

# Criptografia baseada em dados pessoais (abril 2004)

Routo Terada

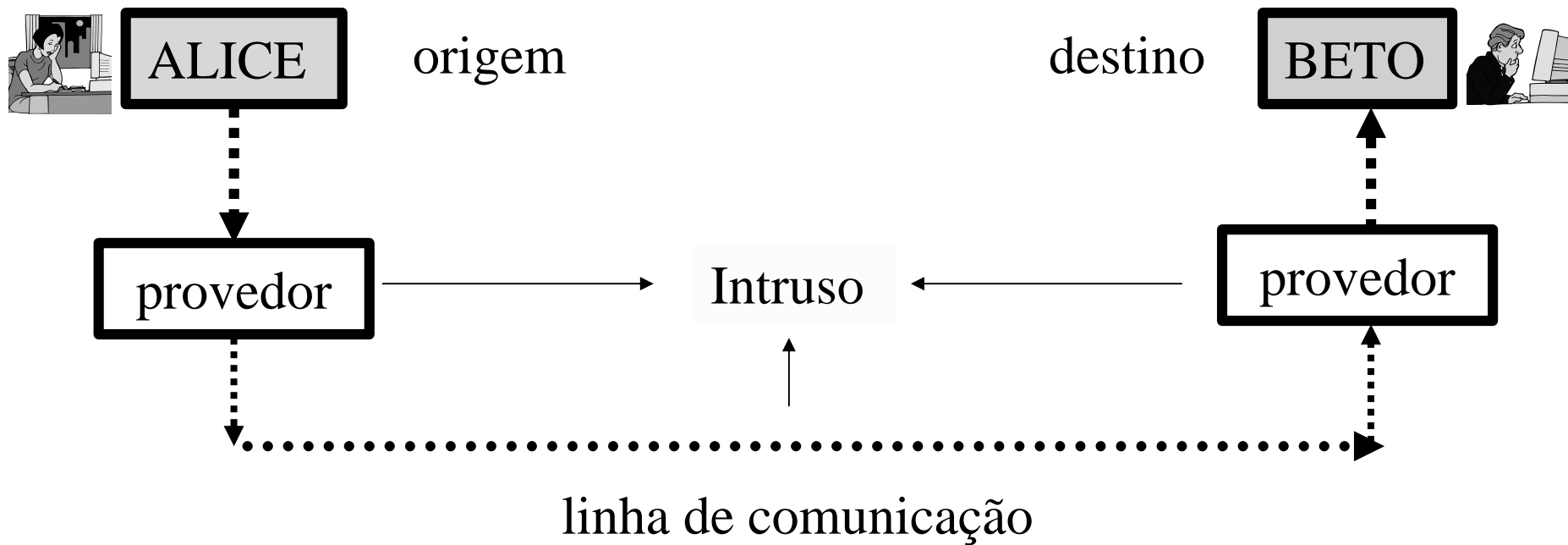
[www.ime.usp.br/~rt](http://www.ime.usp.br/~rt)

Depto. Ciência da Computação - USP

# AGENDA

- Sistemas baseados em dados pessoais (sem PKI)
- Aplicações diversas:
  - Chaves públicas com prazo
  - Viagem com um *notebook*
  - Divisão por tipo de assunto
  - Divisão por tipo de serviço
  - Criação de grupos

## Cenário geral

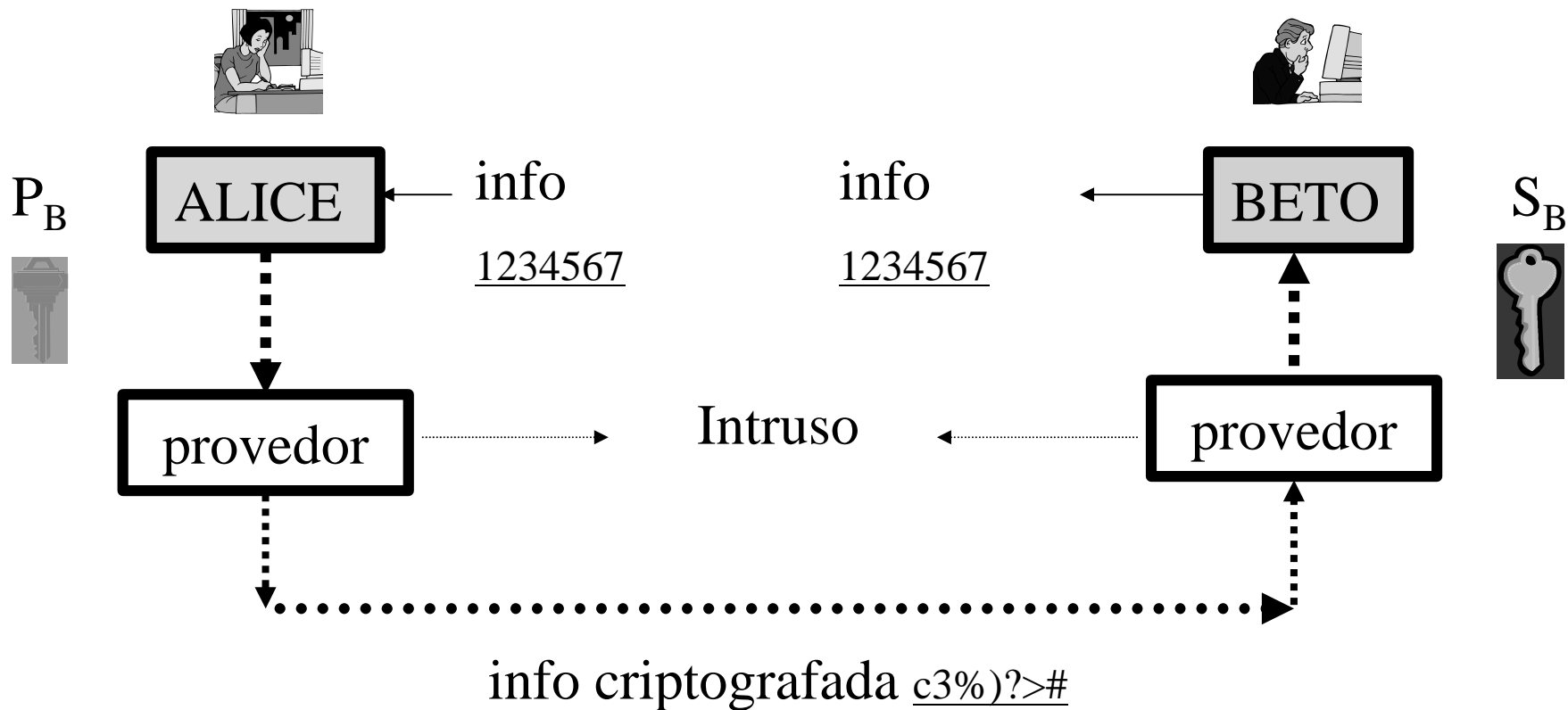


Objetivo: esconder info (como o número do seu cartão de crédito) de algum intruso na linha ou no provedor

# Modelo Diffie e Hellman (Stanford) 1976

Chave *pública* do Beto

Chave *particular* do Beto



$G_1, G_2$ :

grupos de ordem prima  $q$  (*160 bits*),

onde o

Problema do Logaritmo Discreto

seja difícil e

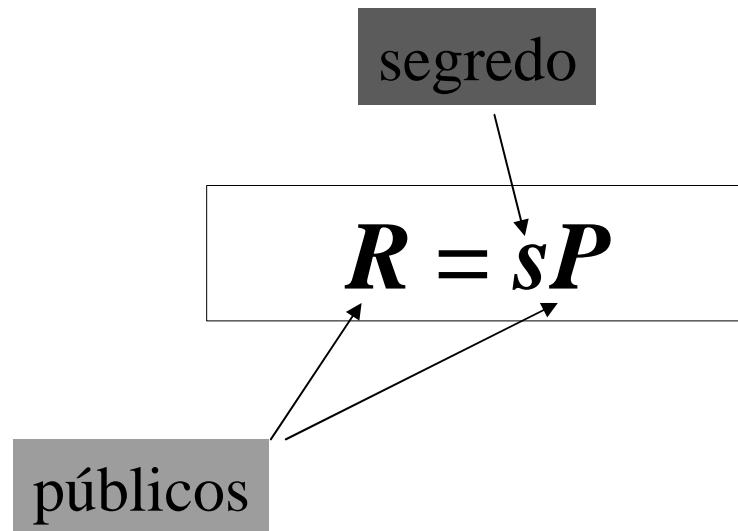
para os quais existe um mapeamento  
bilinear computável

$$t : G_1 \times G_1 \rightarrow G_2,$$

onde  $t$  representa o emparelhamento  
de *Tate*.

# Par de Chaves Padrão

- Par de chaves pública/particular padrão  $(R, s)$ :
- Sejam  $R \in G_1$ ,  $s \in \mathbb{F}_q$  e  $P$  um ponto fixo em  $G_1$  e de conhecimento público. Temos que:



Serão utilizadas as seguintes funções de “hashing”:

$$H_1 : \{0,1\}^* \rightarrow G_1;$$

$$H_2 : \{0,1\}^* \rightarrow F_q;$$

$$H_3 : G_2 \rightarrow \{0,1\}^*.$$

# Chaves

Par de chaves baseadas em dados pessoais  $(Q_{ID}, S_{ID})$ :

onde  $Q_{ID}$  e  $S_{ID} \in G_1$  e

existe uma Autoridade de Confiança

*(Trusted Authority – TA)*

com um par de chaves padrão  $(R_{TA}, s)$

de modo que valem as seguintes relações:

$$S_{ID} = sQ_{ID}$$

segredo

$$Q_{ID} = H_1(ID)$$

público

onde  $ID$  é o string identificador (dados pessoais)

(por exemplo:  $Q_{Beto} = \text{Beto@ime.usp.br}$ )

# Criptografia baseada em dados pessoais

Sejam :

$(Q_{Beto}, S_{Beto})$ : par de chaves pública/ particular baseadas em dados pessoais;

$R_{TA}$ : chave pública padrão de uma autoridade de confiança - TA;

$m$ : mensagem a ser transmitida da Alice para Beto

(continua)

# Criptografia baseada em dados pessoais

## Criptografia

$$Q_{Beto} = \text{Beto@ime.usp.br}$$

Alice calcula:

públicos

$$\begin{cases} U = rP \\ V = m \oplus H_3(t(R_{TA}, rQ_{Beto})) \end{cases}$$

$r$  : elemento aleatório de  $F_q$

Analogia: envelope com carta

O texto cifrado é  $(U, V)$

## Decriptografia

Beto calcula:

segredo

$$m = V \oplus H_3(t(U, S_{Beto}))$$

# Criptografia baseada em dados pessoais

## Criptografia

$$Q_{Beto} = \text{Beto@ime.usp.br}$$

Alice calcula:

públicos

$$\begin{cases} U = r P \\ V = m \oplus H_3(t(R_{TA}, r Q_{Beto})) \end{cases}$$

$r$  : elemento aleatório de  $F_q$

Analogia: envelope com carta

PKI não é mais necessária

# Chaves públicas com prazo

- Sistemas baseados em dados pessoais permitem chaves públicas com prazo de validade pré-estabelecido.

basta acrescentar o período de validade no ID:

- Exemplos:

ID = Alice@ime.usp.br || 2003 ou

ID = Alice@ime.usp.br || abril2003

conforme a necessidade.

Revogação de chave  
não é mais necessária

# Viagem com um *notebook*

Suponha que Beto vai fazer uma viagem de 7 dias.

Em vez de colocar sua chave particular padrão no *notebook* e correr o risco de haver comprometimento em caso de roubo,

Ele pode instalar em seu *notebook* as chaves particulares correspondentes aos 7 dias de viagem, da seguinte forma:

- Seja  $(s, \mathbf{R}_{Beto} = s\mathbf{P})$  o par de chaves padrão de Beto (Beto vai agir como TA).

- Beto gera:  
$$S_{Beto\_data1} = sH_1((ID_{Beto} || data1))$$
$$S_{Beto\_data2} = sH_1((ID_{Beto} || data2))$$

...

$$S_{Beto\_data7} = sH_1((ID_{Beto} || data7))$$

(continua)

# Viagem com um *notebook*

Digamos, então, que Alice quer enviar uma mensagem sigilosa  $m$  para Beto na data “ $data\_1$ ”:

- Calcula  $U = rP$ ,  $r$  elemento aleatório de  $F_q$ ;
- Calcula  $V = m \oplus H_3(t(R_{Beto}, r Q_{Beto}))$   
onde  $Q_{Beto} = H_1(ID_{Beto} || data\_1)$ ;

- Envia  $(U, V)$  para Beto;

- Beto calcula  $V \oplus H_3(t(U, S_{Beto\_data1}))$  e recupera  $m$

# Divisão por tipo de assunto

- Suponha que Alice envia uma mensagem para Beto usando o campo “assunto” concatenado com o ID dele.
- Beto, agindo como TA, pode, através de sua chave particular padrão, gerar a chave particular correspondente e decifrar esta mensagem.
- Ex. Alice criptografa uma mensagem usando como
$$Q_{Beto} = H_1(\text{ID}_{Beto} \parallel \textit{assunto})$$
- Beto gera a chave particular  $S_{Beto}$  correspondente e consegue ler a mensagem.

# Divisão por tipo de serviço

- Suponha: Beto possui vários assistentes, cada um responsável por um Departamento (Ex. RH, Finanças).
- Beto pode gerar uma chave particular baseada em dados correspondentes a cada Depto.  
cada Depto. pode decifrar as mensagens de sua responsabilidade,  
mas não consegue decifrar as mensagens dos outros Departamentos.
- $S_{RH} = s H_1(\text{ID}_{\text{Beto}} \parallel \text{RH});$
- $S_{\text{Finanças}} = s H_1(\text{ID}_{\text{Beto}} \parallel \text{Finanças});$

Note que Alice (remetente) só precisa obter os parâmetros públicos  $(R_{\text{Beto}}, Q_{\text{Beto}})$

# Criação de grupos

Suponha que Beto acabou de chegar à cidade para uma reunião.

Mas Beto não conhece ninguém além da Alice. Beto deseja que Alice o pegue no aeroporto, mas como Alice não pode ir, algum amigo de Alice o fará.

Mas como Beto vai disseminar uma mensagem para os amigos da Alice, se ele não os conhece ?

(continua)

# Criação de grupos

Seja  $R_{Alice} = sP$  o par de chaves pública/ particular padrão da Alice.

Alice gera um par de chaves  $(S_{Amigo}, Q_{Amigo})$ , usando como chave pública o hash do identificador *Amigo*.

Ao chegar à cidade, Beto pode criptografar uma mensagem com o par de chaves  $R_{Alice}, Q_{Amigo}$ :

$$U = rP \quad V = m \oplus H_3(t(R_{Alice}, r Q_{Amigo})),$$

e só os amigos de Alice, que possuem  $S_{Amigo}$ , poderão decifrá-la.

# Bibliografia

## Segurança de Dados: Criptografia em redes de computador

Go EDUAR A. POE, Esp.

De qij OGXEW PqFyá ngUH LIA VQSMQs  
noTjps SNB wqL-NKBYD JCP rAdH HnZouoQ  
waxpú qy nQpóhL AAO bFXTZEXE ghuMqsa Ua  
QxvBXPtE yQandUd qA qLAAz avz rcdDYRQ  
nos xFKxof ZpNacaa qd oua oua zqñ Mh  
wVpúKzE yml vna AkaO iyaIDV haaBqyqy  
SzZl QÉpúSW bGenah aNjua wqyáLFA xabXDi  
mÉ JCl qdK ofYLAGT nQOTv qe Qes wTQDP  
SEB nyleLqñ Lpa mBua wds diay AAO cÉpúwqé  
xáZ eH eMq xvKqgn HdwvW qdF qTno davi avz  
Uuacane uk VFEIA IDah XpúXTIax Yc qe wqFqW  
XQZmaUZaxus zé z AqOia unoz noc QHOQBS  
NBH EmMq nk Looza SAlaqgl NQZu qrtjq Lowaf  
KZnk Cia at AhX JwawyaUjdy QDaaBaa  
bzqL Lrtah zW wTLYdy LIA VqgáMFTv  
rAGHEP qaa xNof dno wawQdñq JdA qñz  
kyóXQxje zé ymú. rQhgmxva dno wUkL qñ  
AQGb mfo wYwaaQD car jax wacñh qáWw  
Cto o yx qno JdGtzaP rax Vnkqes QLxh  
qñJaa qñqño hudaA h wafA e puaEdo vna wñ  
Kj emy Lu qñz

autor: Routo Terada (USP)

(à venda nas livrarias da FEA e da Escola Politécnica)

Nos últimos anos tem havido um avanço na popularização da rede Internet e o advento das chamadas “lojas virtuais” para comércio pela Internet, e das “home-bankings” que possibilitam transações bancárias através de uma senha. Por outro lado, com a Internet, a proteção da privacidade se tornou extremamente importante para cada cidadão, pois os seus dados pessoais trafegam na Internet, possibilitando falsificações e fraudes eletrônicas, além de disseminação de vírus eletrônicos. Criptografia é a chave que permite solucionar tecnologicamente estes problemas. Os objetivos deste livro são de apresentar os problemas e de fornecer as respectivas soluções práticas em segurança de redes de computador. São: Aplicações e técnicas de proteção de informação sigilosa. Autenticação da origem e destino de documentos eletrônicos: assinatura eletrônica. Técnicas de identificação de usuários em redes de computador: proteção de cartão magnético de identificação ou senha. Proteção de integridade de banco de dados. Detecção e controle de presença de vírus eletrônico.

Os algoritmos DES e RSA, largamente utilizados em sistemas comerciais, são detalhados e analisados. Além do RSA, são descritos outros algoritmos de chave pública. Ademais são apresentados algoritmos de “hashing” e de compactação. Há informações sobre os sistemas PGP, TLS, e um programa RSA na linguagem Java.

É destinado tanto para profissionais de Informática, de Telecomunicações, como de Engenharia de Computação. É apropriado também para estudantes, para estudo autônomo, ou para consultas.

## Bibliografia

International Association for Cryptologic Research

<http://www.iacr.org/>

Electronic Proceedings of the Eurocrypt and Crypto Conferences  
1981-1997, Kevin S. McCurley and Claus Dieter Ziegler, Editors,  
Springer-Verlag 1998

<http://www.iacr.org/cd/>

## Livros

1. Douglas Stinson: Cryptography, CRC-Press 1995
2. Al Menezes et al.: Applied Cryptography, CRC-Press, 1997
3. R. T., Segurança de dados em rede de computadores, Ed. E. Blucher, 2000

## Problema do logaritmo discreto (PLD)

- Dados  $a$ ,  $p$  e  $x$ , é “fácil” calcular  $y = a^x \bmod p$ ;
- Porém, dados  $a$ ,  $p$  e  $y$ , é “difícil” calcular  $x$ .

## **Em Curvas Elípticas (PLD-CE)**

- Dados  $s$  e  $P$ , é “fácil” calcular  $R = sP$
- Porém, dados  $R$  e  $P$ , é “difícil” calcular  $s$ .