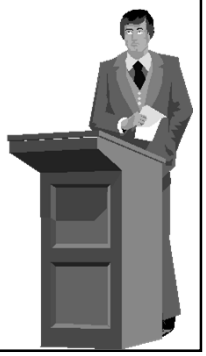
Criptografia de Chave Pública

Prof. Dr. Volnys Borges Bernal[2]
Prof. Dr. Adilson Eduardo Guelfi[1]

(1) Faculdade de Informática de PP
UNOESTE

(2) Laboratório de Sistemas Integráveis
Escola Politécnica da USP



Agenda

- **Modelo de Criptografia de Chave Pública**
- **Criptografia de Chave Pública - Utilização**
  - Confidencialidade
  - Autenticidade
  - Confidencialidade com autenticação
- **Criptografia de Chave Pública - Características**
- **Principais Algoritmos**
- **Exercícios**
- **Referências Bibliográficas**

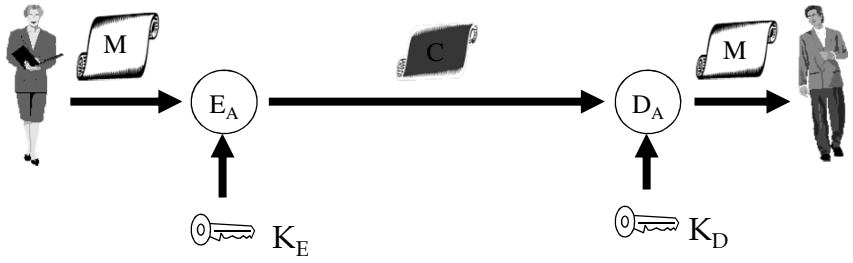
Modelo de Criptografia de Chave Pública

Modelo de Criptografia de Chave Pública

- **Modelo lançado para resolver os problemas mais característicos associados a criptografia simétrica**
  - Problema de distribuição de chaves
  - Problema das assinaturas digitais
    - Autoria e validade para mensagens digitais
    - Requisito um pouco mais amplo do que uma simples autenticação
- **1976: Diffie e Hellman apresentaram um método que resolvia os dois problemas anteriores**

Modelo de Criptografia de Chave Pública

- **Criptossistema em que a criptografia e a decifração são realizadas usando diferentes chaves**
- **Utiliza duas chaves (par)**
  - Uma para cifrar (K_E) e outra para decifrar (K_D)
  - Conhecendo-se uma das chaves, o algoritmo e um texto cifrado deve ser inviável computacionalmente descobrir a outra chave parceira

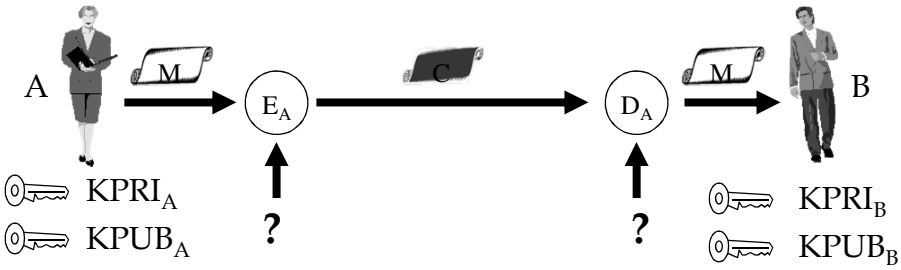


Modelo de Criptografia de Chave Pública

- **O par de chaves criptográficas**
  - **<u>Fica associado à cada entidade</u>**
  - Uma chave é pública e de conhecimento de todos (chave pública)
  - Outra chave é secreta à entidade, gerada localmente e nunca deve ser distribuída (chave privada)
- **Notação**
  - Criptografia Simétrica (convencional)
    - Chave simétrica: K
  - Criptografia Assimétrica (criptografia de chave pública)
    - Chave Privada: KPRI
    - Chave Pública: KPUB

Modelo de Criptografia de Chave Pública

- **Temos então 4 chaves!**
  - Qual chave utilizar, e em que caso?
    - Depende de que tipo de serviço de segurança deseja-se obter



Criptografia de Chave Pública - Utilização

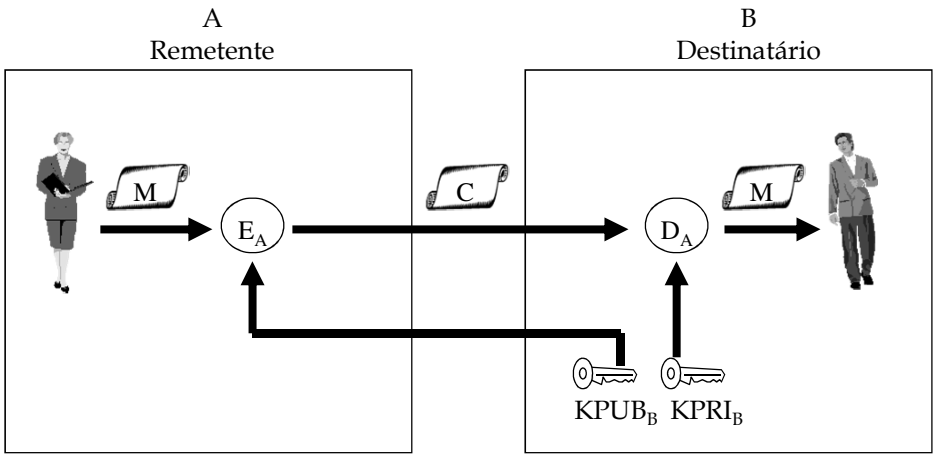
Utilização

- **Criptografia de chave pública pode ser utilizada para os seguintes casos:**
  - Confidencialidade
  - Autenticação
  - Confidencialidade e Autenticação

Utilização: Confidencialidade

- **Objetivo:**
  - Manter o sigilo de determinada informação
- **Funcionamento**
  - O remetente cifra a mensagem utilizando a chave pública do destinatário e depois transmite
  - O destinatário recebe o texto cifrado e depois decifra a mensagem utilizando sua chave privada.
  - Como somente o destinatário conhece sua chave privada que se manteve secreta, somente ele pode recuperar a mensagem, e assim consegue-se obter o nível de sigilo desejado.

Utilização: Confidencialidade (cont.)



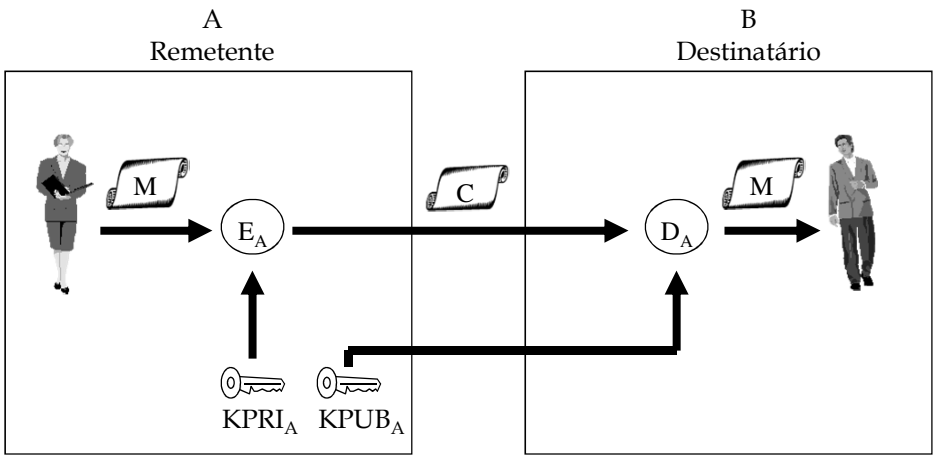
Utilização: Confidencialidade (cont.)

- **Funcionamento**
  - Criptografia
    - **$C = E (KPUB_B , M)$**
  - Decifração
    - **$M = D (KPRI_B , C)$**

Utilização: Autenticação

- **Objetivo**
  - Ter noção sobre o autor de determinada informação
- **Funcionamento**
  - O remetente cifra a mensagem com sua chave privada e depois transmite.
  - A decifração da mensagem pode ser realizada por qualquer outra entidade utilizando a chave pública do remetente
  - Somente o remetente poderia ter preparado o texto cifrado uma vez que somente ele conhece sua chave privada que se manteve secreta
  - Consegue-se mensagem autenticada quanto a origem

Utilização: Autenticação (cont.)



Utilização: Autenticação (cont.)

- **Nível de Autenticação**
  - Neste caso, a autoria pode ser admitida se considerarmos que somente o remetente possui a chave privada
  - O criptograma não pode ter sido gerado por outra chave (pessoa) já que somente o remetente possui a chave privada associada à chave pública de decifração

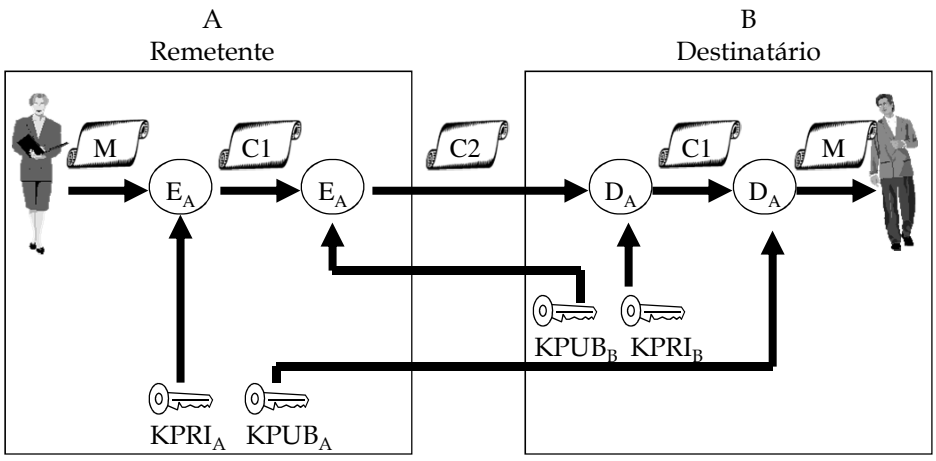
Utilização: Autenticação (cont.)

- **Funcionamento**
  - Ambos texto legível e texto cifrado precisam ficar armazenados juntos para fins práticos de verificação
  - Criptografia
    - **$C = E(KPRI_A, M)$**
  - Decriptação
    - **$M = D(KPUB_A, C)$**
- **OBS:**
  - O esquema de autenticação não provê confidencialidade, uma vez que qualquer entidade pode decifrar a mensagem original com a chave pública do remetente

Utilização: Confidencialidade e Autenticação

- **Objetivo**
  - Manter secreta determinada informação e permitir ao destinatário ter noção sobre sua autoria (autor)
- **Funcionamento**
  - O remetente cifra a mensagem inicialmente com sua chave privada e, em seguida, com a chave pública do destinatário
  - O destinatário decifra a mensagem original com sua chave privada e, em seguida, com a chave pública do remetente

Utilização: Confidencialidade e autenticação



Utilização: Confidencialidade e autenticação

- **Confidencialidade**
  - Primeira decifração
  - Somente o destinatário pode decifrar a mensagem, pois somente ele possui e conhece a chave privada $KPRI_B$
- **Autenticação**
  - Segunda decifração
  - O destinatário pode admitir a autoria da entidade A, já que somente o remetente possui e conhece sua chave privada $KPRI_A$

Utilização: Confidencialidade e autenticação

- **Funcionamento**
  - Criptografia

    $C2 = E(KPUB_B, C1)$

    $C2 = E(KPUB_B, E(KPRI_A, M))$
  - Decifração

    $M = D(KPUB_A, C1)$

    $M = D(KPUB_A, D(KPRI_B, C2))$

Criptografia de Chave Pública - Características

Características

- **Flexibilidade**
  - Existência de 2 chaves, com possibilidade de tornar uma pública
  - Fundamental para alguns serviços como autenticação
- **Custo computacional**
  - A criptografia de chave pública é muito mais lenta que a criptografia simétrica
    - Em software: cerca de 100 vezes mais lenta que a criptografia simétrica em software
    - Em hardware: cerca de 1000 vezes mais lenta que a criptografia simétrica em hardware

Características

- **Em relação à criptografia simétrica …**
  - Radicalmente distinta: envolve a utilização de duas chaves distintas
  - **Não torna obsoleta a criptografia simétrica**
    - Devido à sobrecarga de processamento (custo computacional) causada pela criptografia de chave pública
- **Problema da Distribuição de Chaves**
  - Resolve quanto a confidencialidade na distribuição da chave secreta K de criptografia simétrica (canal seguro)
  - Não resolve quanto a autenticação da entidade que distribui a chave secreta K, pois ainda falta o aspecto da autenticidade da chave pública que pode ser distribuída livremente

Principais Algoritmos

Principais Algoritmos

- **RSA (Rivest-Shamir-Adleman)**
  - Algoritmo publicado em 1978 com valores típicos para tamanho de chaves: 512, 1024, 2048 bits
  - Valor atual mínimo considerado seguro para tamanho de chave: 2048 bits
- **ECC "*Elliptic Curve Cryptography*"**
  - Baseada na teoria ou aritmética de Curva Elíptica
  - Tamanhos de chave: 224 ou 256 bits

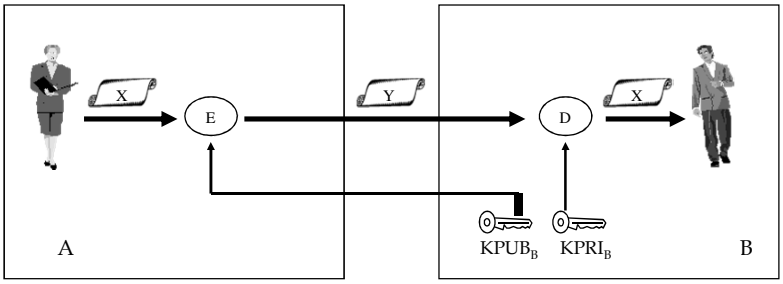
Exercícios

Criptografia de Chave Pública

Exercícios

(1) A figura a seguir mostra um esquema de criptografia de chave ...

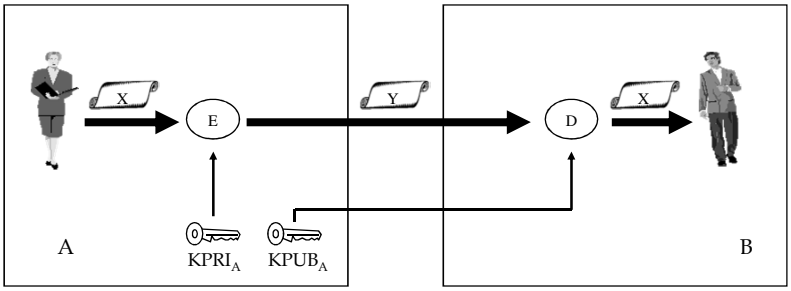
(a) convencional utilizado para a confidencialidade de uma mensagem
(b) convencional utilizado para a autenticidade de uma mensagem
(c) pública utilizado para a confidencialidade de uma mensagem
(d) pública utilizado para a autenticidade (autoria) de uma mensagem
(e) pública utilizado para a confidencialidade e autenticação de uma mensagem



Exercícios

(2) A figura a seguir mostra um esquema de criptografia de chave ...

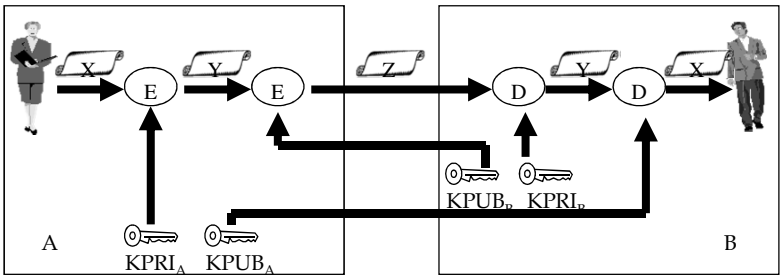
(a) convencional utilizado para a confidencialidade de uma mensagem
(b) convencional utilizado para a autenticidade de uma mensagem
(c) pública utilizado para a confidencialidade de uma mensagem
(d) pública utilizado para a autenticidade (autoria) de uma mensagem
(e) pública utilizado para a confidencialidade e autenticação de uma mensagem



Exercícios

(3) A figura a seguir mostra um esquema de criptografia de chave ...

(a) convencional utilizado para a confidencialidade de uma mensagem
(b) convencional utilizado para a autenticidade de uma mensagem
(c) pública utilizado para a confidencialidade de uma mensagem
(d) pública utilizado para a autenticidade (autoria) de uma mensagem
(e) pública utilizado para a confidencialidade e autenticação de uma mensagem



Exercícios

(4) Os algoritmos DES, IDEA e RSA são respectivamente:

(a) Algoritmo de criptografia de chave pública, função hash e algoritmo de criptografia de chave convencional
(b) Algoritmo de criptografia de chave convencional, algoritmo de criptografia de chave pública, função hash
(c) Algoritmo de criptografia de chave convencional, algoritmo de criptografia de chave pública e algoritmo de criptografia de chave pública
(d) Função hash, algoritmo de criptografia de chave pública e função hash
(e) Algoritmo de criptografia de chave pública, algoritmo de criptografia de chave pública e função hash
(f) Algoritmo de criptografica de chave convencional, algoritmo de criptografia de chave convencional e algoritmo de criptografia de chave pública

Exercícios

(5) Utilize o utilitário openssl para gerar um par de chaves RSA de 512 bits.

(a) Gere o par de chaves e armazene em um arquivo no formato PEM:

openssl genrsa –out *privkey1.pem* 512

(b) Extraia a chave pública e armazene em um arquivo

openssl rsa –in *privkey1.pem* –pubout –out *pubkey1.pem*

Exercícios

(6) Crie um pequeno arquivo com no máximo 20 caracteres (menor que um bloco RSA de 512 bits) e proteja com criptografia RSA.

openssl rsautl –in *messagem.txt* –out *criptograma.rsa*
–pubin –inkey *pubkey1.pem* –encrypt

(7) Decifre o criptograma

openssl rsautl –in *criptograma.rsa* –out *mensagem.out*
–inkey *privkey1.pem* -decrypt

Exercícios

(8) Utilize o utilitário openssl para gerar um par de chaves RSA de 512 bits com proteção da chave privada com criptografia 3des.

openssl genrsa –des3 –out *privkey2.pem* 512

Referências Bibliográficas

Referências Bibliográficas

- **Criptografia e Segurança de Redes - Princípios e Práticas (4a. Edição)**
  - Willian Stallings, Pearson. 2008
- **APPLIED CRYPTOGRAPHY - PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C**
  - SCHNEIER, BRUCE, Editora: JOHN WILEY CONSUMER, Edição: 2ª, 1996
- D. Hankerson, A. Menezes, S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer
- **RSA Laboratories**
  - http://www.rsasecurity.com/rsalabs
- http://www.certicom.com/ecc_tutorial/ ecc_javaCurve.html