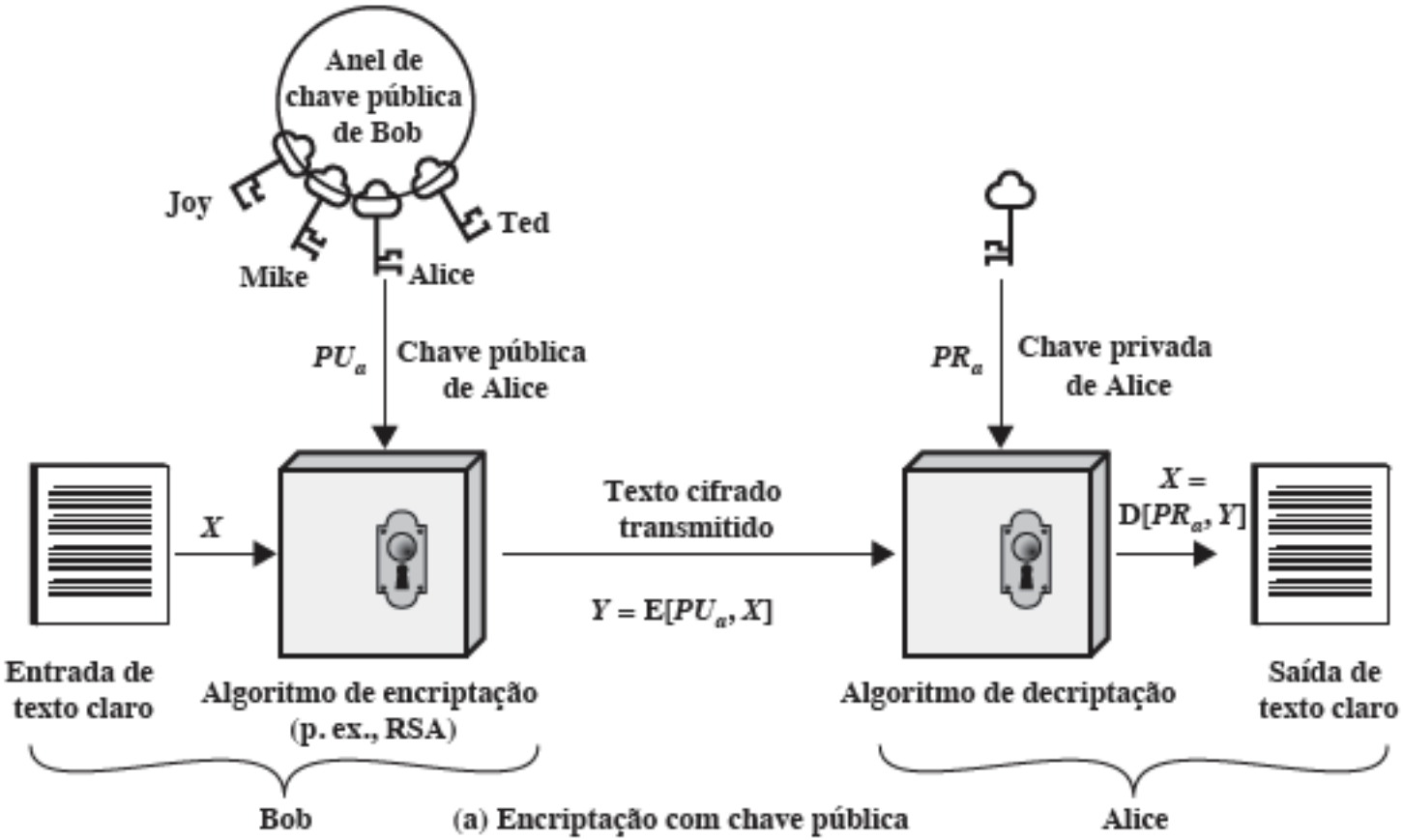
- Princípios
  - É computacionalmente inviável determinar a chave de decriptografia dado apenas o conhecimento do algoritmo e chave de criptografia
  - Qualquer uma das chaves relacionadas pode ser usada para criptografia, com outra usada para a decriptografia

Elementos

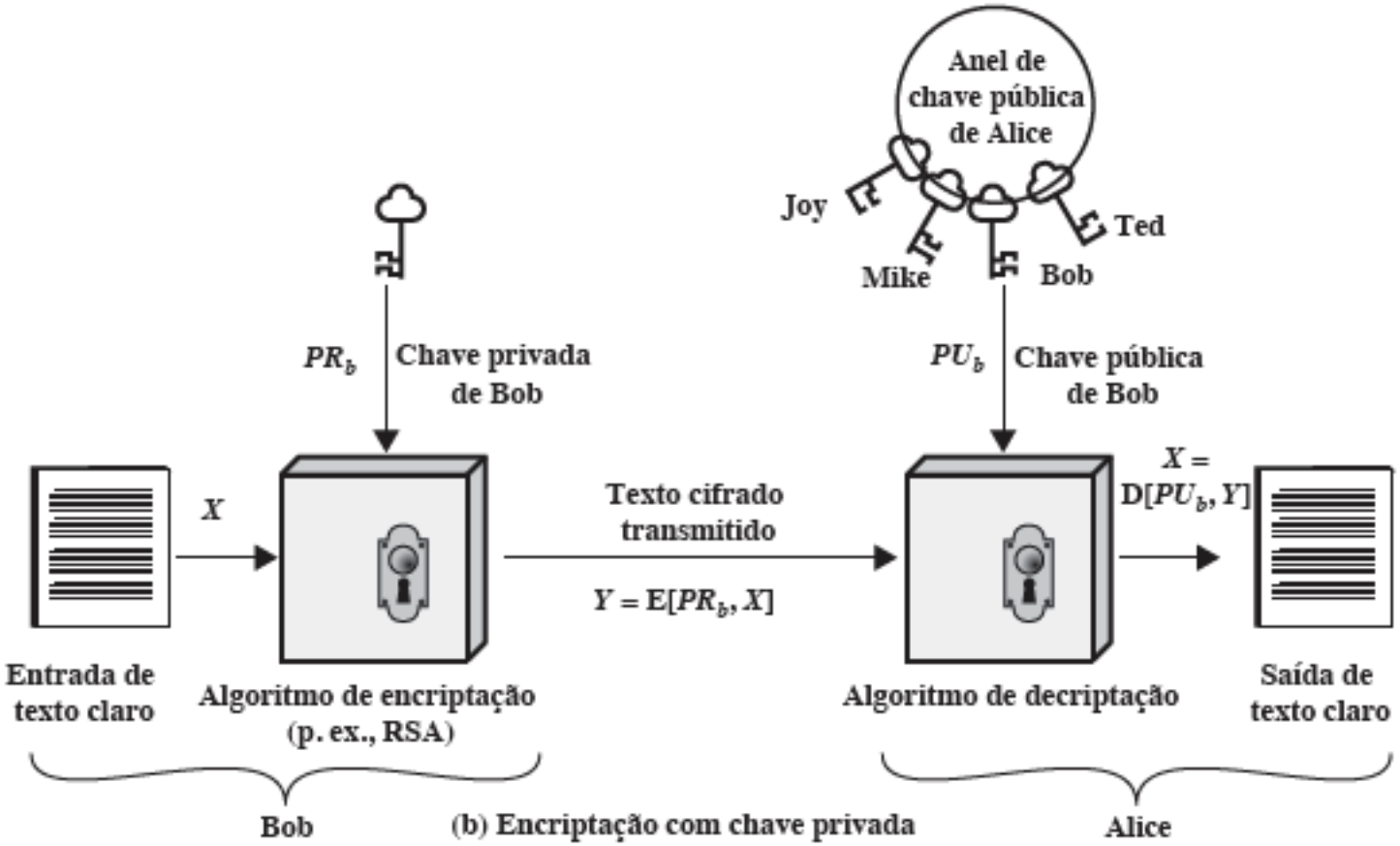
- Texto claro (mensagem)
- Algoritmo de criptografia e decriptografia
- Chaves pública e privada
- Texto cifrado

Etapas

1. Cada usuário gera um par de chaves para criptografia/decriptografia
2. Cada usuário coloca uma das chaves num repositório publicamente acessível
3. Se Bob deseja enviar mensagem para Alice, Bob criptografa a menagem usando a chave pública de Alice
4. Quando Alice recebe a mensagem, ela a decriptografa usando sua chave privada. Nenhum outro destinatário é capaz de decriptografar, pois não tem acesso a chave privada



(a) Encriptação com chave pública



(b) Encriptação com chave privada

Criptografia Assimétrica x Simétrica

Simétrica

(Convencional)

- Algoritmo + chave única para criptografia e decriptografia
- Compartilhamento de chave
- Chave deve permanecer secreta
- Deverá ser impossível decifrar uma mensagem sem informações adicionais
- O conhecimento do algoritmo e amostras de texto cifrado não deve ser suficiente para determinar a chave

Assimétrica

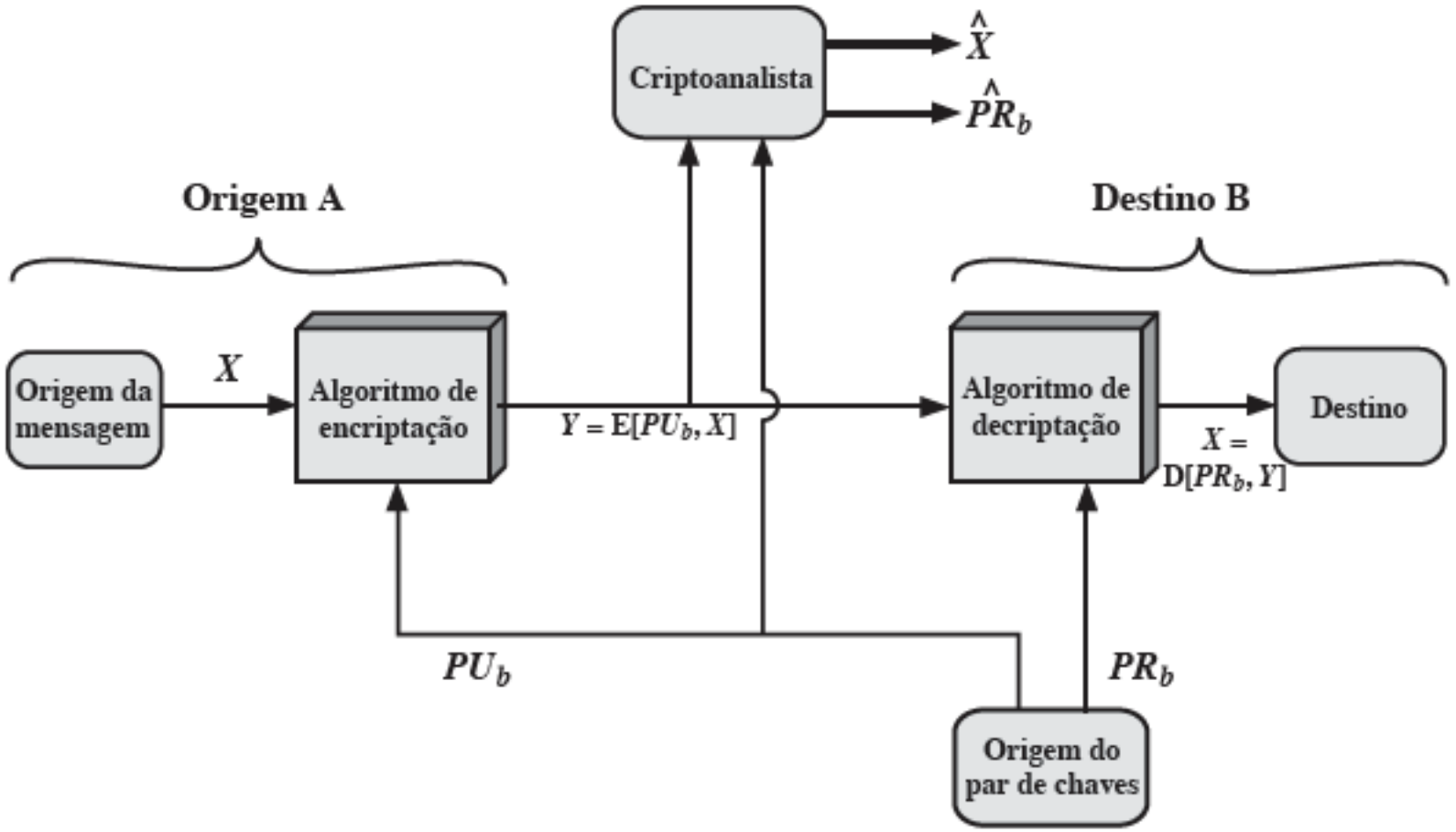
(Chaves pública e privada)

- Algoritmo + par de chaves distintas para criptografia e decriptografia
- Emissor e receptor precisam ter apenas uma das chaves do par
- Uma das chaves permance secreta
- Deverá ser impossível decifrar uma mensagem sem informações adicionais
- O conhecimento do algoritmo, amostras de texto cifrado e uma das chaves não devce ser suficiente para determinar a chave

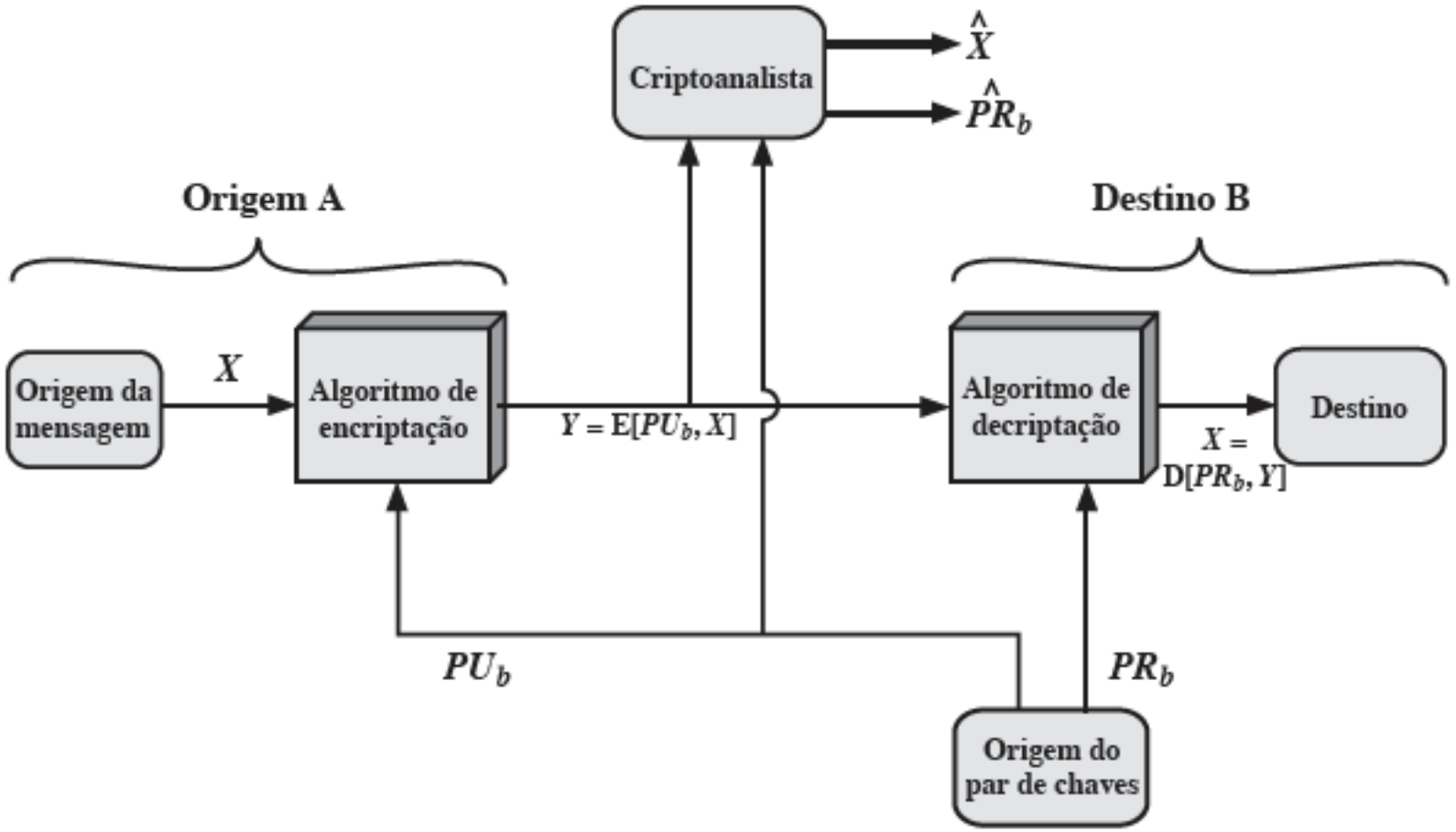
Aplicações

- Criptografia / Decriptografia
- Assinatura Digital
- Troca de chave

Criptografia / Decriptografia 1

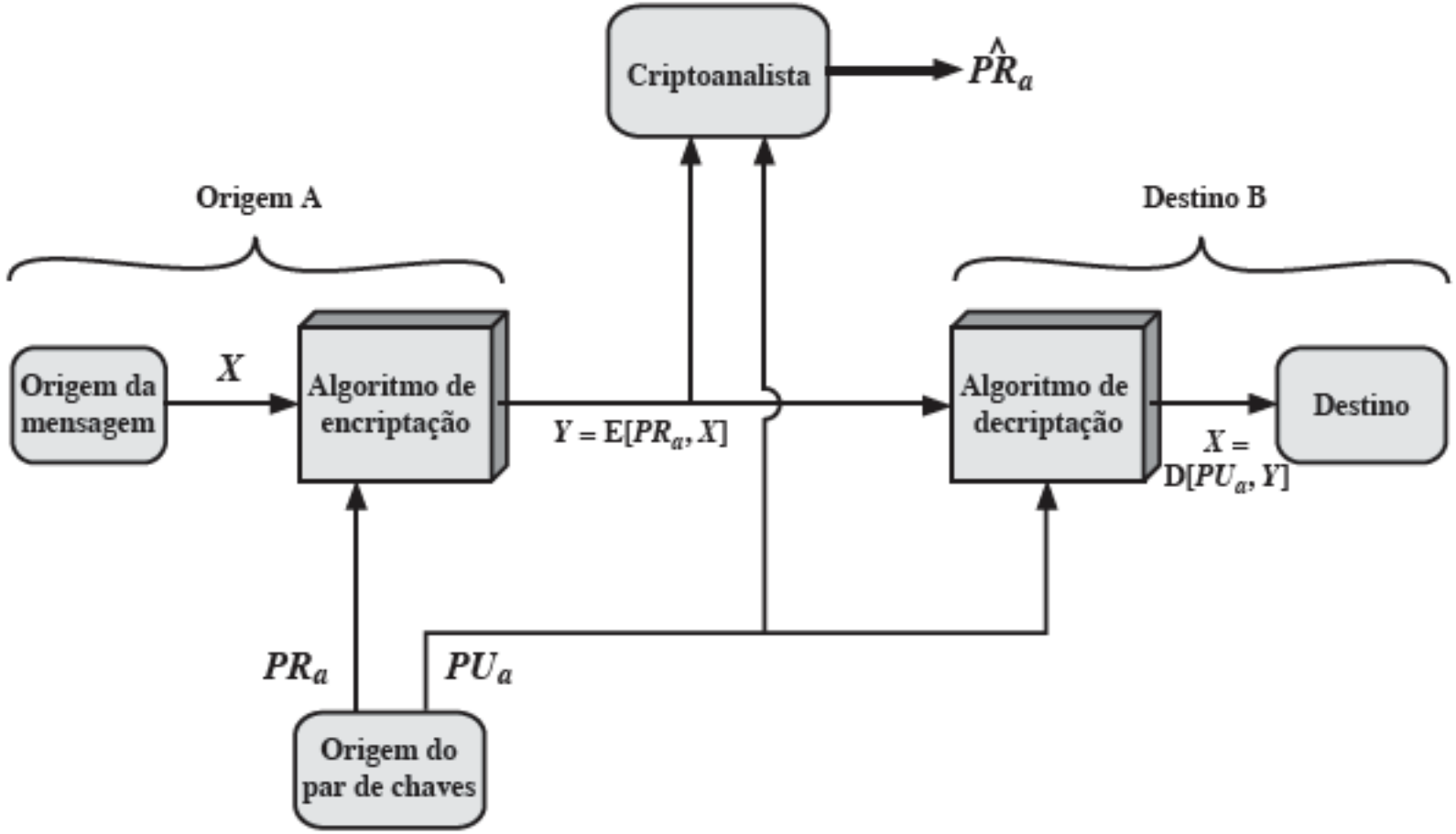


Criptografia / Decriptografia 1

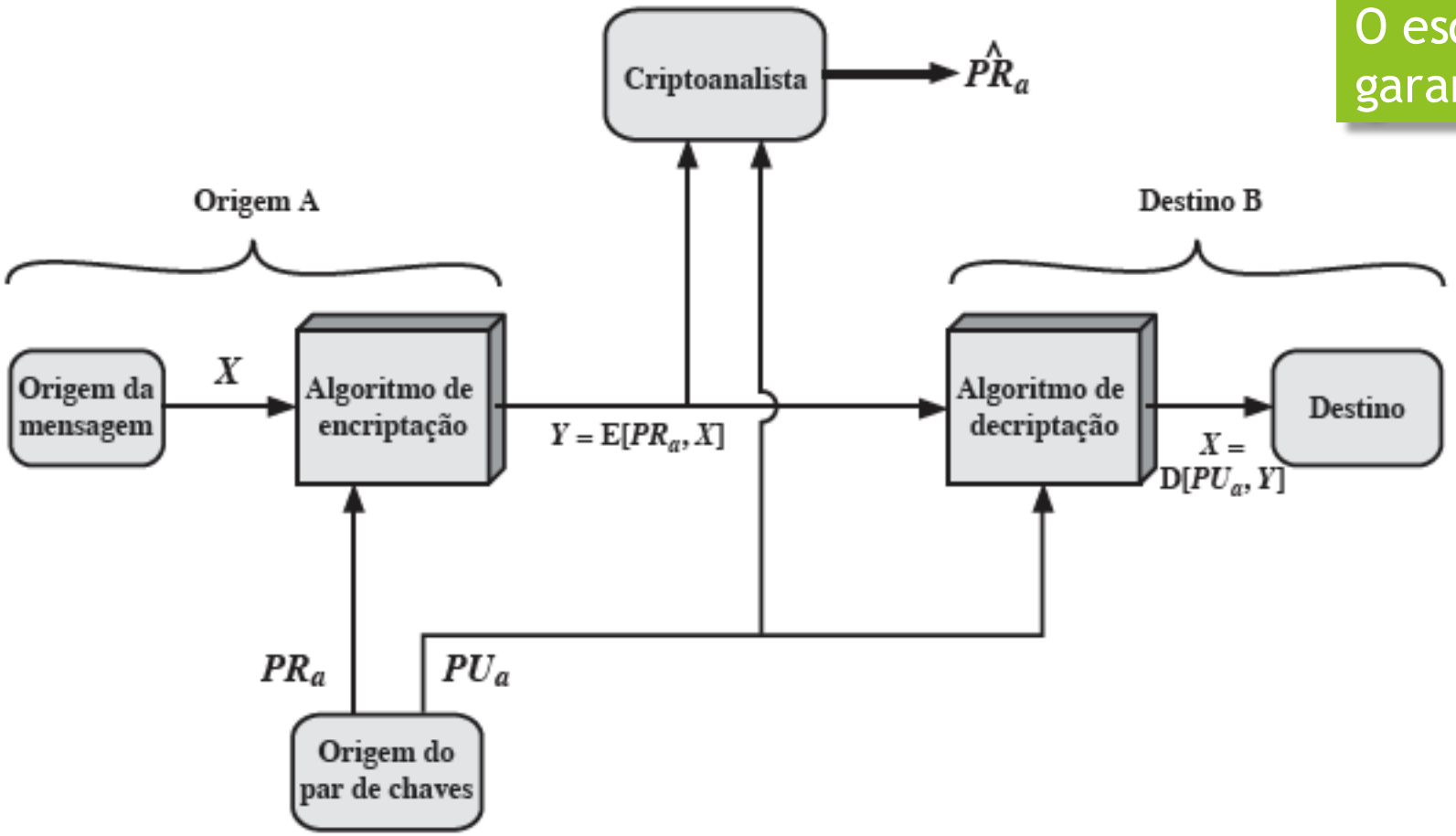


O esquema mostrado garante confidencialidade?

Criptografia / Decriptografia 2

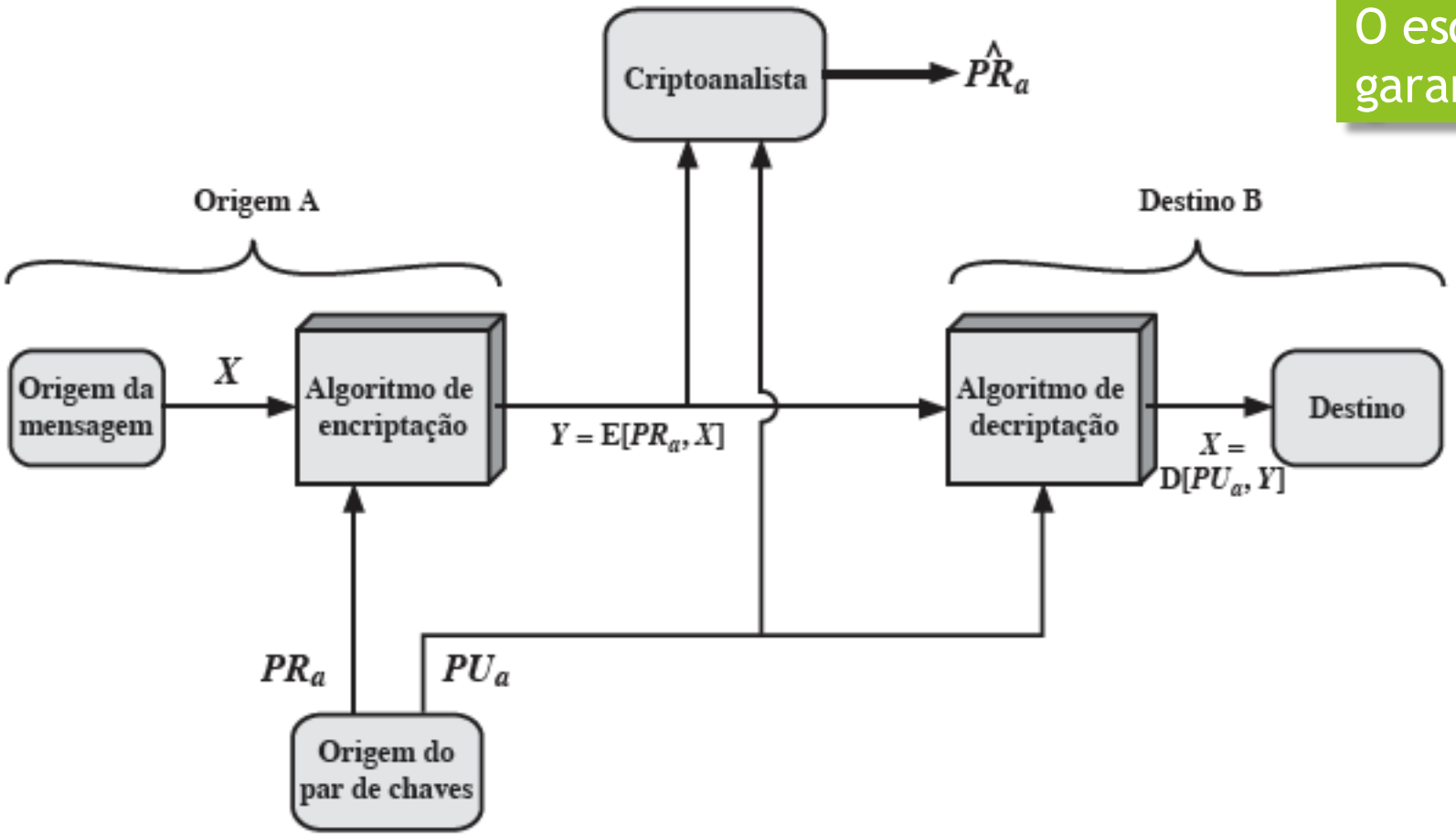


Criptografia / Decriptografia 2



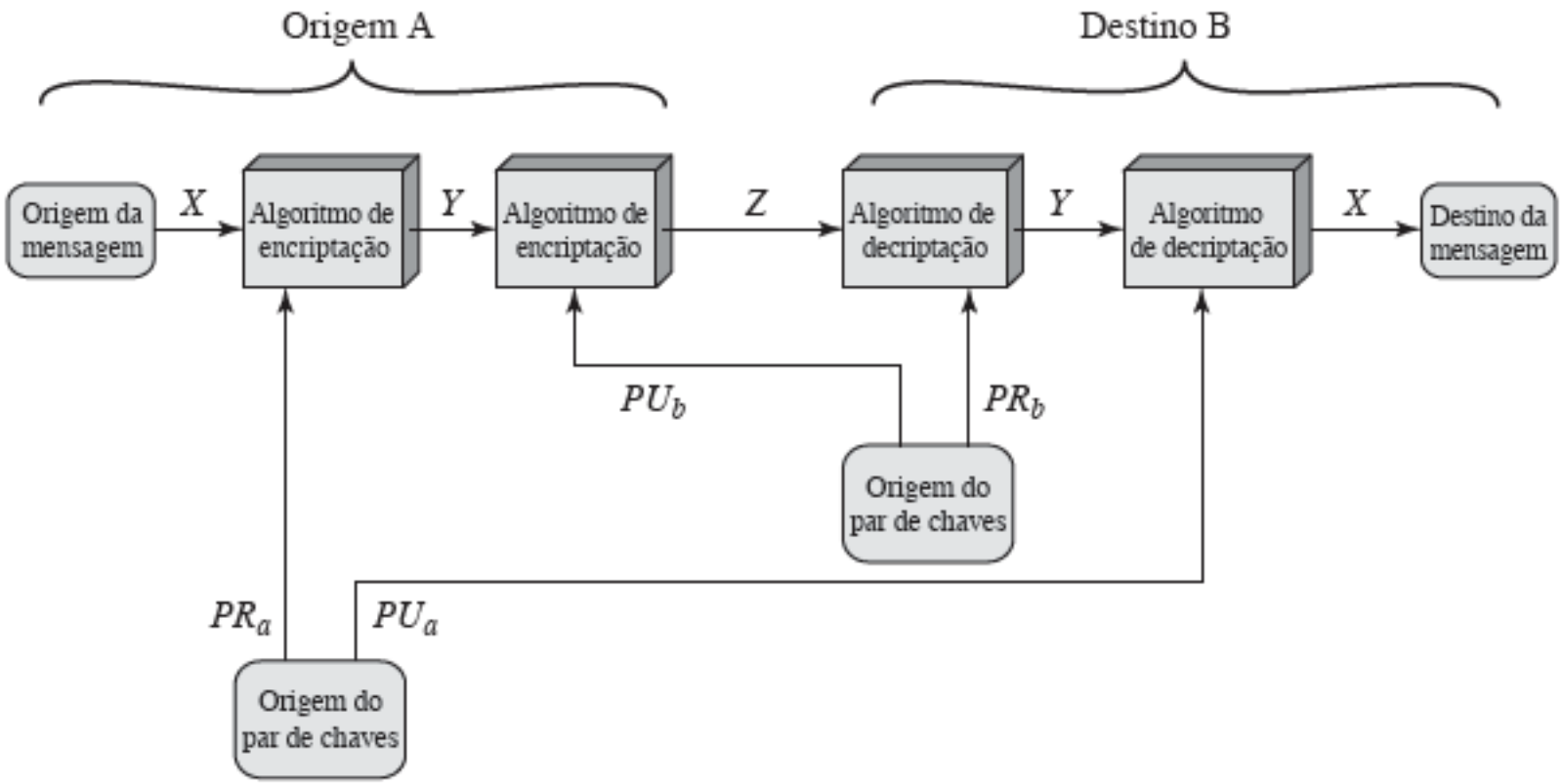
O esquema mostrado garante confidencialidade?

Criptografia / Decriptografia 2

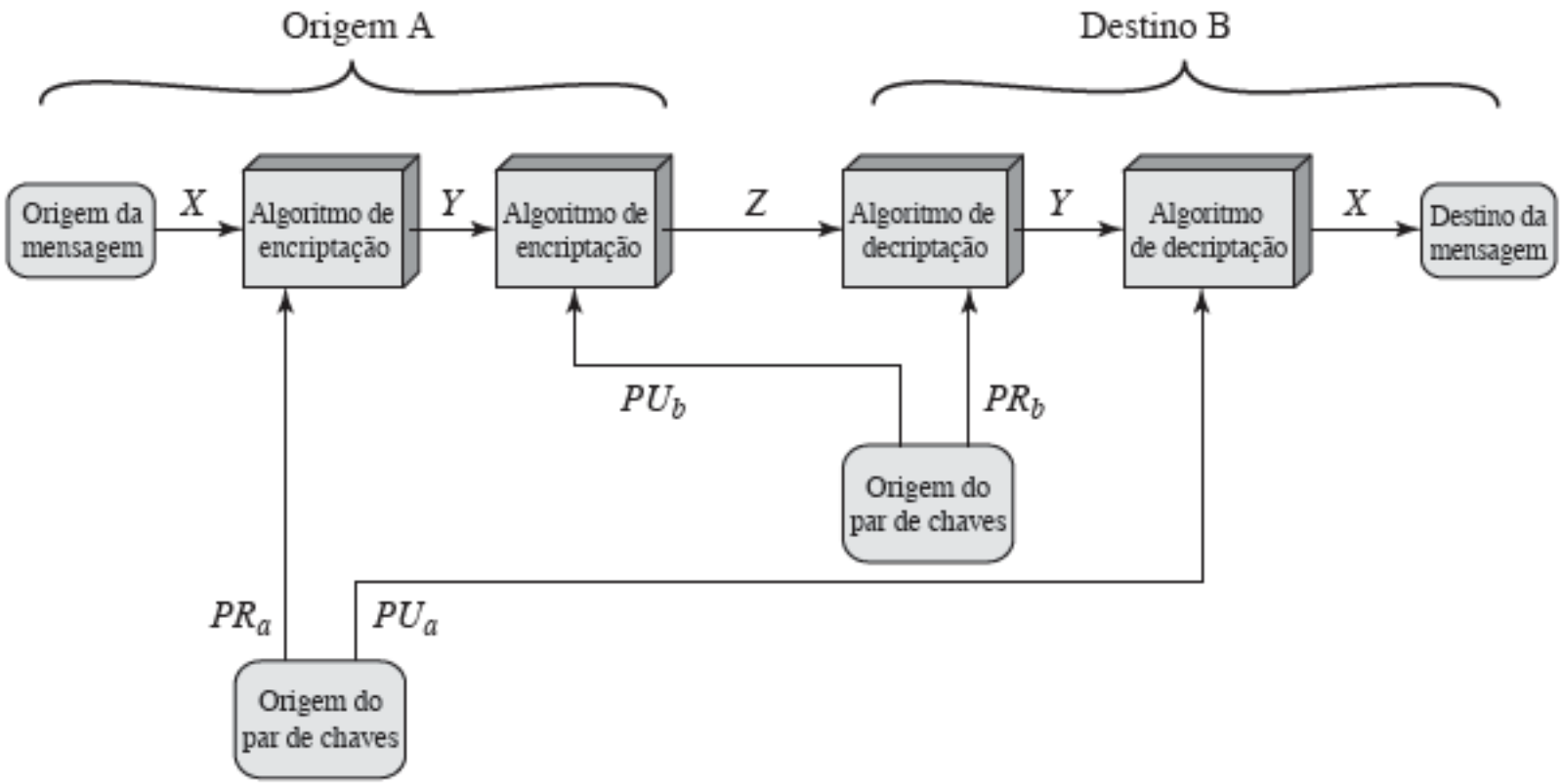


O esquema mostrado garante autenticidade?

Criptografia / Decriptografia 3



Criptografia / Decriptografia 3



O esquema mostrado garante autenticidade? E a confidencialidade?

Requisitos para Criptografia Assimétrica

- *Whitifield Diffie* e *Martin Hellman* postularam um sistema criptográfico baseado em duas chaves em 1976 e estabeleceram as condições que um algoritmo para implementar esse sistema deveria atender.
- Os pesquisadores não demonstraram a existência de tal algoritmo

Requisitos para Criptografia Assimétrica

1. Ser computacionalmente fácil gerar um par de chaves pública e privada
2. Ser computacionalmente fácil para um emissor A, de posse da chave pública de um receptor B, gerar o texto cifrado (C) referente a uma mensagem M, C = E(PUb, M)
3. Ser computacionalmente fácil para B decriptografar o texto cifrado (C) resultante usando a chave privada para recuperar a mensagem M, M = D(PRb, C)
4. Ser computacionalmente inviável para um adversário, conhecendo a chave pública PUb determinar a chave privada PRb
5. Ser computacionalmente inviável para um adversário, conhecendo pública PUb e um texto cifrado C, recuperar a mensagem original M

Criptoanálise de chave pública

- Vulneráveis a ataques de força bruta
- Uso de chaves de tamanho adequado
  - Chaves demasiadamente grandes exigem capacidade computacional que cresce exponencialmente
  - Chaves muito pequenas expõe o algoritmo a ataques de força bruta
- Outro ataque é buscar encontrar a chave privada a partir da chave pública
  - Ainda não há provas da matemáticas que isso é inviável
  - Ainda não há relatos de que isso foi realizado
  - Logo, algoritmos de chave assimétrica ainda são “suspeitos”

Criptoanálise de chave pública

- Vulneráveis a ataques de mensagem provável
  - Quando se usa como mensagem uma chave simétrica de 56 bits (DES, por exemplo)
  - Um adversário poderia criptografar todas as possíveis chaves de 56 bits usando a chave pública para encontrar a chave criptografada em combinação com o texto cifrado capturado
  - Para qualquer tamanho de chave assimétrica, o ataque é reduzido a um ataque de força bruta de 56 bits

Diffie-Hellman para RSA

- Depois do artigo pioneiro de *Diffie* e *Hellman (1976)* iniciou-se uma corrida para criar um algoritmo que atendesse aos requisitos proposto pelos autores
- Em 1978, *Ron **Rivest***, *Adi **Shamir*** e *Len **Adleman***, pesquisadores do MIT, publicaram uma das primeiras propostas e a mais aplicada até hoje

Características RSA

- Cifra de bloco tipicamente de 1024 bits

Segurança RSA

- Abordagens de ataque
  - Força bruta
  - Ataques matemáticos
  - Ataques de temporização (*timing attack*)
  - Ataques de texto cifrado escolhido

Força Bruta

- Contramedida é utilizar chaves de tamanho adequado através do compromisso entre segurança e agilidade do sistema

Ataques Matemáticos

- O algoritmo RSA baseia-se em dois números primos p e q
- n = pq
- As chaves são geradas a partir de n
- As estratégias de ataques consistem artifícios matemáticos para encontrar n

Timing Attacks

- Buscam estimar n através do tempo de processamento das operações multiplicação modular para e assim fazer suposições sobre o valor de n

Referências

- Criptografia e Segurança de Redes. Stalings, William. 4a. Ed.
  - Capítulo 9.