Criptografia de chave pública

Prof. Vilmar Abreu Junior
vilmar.abreu@pucpr.br

PUCPR ESCOLA POLITÉCNICA

Agenda

- Termos
- Conceitos básicos
- Elementos
- Tipo de ataques
- Algoritmos

Criptografia de chave pública

- Também conhecida como: Criptografia **assimétrica**;
- Proposta em 1976, foi o primeiro avanço revolucionário na criptografia em milhares de anos;
- A cifração e decifração da informação é realizada utilizando **duas chaves**;

Criptografia de chave pública (cont.)

- Utilizar **duas** chaves tem profundas consequências nas áreas de **confidencialidade**, **distribuição** de chaves e **autenticação**!
- Algoritmos baseados em **funções matemáticas** ao invés de simples operações (substituição/transposição);

Antes de mais nada, é bom saber:

- Criptografia de chave pública **NÃO** é mais segura do que a criptografia simétrica
  - Segurança está relacionada ao **comprimento** da chave e do esforço necessário para **quebra** de uma cifra
- Apesar de mais moderna, a criptografia simétrica **NÃO** está obsoleta
  - Criptografia de chave pública tem um elevado **custo computacional**
- Distribuição de chaves **NÃO** é mais simples.

Motivação

- Resolver o problema complexo de **distribuição de chaves** em criptografia simétrica: Duas entidades tem que compartilhar a mesma chave, de algum modo.
- Normalmente através de um KDC, um dos criadores da chave pública disse:
  - ”Qual a razão de fazer algoritmos seguros, com chaves de comprimento apropriado, se dependem de uma terceira entidade (KDC) que pode ser comprometida?”

Conceitos

- Criptografia de chave pública utiliza uma chave para **cifrar** as informações e uma outra chave **diferente**, porém relacionada, para **decifrar** as informações;
- É computacionalmente **inviável** determinar a chave de decifração tendo conhecimento do algoritmo e da chave de cifração;
- **Qualquer** uma das chaves pode ser utilizada para cifrar, sendo obrigatório utilizar a outra para decifrar.

Conceitos (cont.)

- Como o nome sugere, a chave pública do par **torna-se pública** para outros usarem, enquanto a chave privada é de conhecimento apenas do seu **proprietário**;
- O algoritmo criptográfico depende de uma **chave para cifração** e de outra chave relacionada para a **decifração**.

Elementos

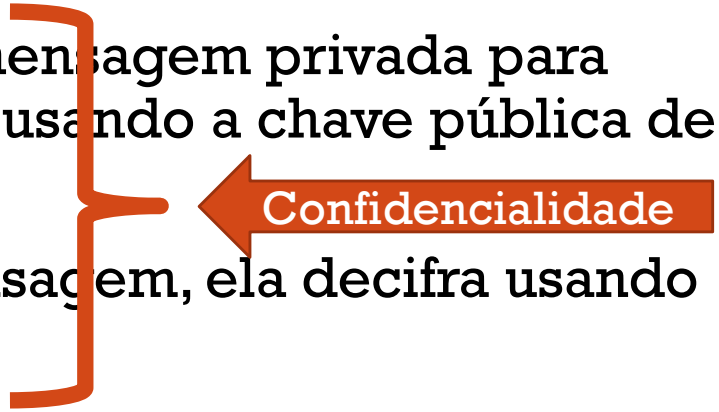
- **Texto às claras**: Mensagem/dado original;
- **Algoritmo de cifração**: Executa várias transformações no texto às claras, baseado na teoria dos números;
- **Chave pública e privada**: Par de chaves que foi selecionado, de modo que, se uma é usada para cifrar a outra é usada para decifrar.

Elementos (cont.)

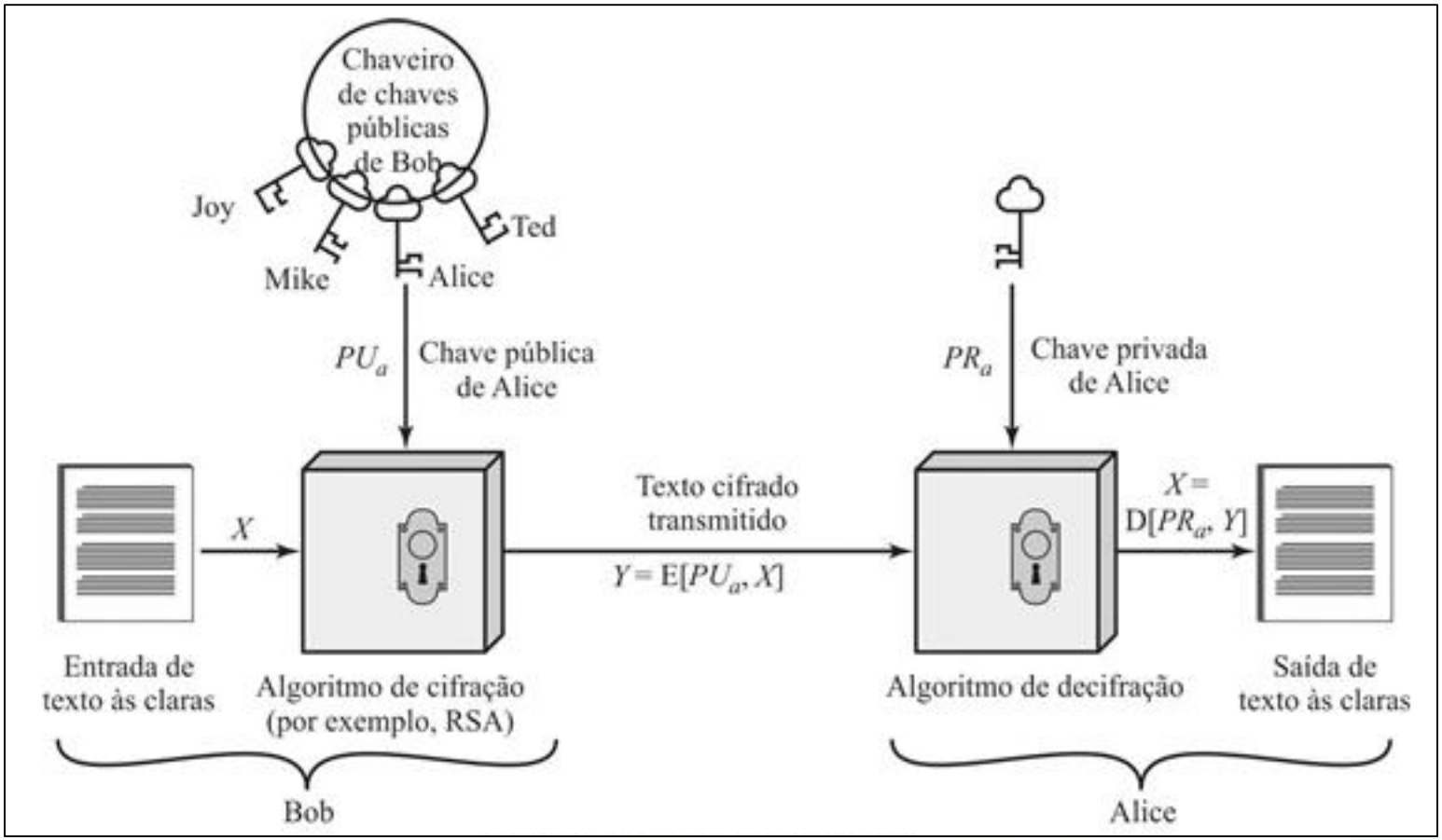
- **Texto cifrado:** Mensagem/dado embaralhado produzido pelo algoritmo de cifração, utilizando o texto às claras e a chave secreta;
- **Algoritmo de decifração:** Recebe o texto cifrado e a chave equivalente, para produzir o texto às claras.

Cifrando com chave pública

1. Cada usuário gera um par de chaves, para cifrar e decifrar
2. Cada usuário coloca uma das chaves em registro público ou arquivo acessível e outra chave é mantida privada. Dessa forma, determinado usuário pode ter uma coleção de chaves públicas
3. Se Bob deseja enviar uma mensagem privada para Alice, ele cifra a mensagem usando a chave pública de Alice
4. Quando Alice recebe a mensagem, ela decifra usando sua chave privada



Cifrando com chave pública (cont.)

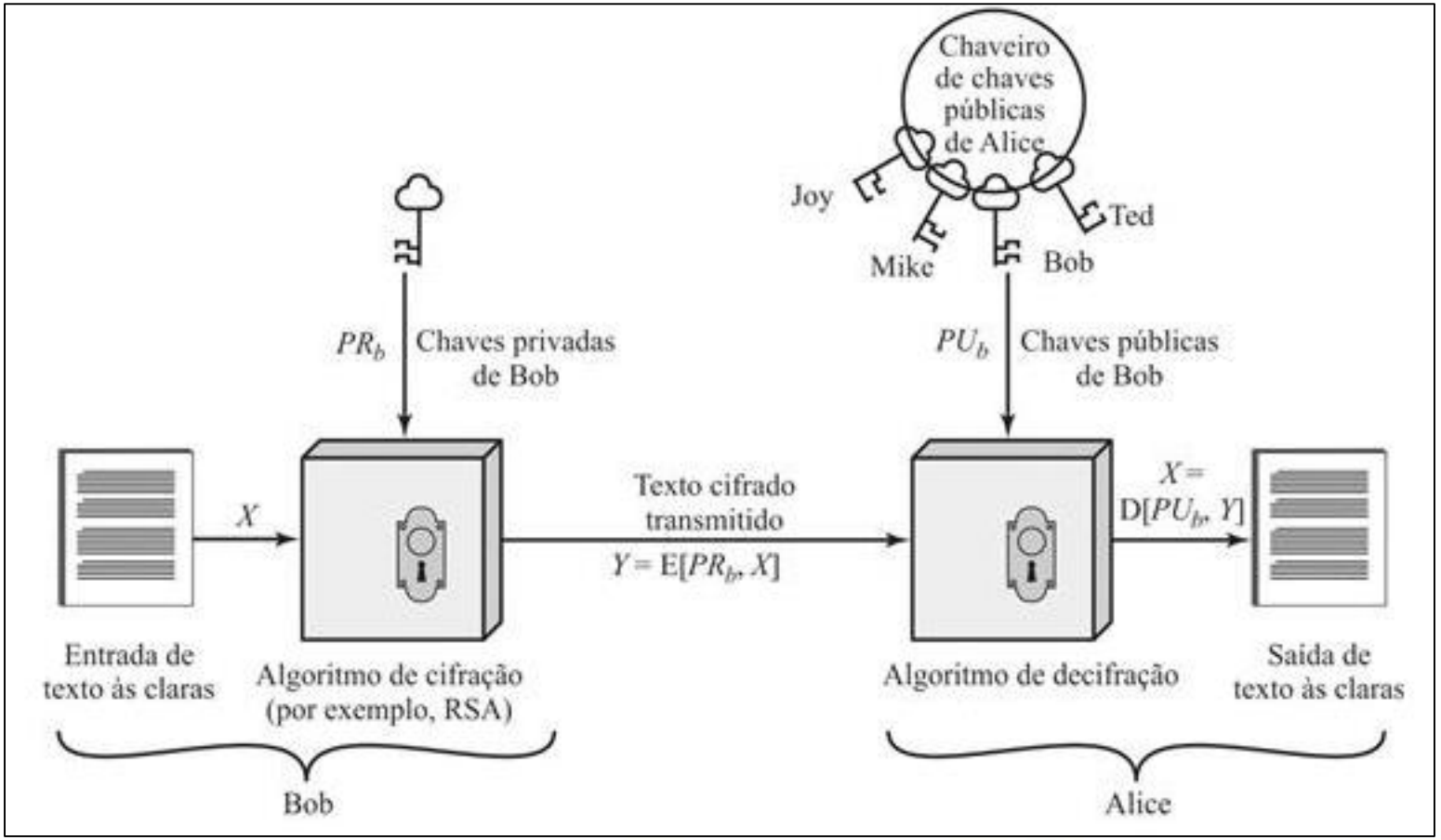


Cifrando com chave privada

1. Cada usuário gera um par de chaves, para cifrar e decifrar
2. Cada usuário coloca uma das chaves em registro público ou arquivo acessível e outra chave é mantida privada. Dessa forma, determinado usuário pode ter uma coleção de chaves públicas
3. Se Bob deseja enviar uma mensagem para quem conhece sua chave pública, ele cifra a mensagem usando a sua chave privada
4. Quem conhece a chave pública, decifra a mensagem e tem a garantia que foi Bob que enviou

Autenticidade

Cifrando com chave privada



Premissas

- Deve ser computacionalmente fácil uma entidade **gerar** um par de chaves (público e privado);
- Deve ser computacionalmente fácil para um remetente (Bob) que conheça uma chave pública **cifrar** um texto;
- Deve ser computacionalmente fácil para um destinatário (Alice) **decifrar** um texto para recuperar a mensagem original.

Premissas (cont.)

- Deve ser computacionalmente inviável que um oponente que conheça a chave pública **determinar** a chave privada;
- Deve ser computacionalmente inviável que um oponente que conheça a chave pública e o texto cifrado na pública consiga **decifrar** a mensagem;
- Qualquer uma das chaves pode ser utilizada para cifrar, sendo que a outra para decifrar.

Como atacar?

- Há duas abordagens gerais para atacar um esquema de cifração simétrica:
  - **Criptoanálise;**
  - **Ataque de força bruta.**

Algoritmos

- Os algoritmos são baseados em uma função de direção única (*one-way*);
- Os algoritmos mais conhecidos são:
  - RSA (1977)
  - Diffie e Hellman (1976)
  - Digital Signature Algorithm (1991)
  - Curvas Elipticas (1985)

Aplicações

A criptografia de chave pública pode ser utilizada principalmente em:

- Cifração/Decifração
- Distribuição de chaves simétricas
- Assinatura Digital

Distribuição de chave simétrica (simples)

1. Bob gera um par de chaves (PU_{bob}/ PR_{bob}) e encaminha uma mensagem para Alice contendo a PU_{bob} e um identificador;
2. Alice gera uma chave secreta ($K_{sessão}$) e encaminha para Bob, cifrando na PU_{bob};
3. Bob decifra a mensagem utilizando PR_{bob} e armazena $K_{sessão}$;
4. Bob descarta PU_{bob}/ PR_{bob}.

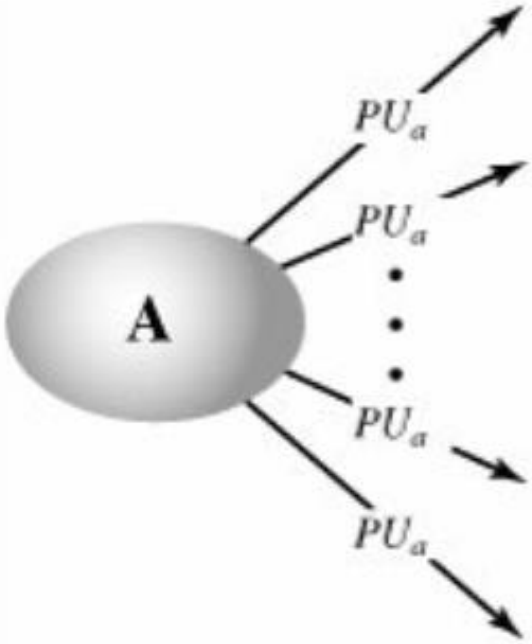
Distribuição de chaves assimétricas

As principais técnicas de distribuição de chaves públicas são:

- **Anúncio público**
- Diretório público
- Autoridade pública
- Certificado

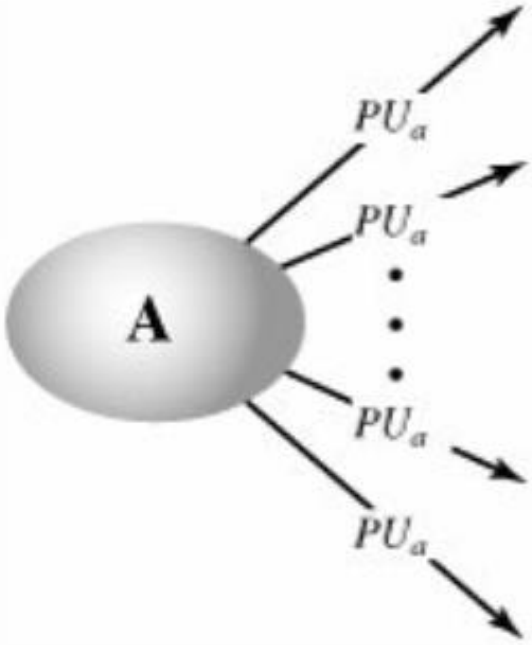
Anúncio Público

- Disponibiliza as chaves públicas para qualquer entidade (por *broadcast*, por exemplo);



Anúncio Público (cont.)

- **Desvantagem**: Qualquer um pode forjar a chave pública de outra entidade.



Distribuição de chaves assimétricas

As principais técnicas de distribuição de chaves públicas são:

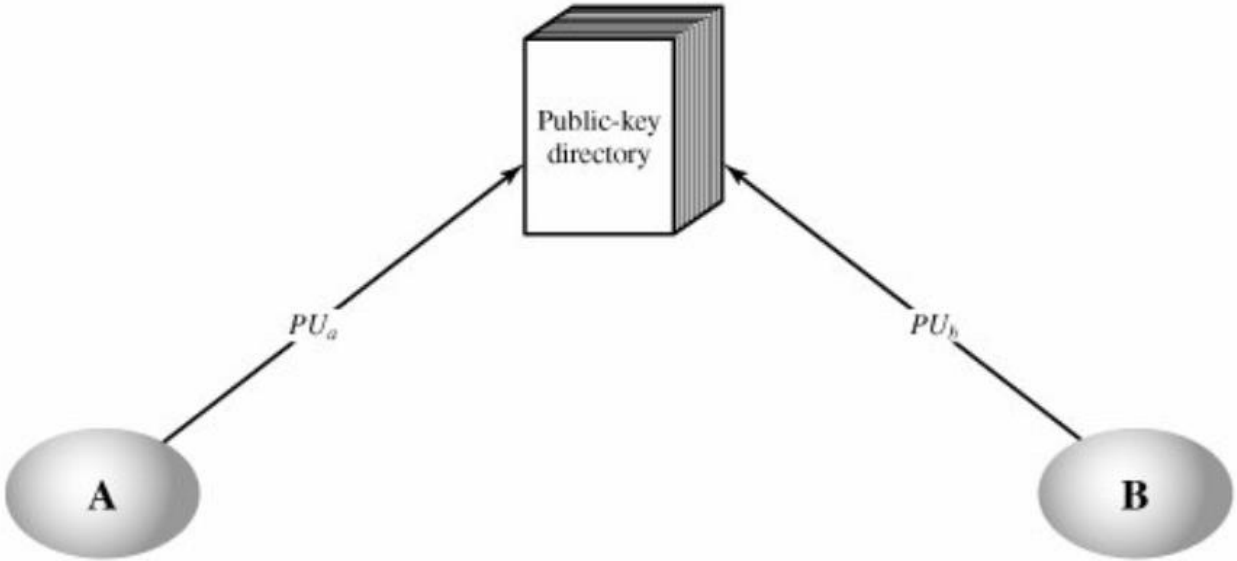
- Anúncio público
- **Diretório público**
- Autoridade pública
- Certificado

Diretório público

- Uma entidade confiável mantém um **dicionário** (mapeamento de entidade e chave pública) para cada participante;
- Cada participante deve registrar sua chave pública;
- Cada participante pode atualizar sua chave pública a qualquer momento;

Diretório público (cont.)

- **Desvantagem**: Caso o diretório seja comprometido, o oponente pode forjar ser qualquer entidade.



Distribuição de chaves assimétricas

As principais técnicas de distribuição de chaves públicas são:

- Anúncio público
- Diretório público
- **Autoridade pública**
- Certificado

Autoridade pública

- Baseado no diretório público, cada participante possui uma chave pública na Autoridade, sendo que apenas a Autoridade conhece a chave privada;
- O processo é composto de 6 etapas:

Autoridade pública (cont.)

1. Bob envia uma mensagem cifrada na $PU_{autoridade}$ para a Autoridade, solicitando a PU_{alice};
2. Autoridade responde a mensagem cifrada na $PR_{autoridade}$. A mensagem contém a chave pública de Alice (PU_{alice});
3. Bob armazena PU_{alice} e a utiliza para cifrar a mensagem para Alice. A mensagem contém um identificador de Bob.

Autoridade pública (cont.)

4. Alice solicita a PU_{bob} para a Autoridade, seguindo o mesmo procedimento;
   - Nesse momento Bob e Alice possuem as chaves públicas;
5. Alice gera um *nonce* e encaminha para Bob, cifrando na PU_{bob}
6. Bob responde Alice executando uma função sobre o nonce recebido, cifrando na PU_{alice}

Autoridade pública (cont.)

- **Desvantagem**: Caso a autoridade seja comprometida, o oponente pode forjar ser qualquer entidade.

Distribuição de chaves assimétricas

As principais técnicas de distribuição de chaves públicas são:

- Anúncio público
- Diretório público
- Autoridade pública
- **Certificado (Tema de estudo futuro)**

ESCOLA
POLITÉCNICA