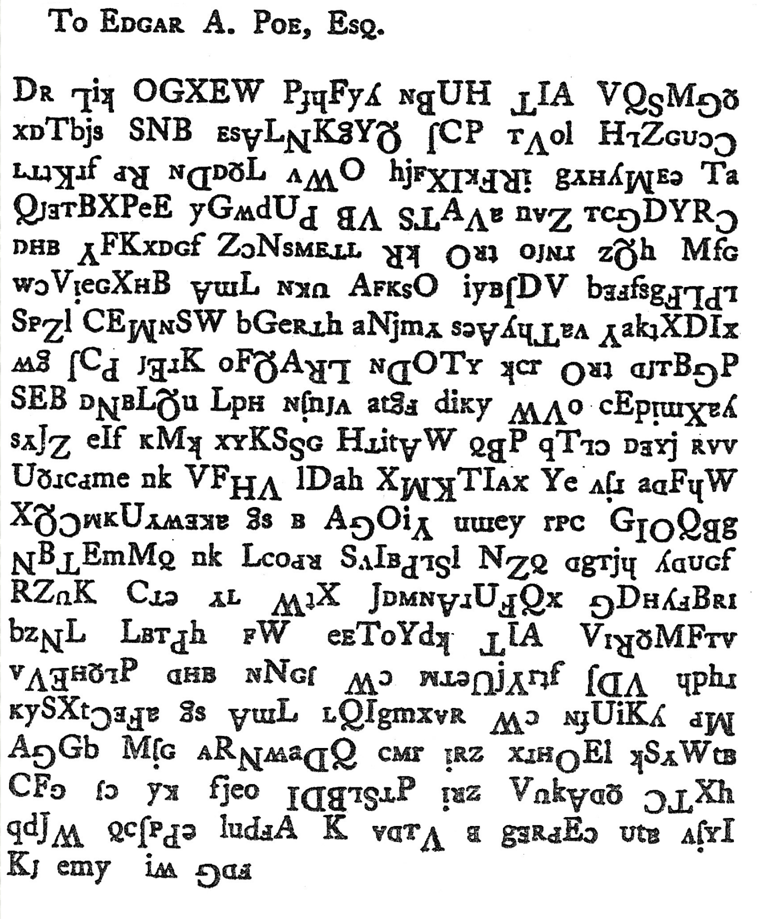
Segurança de Dados – Criptografia

Routo Terada

www.ime.usp.br/~rt

Depto. Ciência da Computação - USP

Livro: Segurança de Dados, R. Terada, Edit. Blücher, ano 2008,



To Edgar A. Poe, Esq.

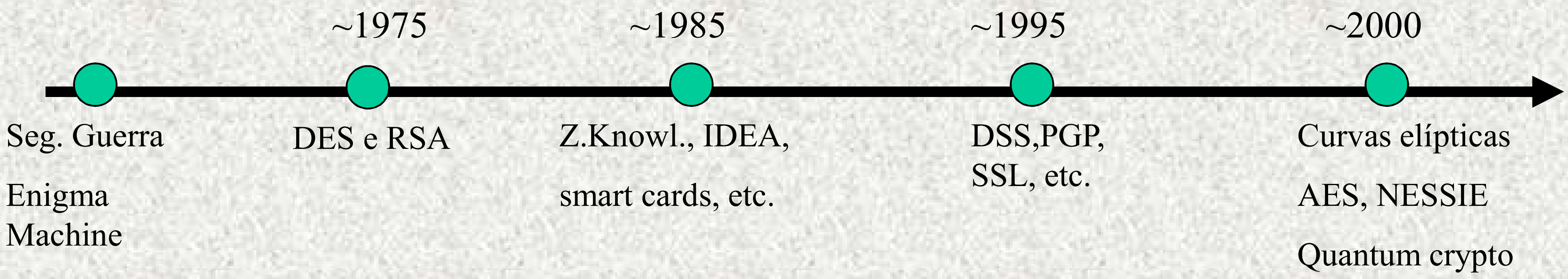
```
DR ꓕiʞ OGXEW PjqFyʎ NgUH ꓕIA VQSMꓨȣ
xDTbjs SNB esⱯLNKȣYȣ ʃCP TɅol HꓕZGUↃↃ
ꓕꓕɹʞɹf dɹ NᗡpȣꓶL ʌMO hjFXꓶꓘɟɹ! gxHʎWƐƐ Ta
QJƐTBXPeE yGʍdUd ꓭɅ SꓕⱯɅɐ nʌZ TCꓨDYRↃ
DHB ⅄FKxDGf ZↄNsMEꓕꓕ ʞꓤ Oɹʇ OJNI zȣh MfG
wↄVieGXHB Ɐɯꓕ Nʞn AFKsO iyBʃDV bɐɟɟsgꓞꓒꓕ
SPZl CEꟽNSW bGeRꓕh aNjmx sɔⱯʎɥꓕɐʌ ⅄akɹXDIx
ʍg ʃCd JꓱɹK oFȣⱯꓤꓕ NᗡOTY ʞɔɹ Oɹʇ ɑJTBꓨP
SEB DNBLȣu LpH Nʃnjʌ atgɟ diky ꟽɅo cEpiɯXɐʎ
sxJZ eIf KMʞ xYKSSG HꓕitⱯW ǫgP qꓕɹↄ DƐxj RVV
Uȣɪcame nk VFHɅ lDah XꟽꓘTIAx Ye ʌʃɹ aɑFɥW
XȣↃWKUxʍƐʞɐ gs B AꓨOi⅄ uɯey rPC GIOQgg
NBꓕEmMQ nk Lcoɐꓤ SɅIBꓒꓕSl NZQ ɑgTjɥ ʎɑUGf
RZnK Cꓕↄ xL ꟽɹX JDMNⱯɹUꟻQx ꓨDHʎɟBRI
bzNL LBTꓒh FW eETɔYdʞ ꓕIA VIꓤȣMFTV
VɅƎHȣꓕP ɑHB NNGʃ ꟽↄ MꓕƐUjʎɹɟ ʃDɅ ɥphɹ
KySXtↃƐꟻɐ gs Ɐɯꓕ ꓕQIgmxʌR ꟽↄ NɟUiKʎ ꟽd
AꓨGb Mʃɢ ARNꟽaᗡQ CMɹ !RZ XIHOEl ʞSxWɐB
CFↄ ʃↄ ʎx fjeo IᗡBꓕSꓕP !ɹz VnkⱯɑȣ ↃꓕXh
qdJꟽ Qcʃꓒɔ ludɟA K ʌɑꓕɅ ɐ gɐꓤɟƐↄ uɐɐ ʌʃʎI
KJ emy iꟽ ꓨɑɟ
```

Resumo

- Técnicas de proteção de informação sigilosa
- Autenticação do remetente e destinatário de documentos eletrônicos: assinatura digital/criptográfica
- Proteção de integridade de banco de dados
- Pretty Good Privacy – PGP
- Gnu Privacy Guard - GPG

Breve histórico

- Algoritmos eram *secretos* até meados de 1970
- Década de 1970: algoritmos DES e RSA *públicos*
- Segurança baseada *só* no segredo da chave
- Criptanálise dos algoritmos feita por *especialistas*
- Aprimoramentos sucessivos em (1) *segurança* e (2) *velocidade*



Seg. Guerra

Enigma Machine

~1975

DES e RSA

~1985

Z.Knowl., IDEA,

smart cards, etc.

~1995

DSS,PGP, SSL, etc.

~2000

Curvas elípticas

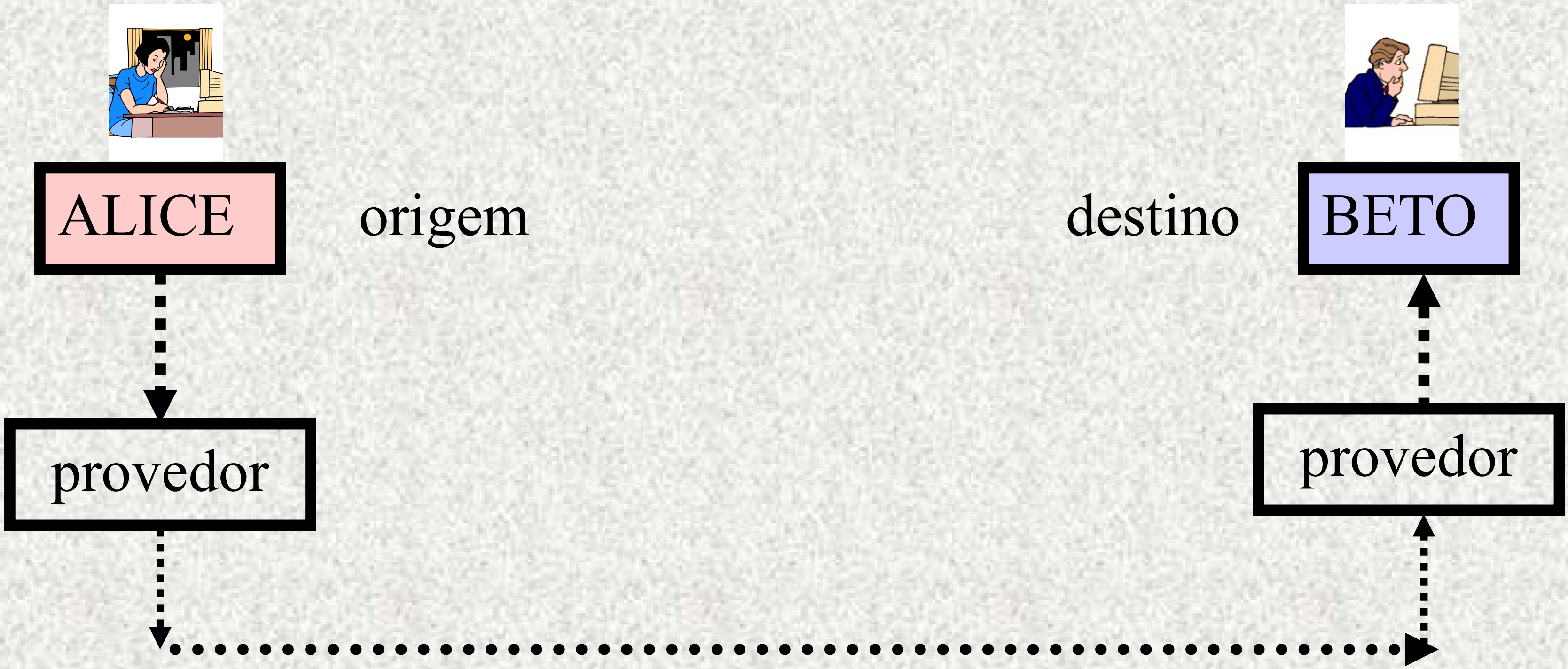
AES, NESSIE

Quantum crypto

Pesquisas Recentes

- Identity Based Encryption: chave pública pode ser, por exemplo, o no. CPF
- Certificateless Public Key Encryption: chave pública pode ser o endereço Email
- Computador quântico
- Criptografia quântica
- Criptografia pós-quântica

Cenário geral



ALICE

origem

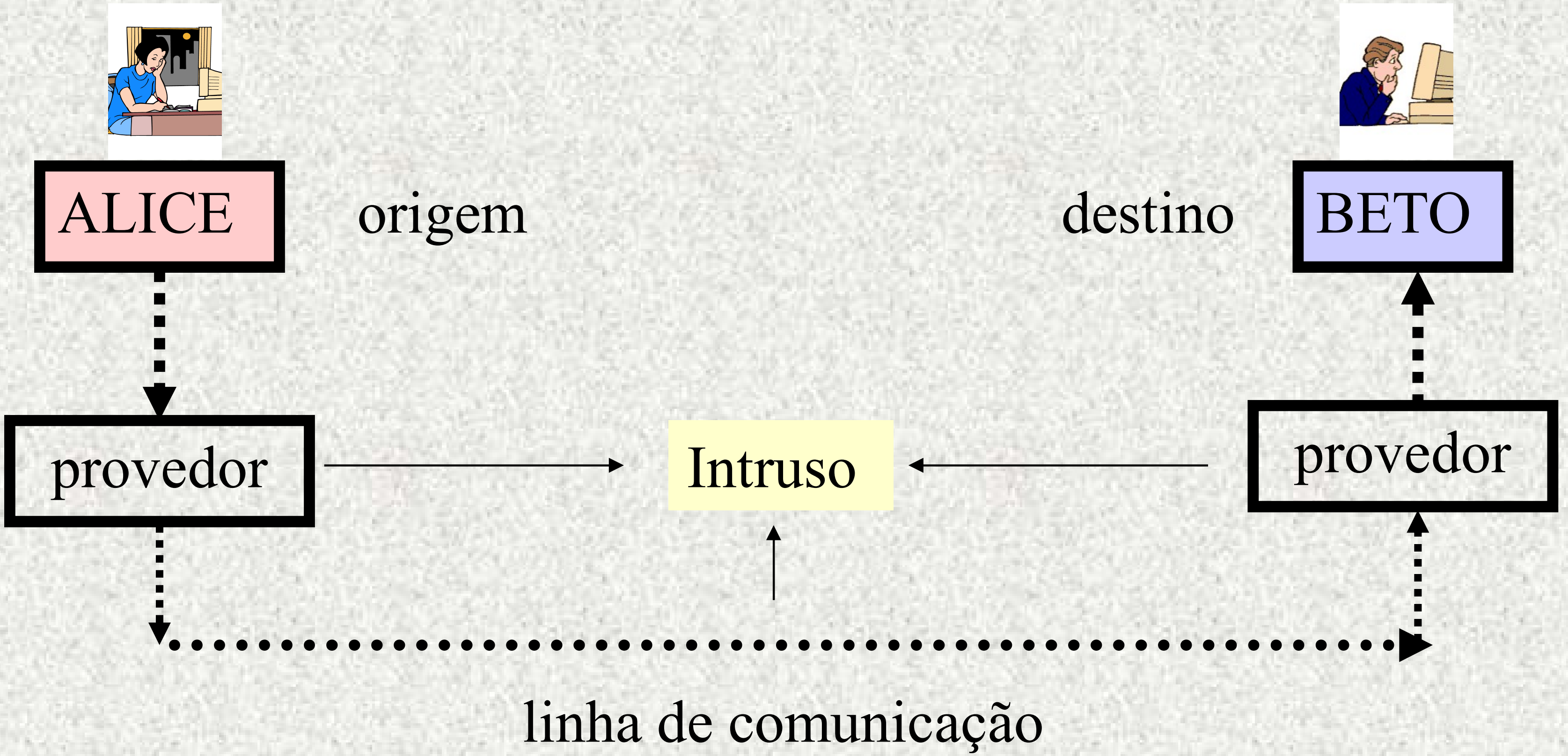
destino

BETO

provedor

provedor

linha de comunicação



ALICE

origem

destino

BETO

provedor

Intruso

provedor

linha de comunicação

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

CIFRA DE CÉSAR

legível	A	B	C	D	E	F	G	H	I	J	K	L	M
ilegível	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*

legível	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ilegível	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	*A*	*B*	*C*

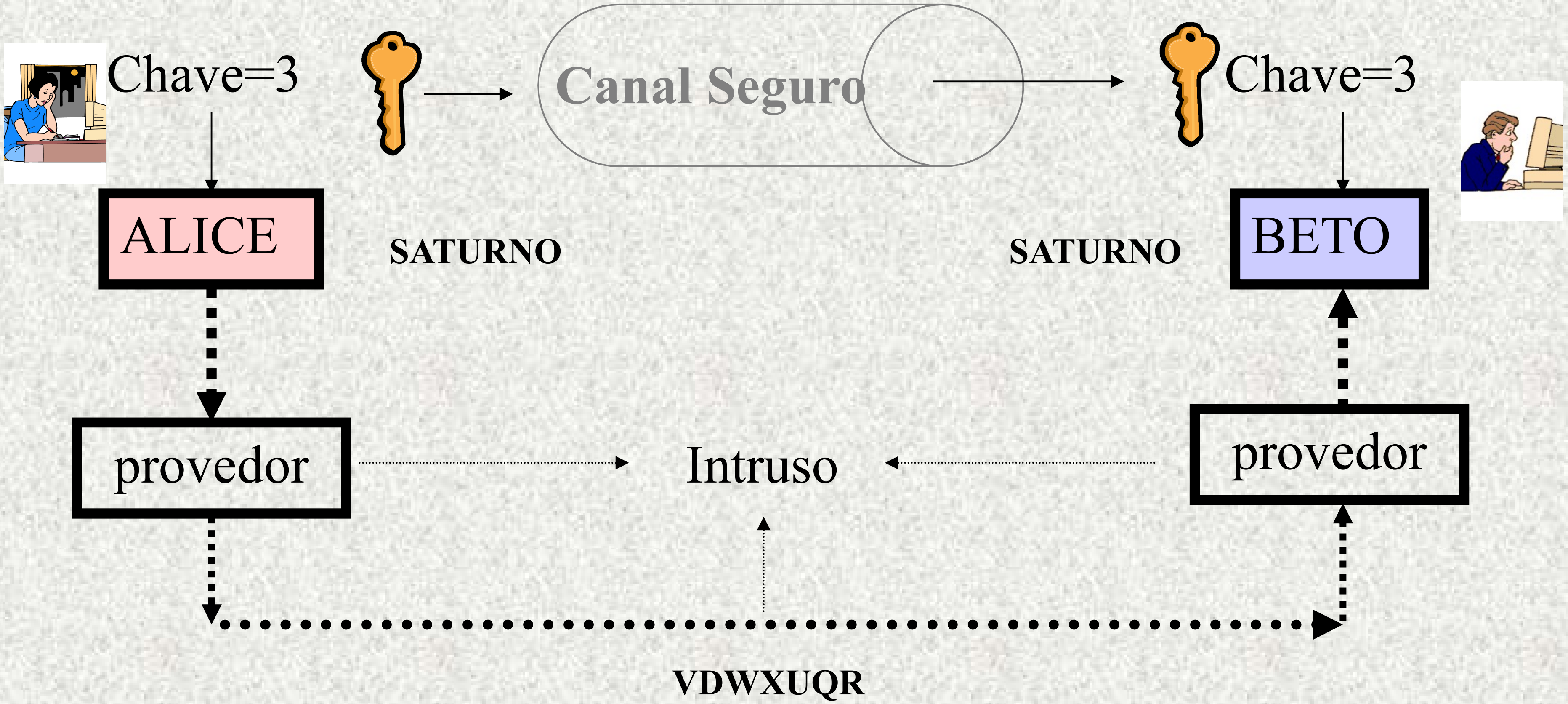
$\xrightarrow[3]{}$

Chave=3

legível	S	A	T	U	R	N	O
ilegível	*V*	*D*	*W*	*X*	*U*	*Q*	*R*

Total de 25 chaves, preserva frequência das letras, fraco

Cifra de César



Chave=3

Canal Seguro

Chave=3

ALICE

SATURNO

SATURNO

BETO

provedor

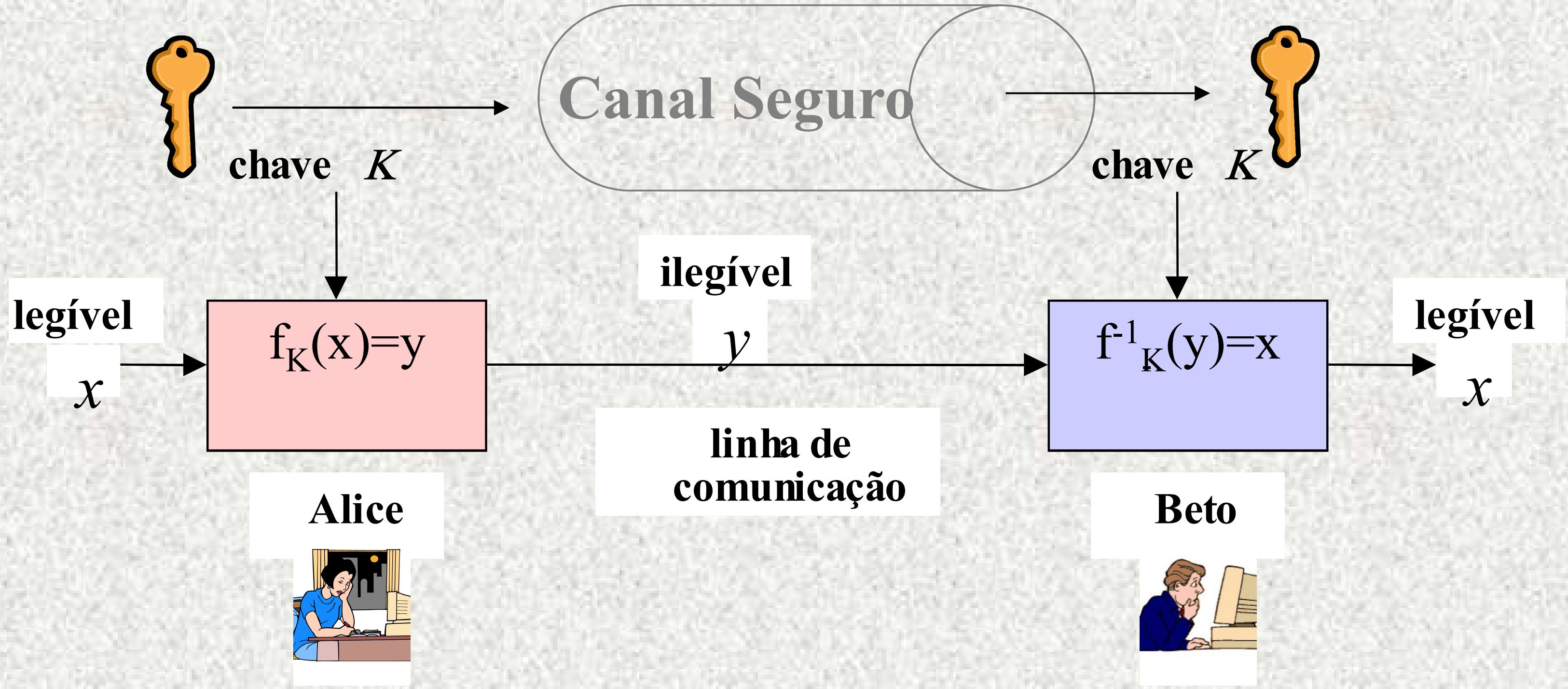
Intruso

provedor

VDWXUQR

Objetivo: VDWXUQR ilegível para o Intruso

Formalmente tem-se uma função matemática e sua inversa



Canal Seguro

chave K

chave K

legível

x

$f_K(x)=y$

ilegível

y

linha de comunicação

$f^{-1}_K(y)=x$

legível

x

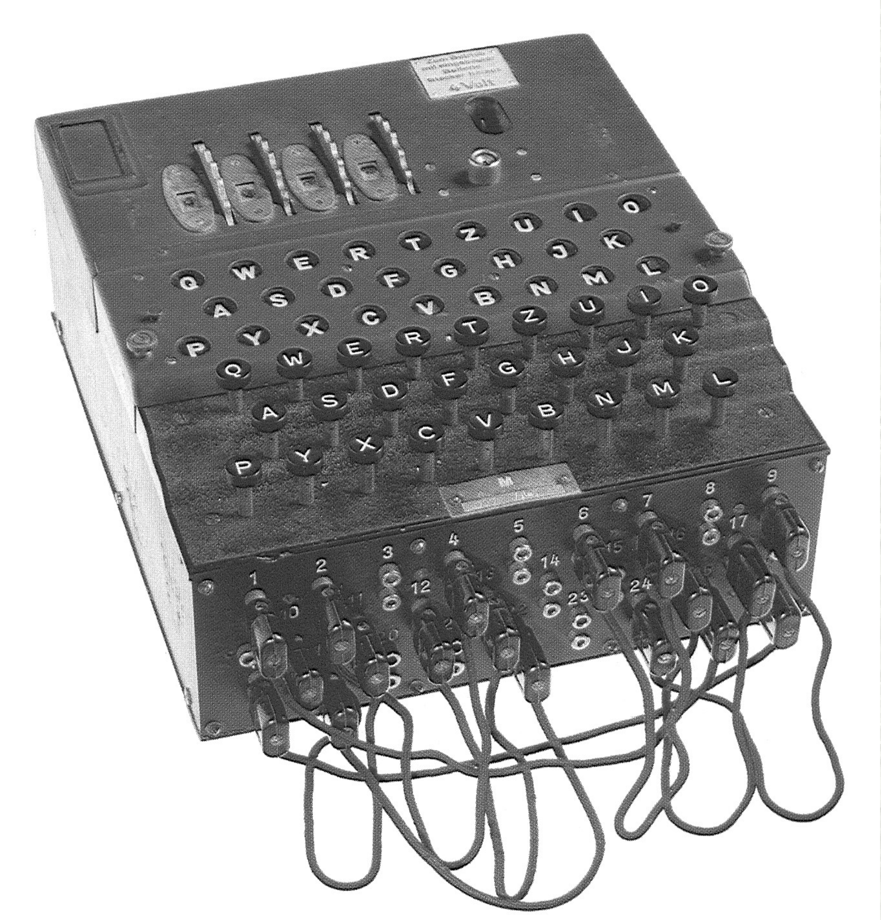
Alice

Beto

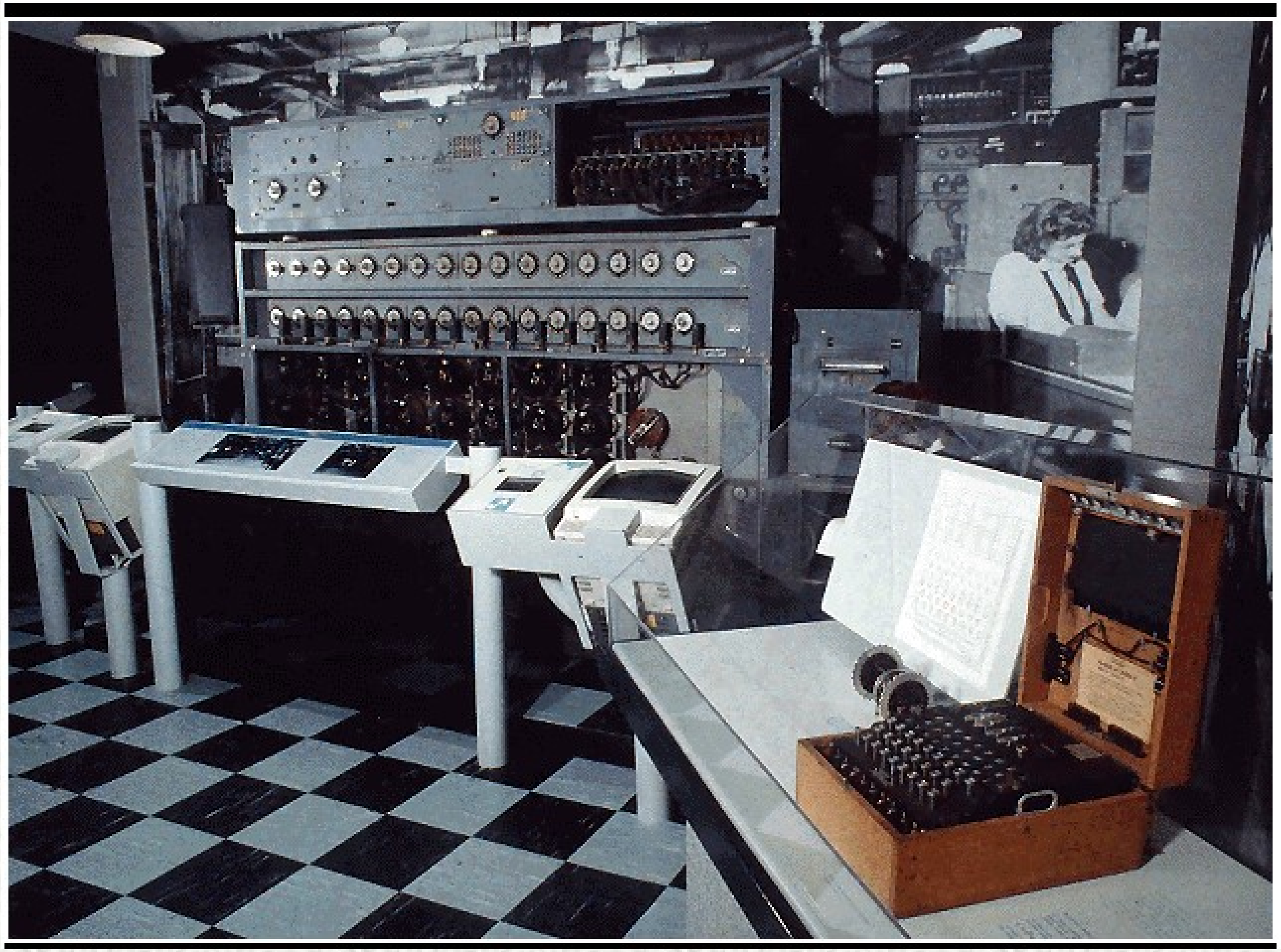
Problema importante: necessidade de combinar previamente a chave K de maneira totalmente segura

N usuários → N*N chaves

ENIGMA – máquina criptográfica alemã (II Guerra Mundial)



ENIGMA e a máquina BOMBE



Pontos importantes

- "insider" - maioria dos crimes eletrônicos causados por "insiders"
- tecnologicamente, manter um passo à frente dos criminosos
- só senha - proteção fraca
- insegurança eletrônica é invisível
- muitos crimes não deixam rastros

Como descobrir uma chave DES?

2^{56} chaves possíveis

Criptanálise Diferencial – 2^{47} tentativas

Biham, Shamir, 1990 ($2^{56}/2^{47}=512$)

Criptanálise Linear – 2^{43} tentativas

Matsui, 1994 ($2^{56}/2^{43}=8.192$)

Outros algoritmos como o DES:

- IDEA pg 57
- SAFER pg 67
- RC5 pg 71
- RC6 pg 75
- FEAL pg 81
- AES → a seguir
- etc.

Advanced Encryption Standard

http://csrc.nist.gov/encryption/aes

128 bits de chave

Algoritmo	Organização
CAST-256	Entrust Technologies, Inc. (Carlisle Adams)
CRYPTON	Future Systems, Inc. (Chae Hoon Lim)
DEAL	Richard Outerbridge, Lars Knudsen
DFC	CNRS - Centre National pour la Recherche Scientifique - Ecole Normale Superieure (Serge Vaudenay)
E2	NTT - Nippon Telegraph and Telephone Corp. (Masayuki Kanda)
FROG	TecApro Internacional S.A. (Dianelos Georgoudis)
HPC	Rich Schroeppel
LOKI97	Lawrie Brown, Josef Pieprzyk, Jennifer Seberry
MAGENTA	Deutsche Telekom AG (Dr. Klaus Huber)
MARS *	IBM (Nevenko Zunic)
RC6 *	RSA Laboratories (Burt Kaliski)
RIJNDAEL *	Joan Daemen, Vincent Rijmen
SAFER+	Cylink Corporation (Charles Williams)
SERPENT *	Ross Anderson, Eli Biham, Lars Knudsen
TWOFISH *	Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson

(*) cinco finalistas na competição (New York -NY, Abril 13-14, 2000)

AES - Advanced Encryption Standard
* sucessor do DES a partir de 2002 *

NIST

- Competição internacional aberta desde 1997
- Bloco de 128 bits na entrada e na saída
- Chave de 128 ou 192 ou 256 bits
- Segurança e velocidade igual ou superior a *Triple-DES*
- Deve ser implementável eficientemente em soft/hard/smart-card
- RIJNDAEL -Joan Daemen, Vincent Rijmen

Criptografia de Chave Pública (permite assinatura digital)

- Modelo de Diffie e Hellman (Stanford)
- Implementado no MIT por Rivest, Shamir e Adleman – RSA
- Outras implementações:

  Rabin pg 117

  El Gamal pg 120

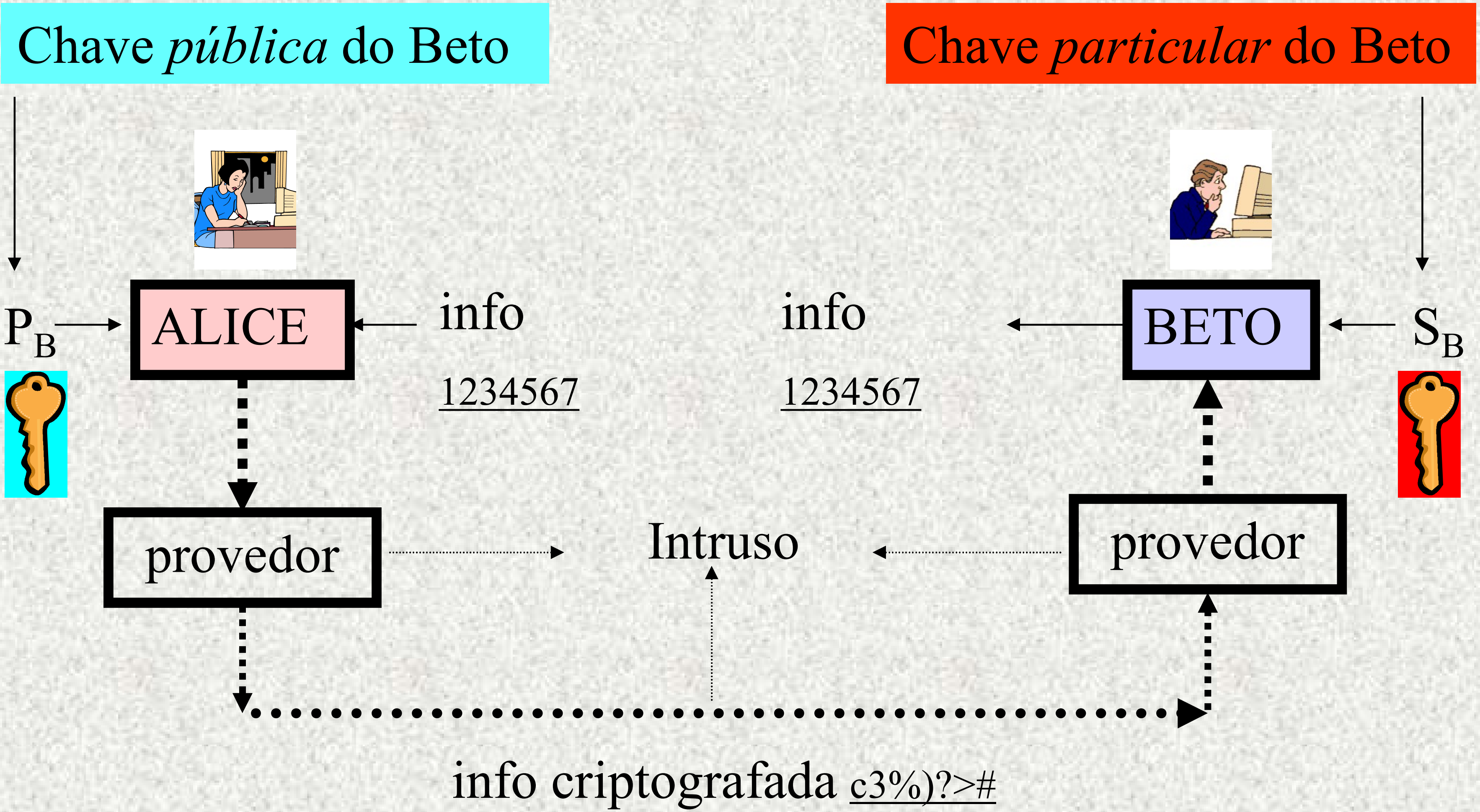
  Curvas Elípticas pg 130

  MH -- Merkle Hellman pg 142

  etc..

Modelo Diffie e Hellman (Stanford) 1976

DH



Chave *pública* do Beto

Chave *particular* do Beto

P_B

ALICE

info

1234567

info

1234567

BETO

S_B

provedor

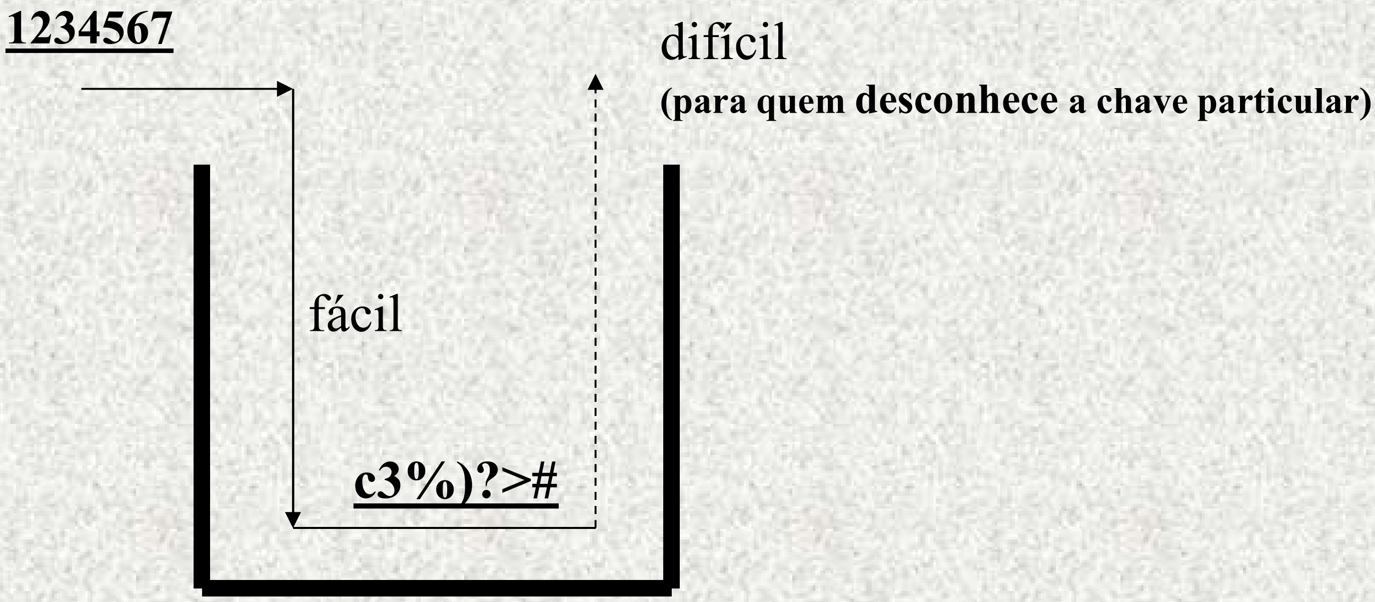
Intruso

provedor

info criptografada c3%)?>#

Objetivo: só Beto pode “abrir” a info.

Conceito: one-way trapdoor function (função unidirecional alçapão)



1234567

difícil

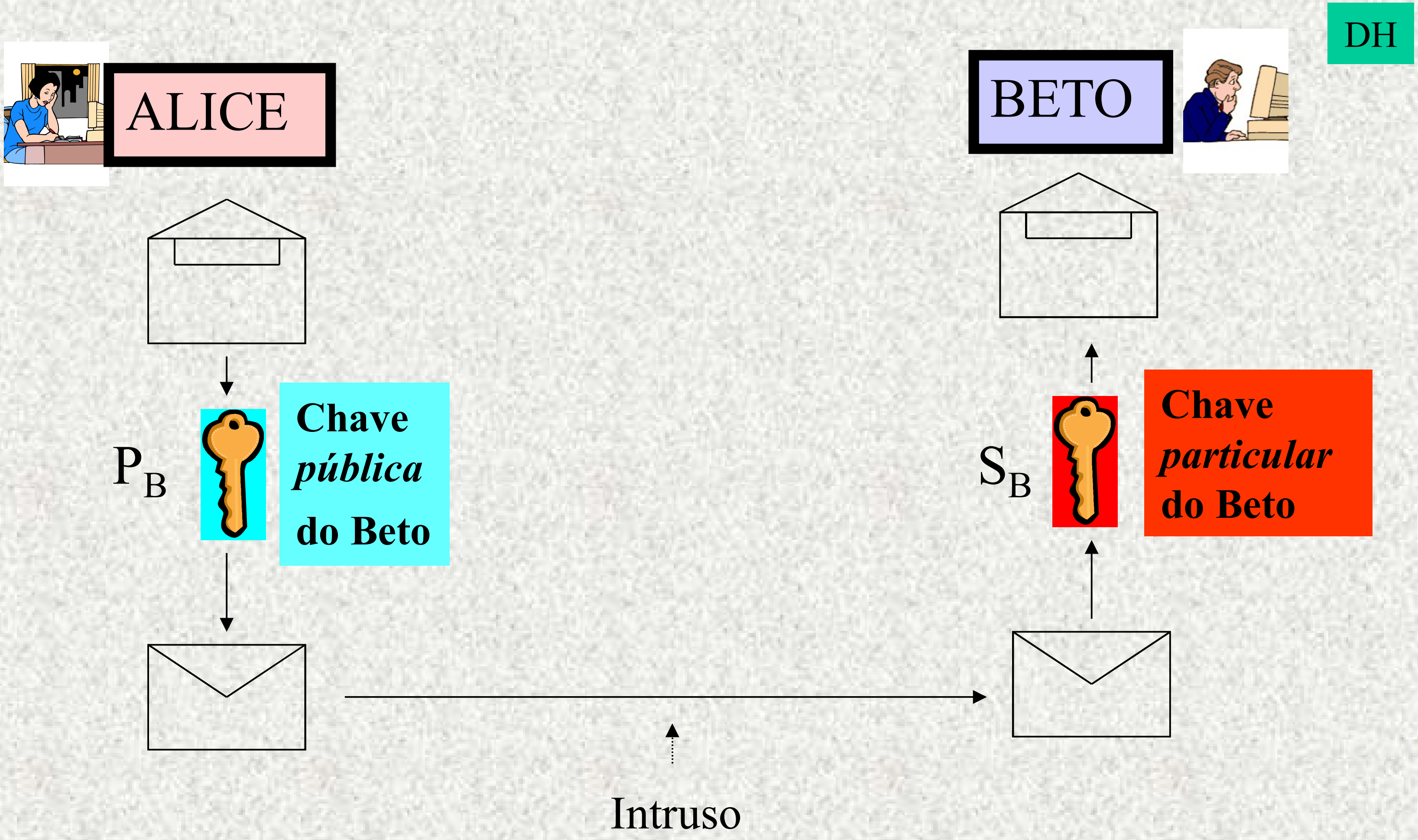
(para quem desconhece a chave particular)

fácil

c3%)?>#

função “armadilha”

DH



ALICE

BETO

P_B

Chave *pública* do Beto

S_B

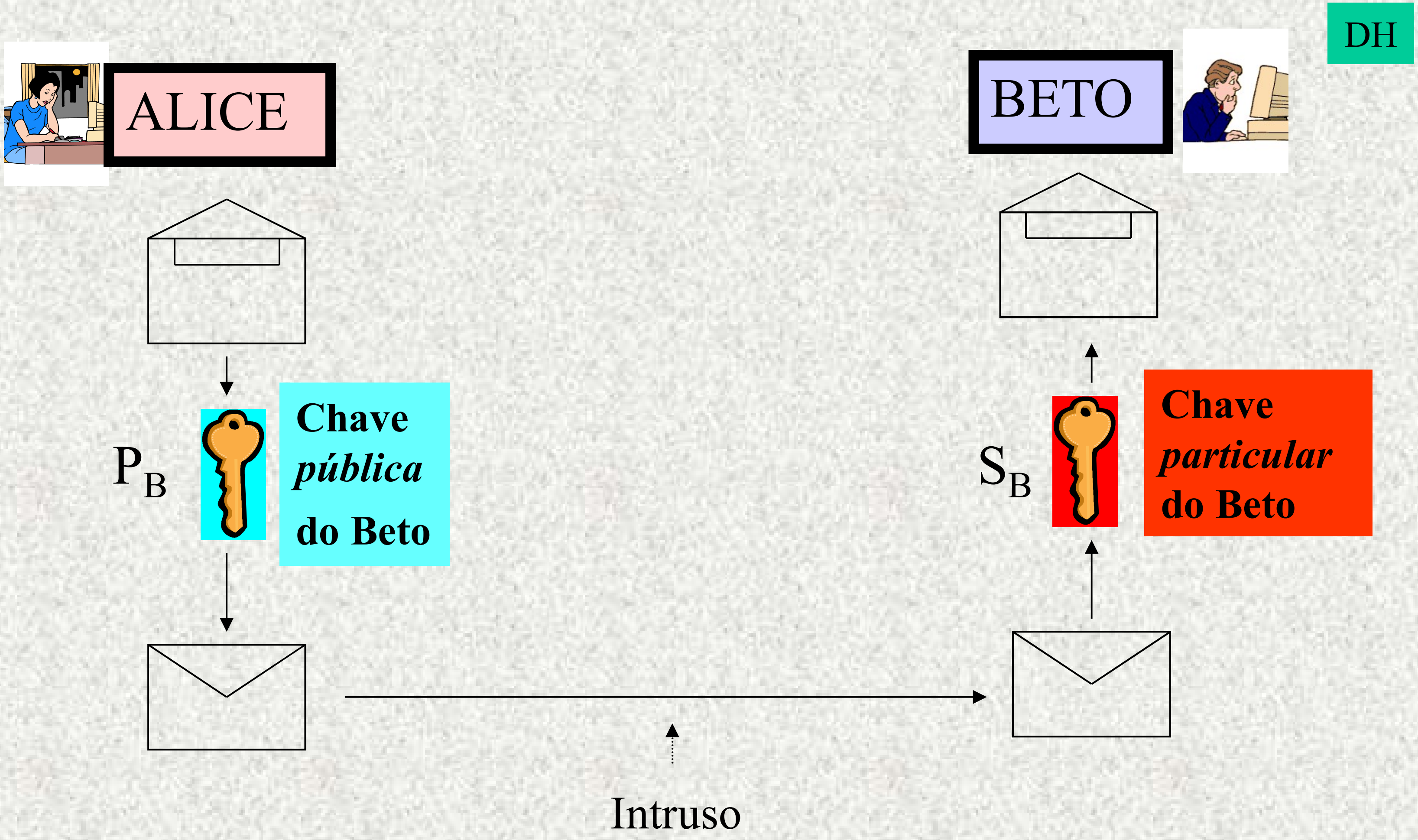
Chave *particular* do Beto

Intruso

(1) É computacionalmente inviável calcular S_B a partir do conhecimento de P_B

(2) É computacionalmente inviável "abrir o envelope" sem conhecer S_B, mas é fácil "fechar o envelope" com a chave P_B

DH



Conseqüência das duas propriedades:
Só Beto pode “abrir o envelope” pois só ele conhece a chave particular.
Isto é, há garantia de **autenticidade do destinatário**.

DH

Observação importante:

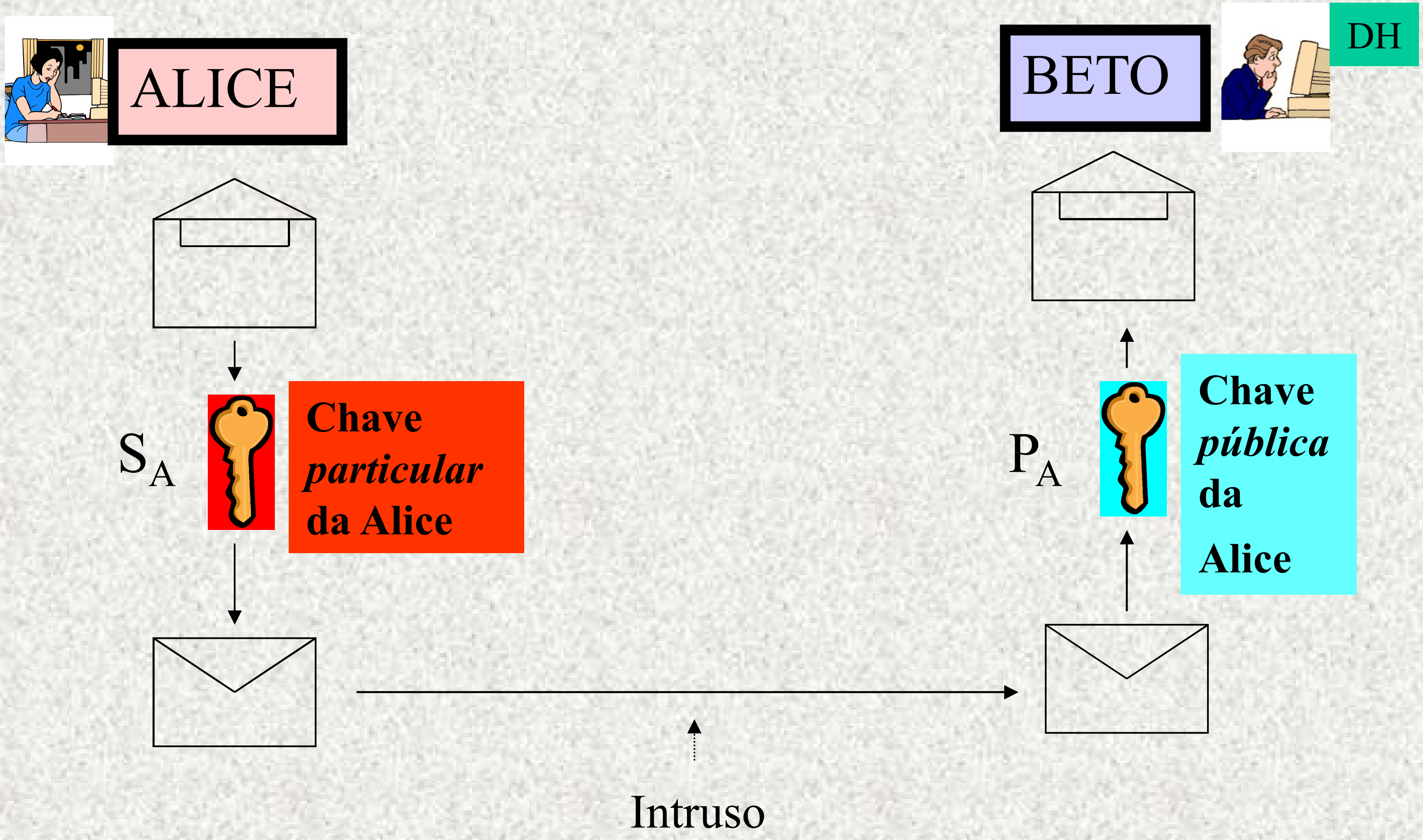
não há mais necessidade de se
combinar previamente a chave secreta,
de maneira segura
(como necessário nos casos DES e AES)
pois a chave pública pode ser até publicada
como em lista telefônica.

Lista de chaves públicas

....	
....	
Alice	821332001823410075
....	
Beto	773955910200231821
....	
....	

Idéia:
“cartório
eletrônico”

Beto, por ex., calcula o seu par de chaves, guarda a particular no seu computador e publica a sua chave na Lista de chaves públicas.



ALICE

BETO

DH

S_A

Chave *particular* da Alice

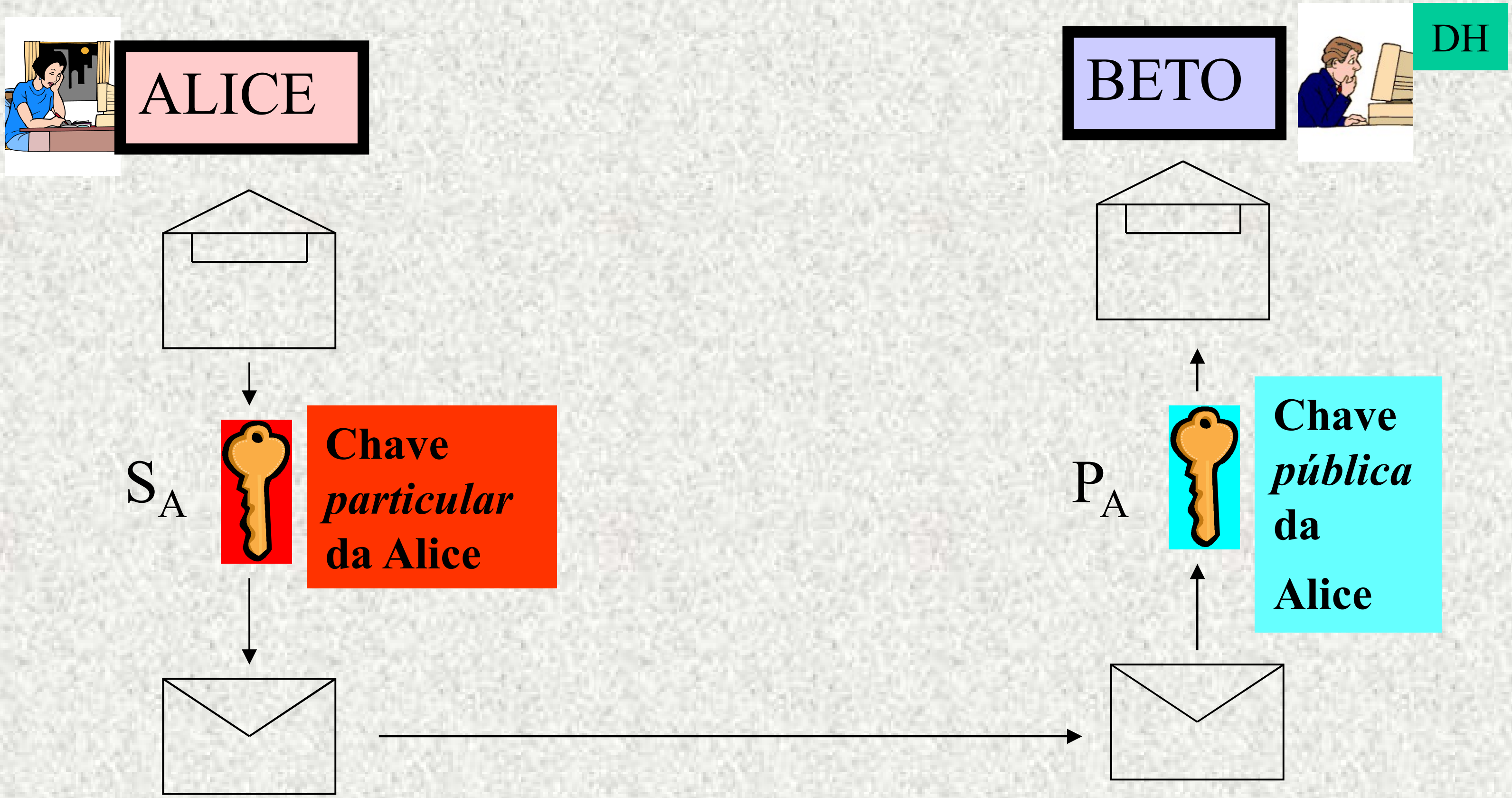
P_A

Chave *pública* da Alice

Intruso

Propriedade adicional (terceira propriedade):

(3) É possível aplicar “fechar o envelope”com a chave particular S_A e “abrir” com a chave pública P_A



ALICE

BETO

DH

S_A

Chave *particular* da Alice

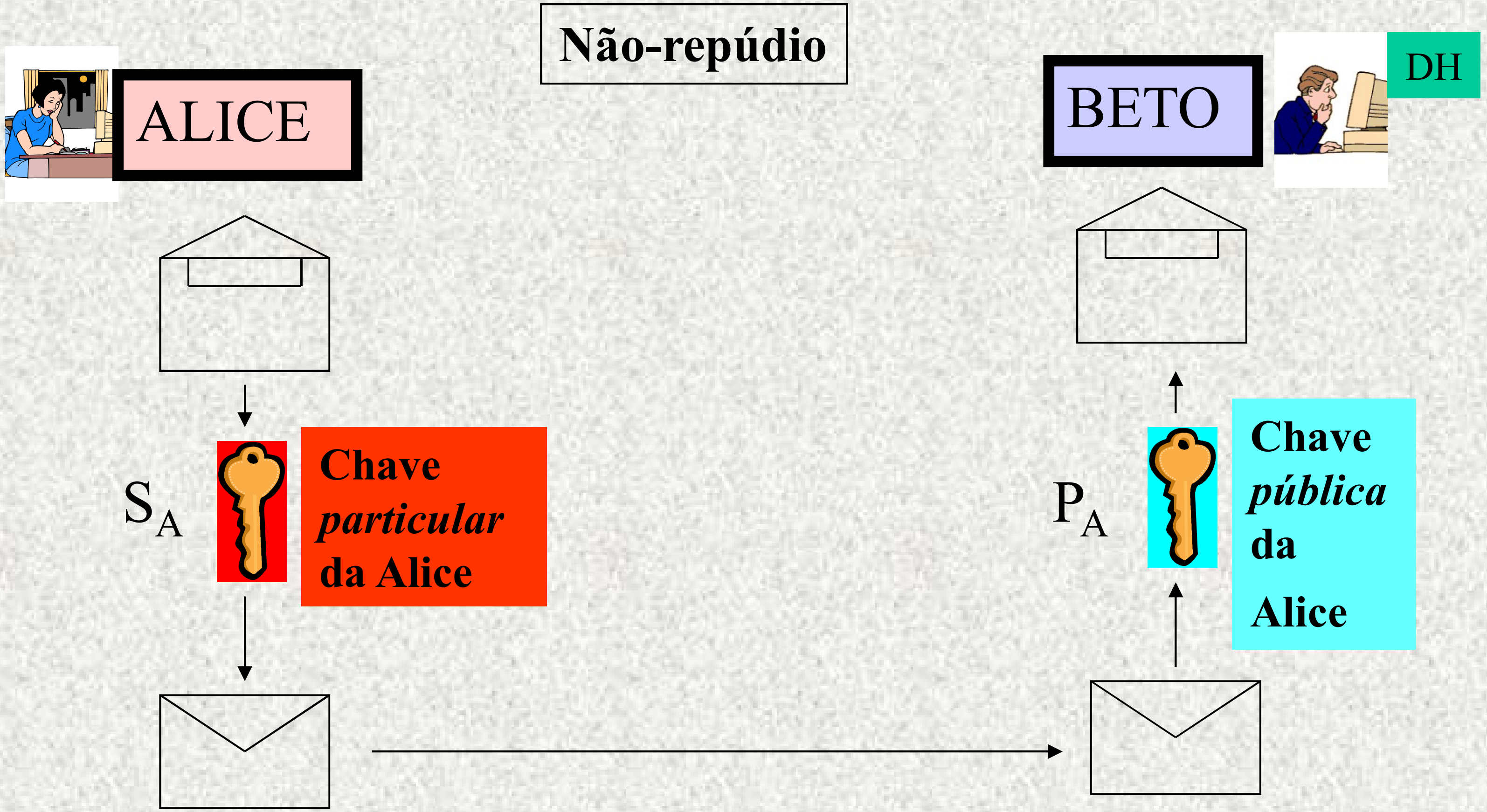
P_A

Chave *pública* da Alice

Conseqüência importante:
Beto sabe que só a Alice verdadeira pode ter enviado o envelope pois ele o abriu com a chave pública da Alice: **autenticação do remetente**
É análogo a Alice ter "assinado" eletronicamente o envelope.

(observe que senha ou DES não autentica o remetente; por quê?)

Não-repúdio



Outra conseqüência importante (não-repúdio):
Alice não pode negar que tenha enviado, pois Beto usou a chave pública da Alice para abrir: **não-repúdio da informação**
É análogo a Alice ter "assinado" um cheque.
(observe que senha ou DES não possui esta propriedade; por quê?)

RSA

Criptografia de chave pública

RSA- Rivest Shamir Adleman, 1978

***q*, *r* primos**

$$n = q \times r, mdc[s, (q-1)(r-1)] = 1, s \times p = 1 \operatorname{mod}[(q-1)(r-1)]$$

Exemplo: *q*=5, *r*=11, *n*=55, *s*=17, *p*=33, 17×33=1 mod 40

Criptografar *x* com chave pública *p*

$$x^p \bmod n = y$$

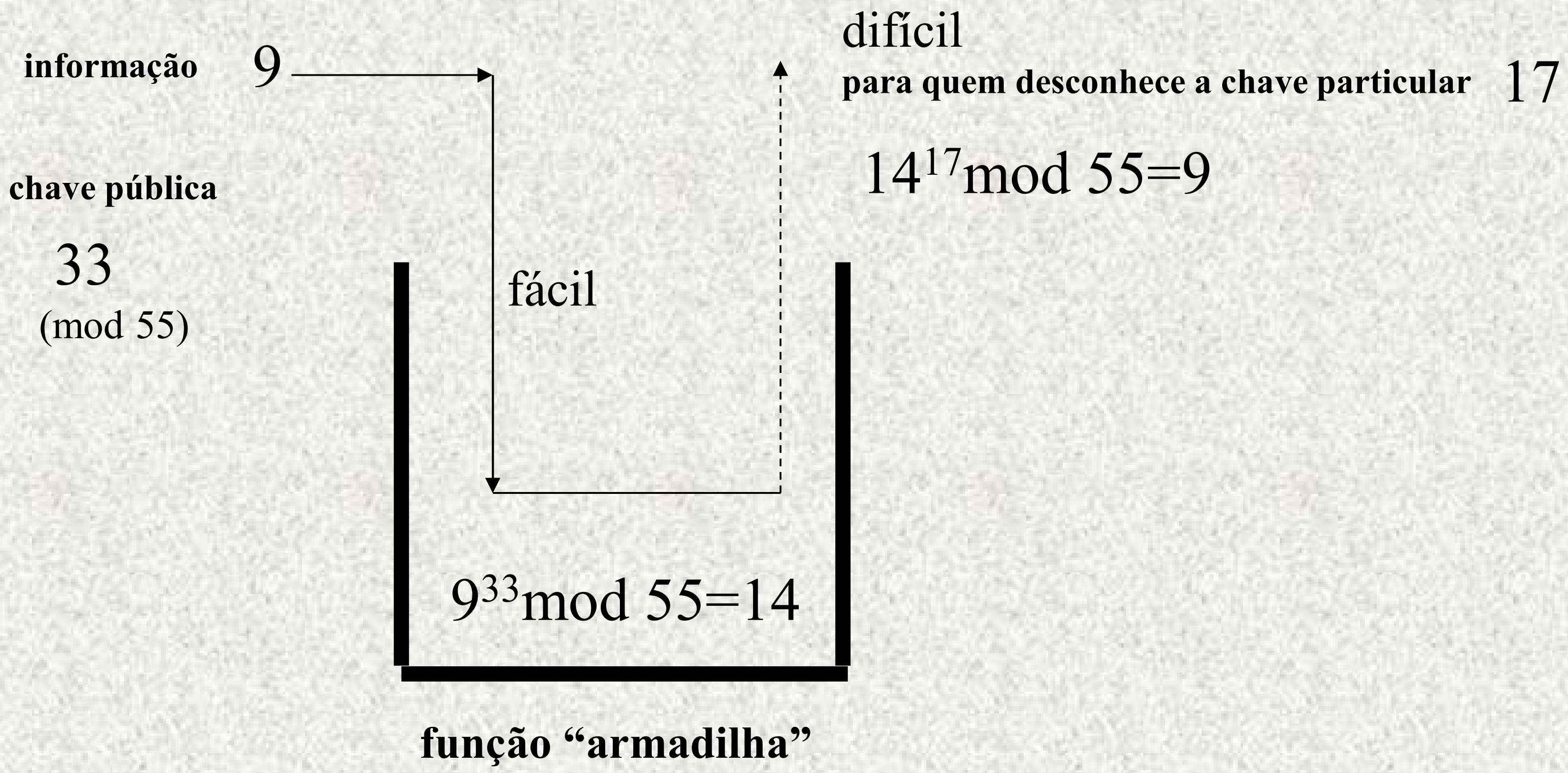
9^{33}mod 55=14

Decriptografar *y* com chave particular *s*

$$y^s \bmod n = x$$

14^{17}mod 55=9

Conceito: one-way trapdoor function (função unidirecional alçapão)



informação 9

chave pública

33

(mod 55)

fácil

$9^{33}\text{mod } 55=14$

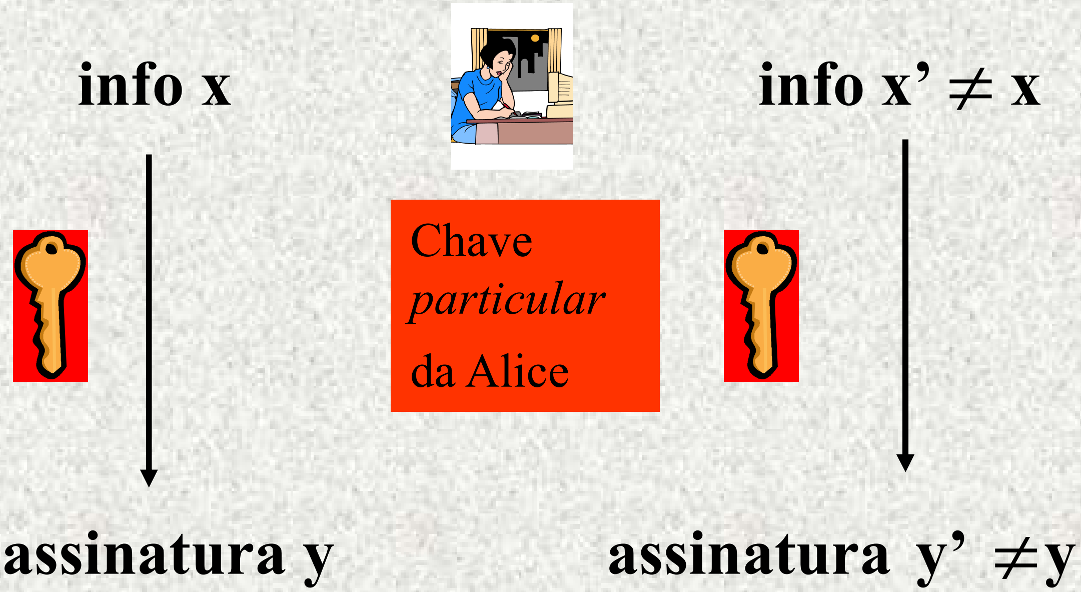
difícil

para quem desconhece a chave particular 17

$14^{17}\text{mod } 55=9$

função “armadilha”

Quando x muda, assinatura y muda correspondentemente.



info x

info x’ ≠ x

Chave *particular* da Alice

assinatura y

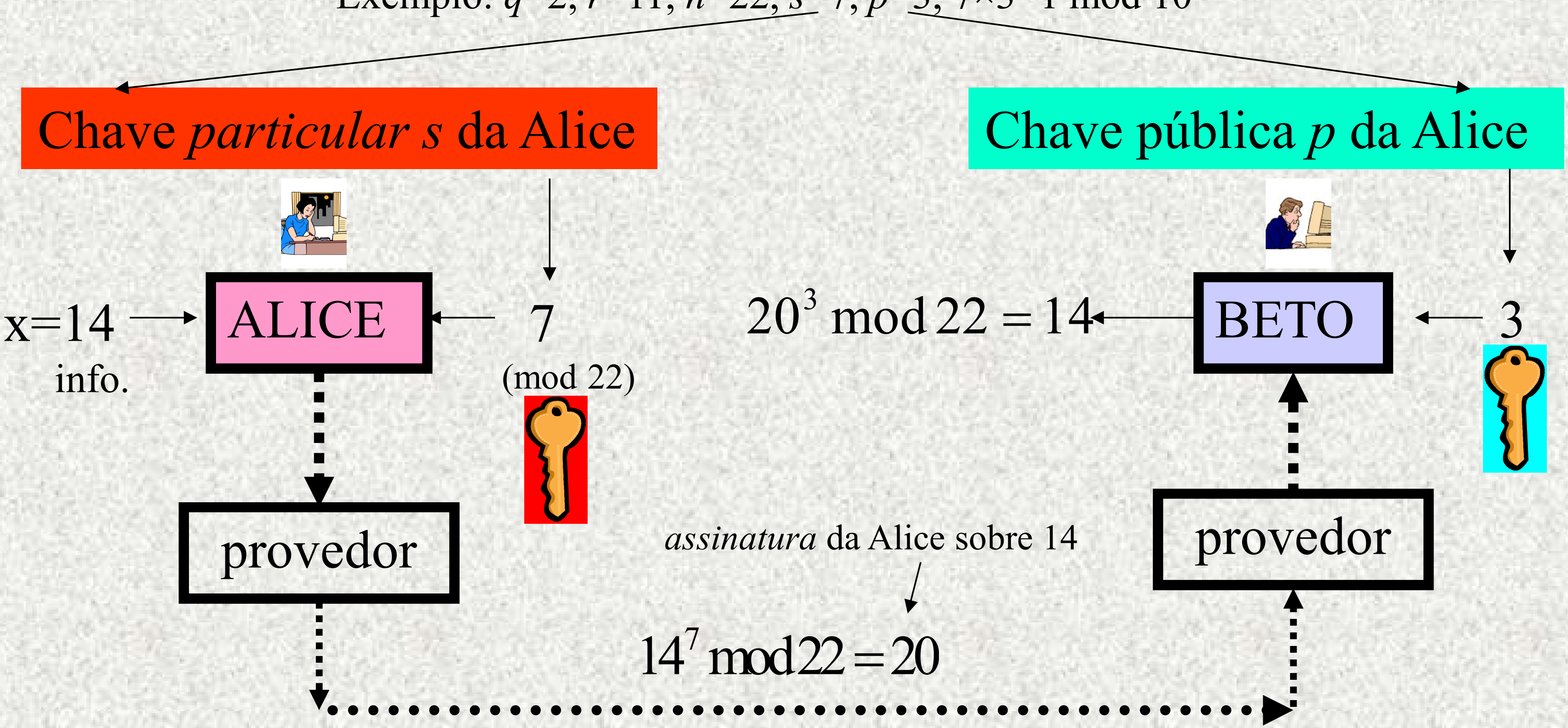
assinatura y’ ≠y

Exemplo a seguir

Integridade da informação

RSA

Exemplo: q=2, r=11, n=22, s=7, p=3, 7×3=1 mod 10



Chave *particular s* da Alice

Chave pública *p* da Alice

x=14
info.

ALICE

7
(mod 22)

$20^3 \bmod 22 = 14$

BETO

3

provedor

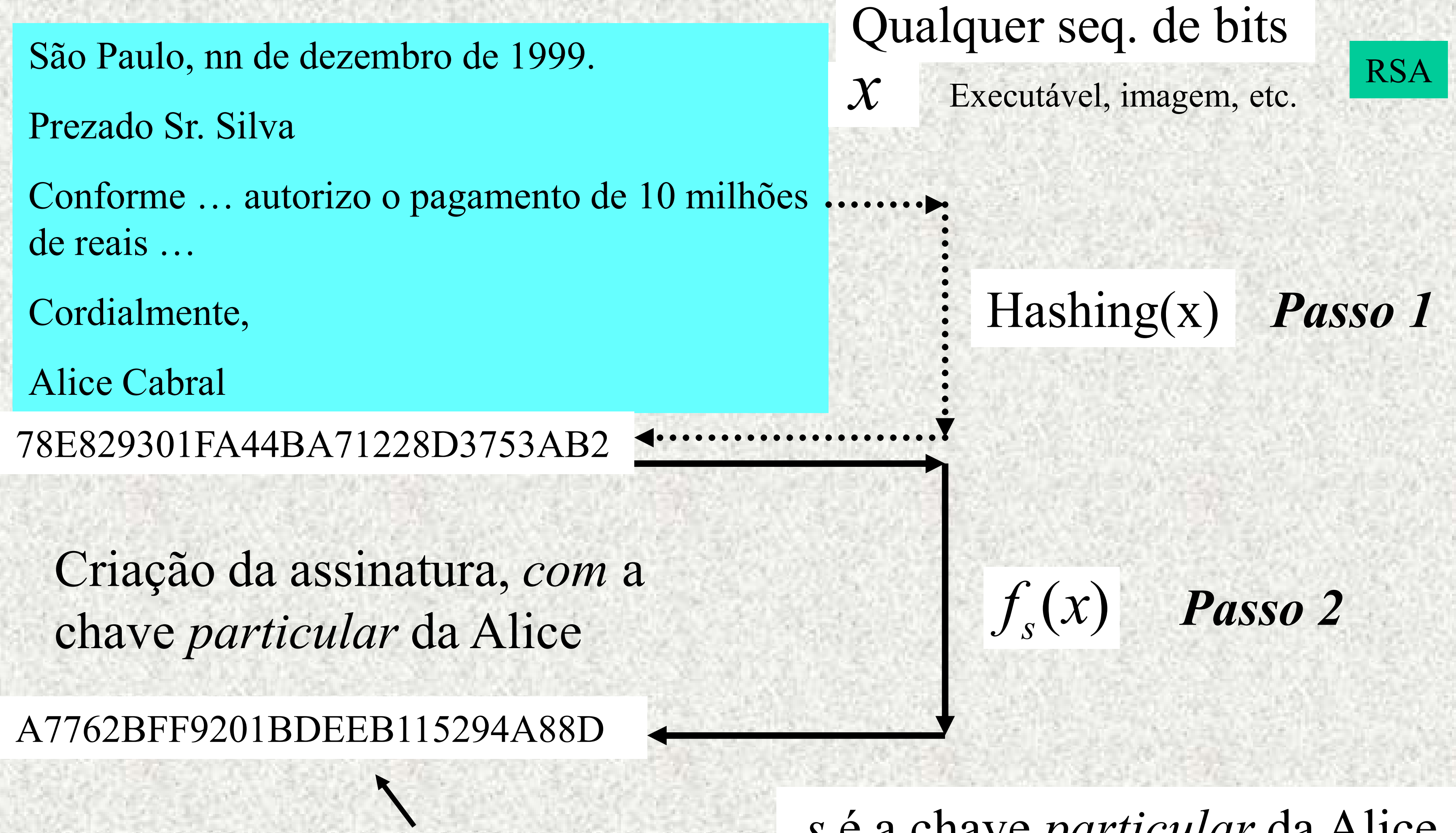
assinatura da Alice sobre 14

$14^7 \bmod 22 = 20$

provedor

Alice usa a chave particular para assinar informação x=14, distinta de 9, anterior. A assinatura y=20 é distinta de 15, anterior. Ou seja, quando x muda, y muda correspondentemente, e então a assinatura garante a *integridade da informação x.*

RSA



Qualquer seq. de bits

x Executável, imagem, etc.

São Paulo, nn de dezembro de 1999.

Prezado Sr. Silva

Conforme … autorizo o pagamento de 10 milhões de reais …

Cordialmente,

Alice Cabral

Hashing(x) ***Passo 1***

78E829301FA44BA71228D3753AB2

Criação da assinatura, *com* a chave *particular* da Alice

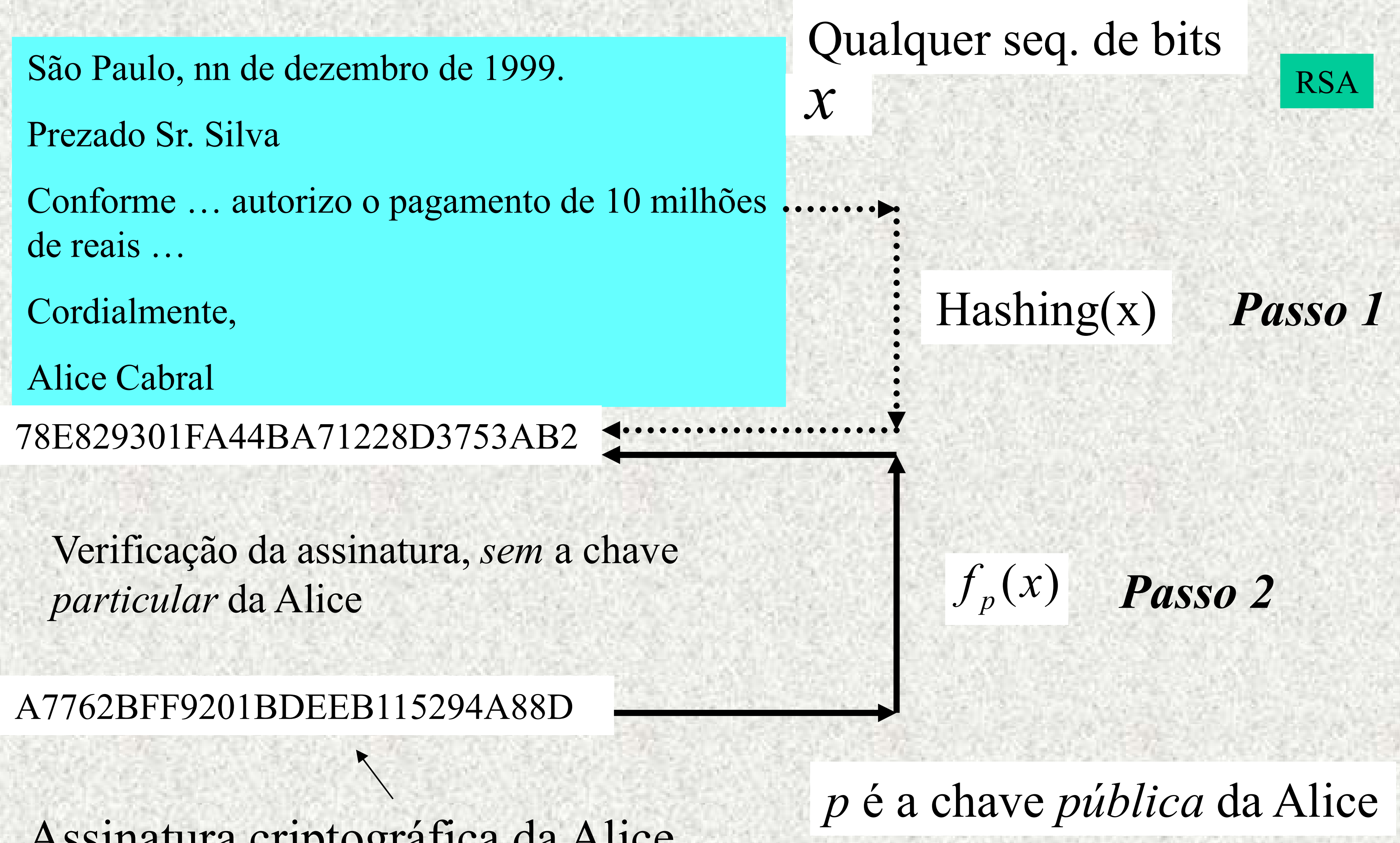
$f_s(x)$ ***Passo 2***

A7762BFF9201BDEEB115294A88D

s é a chave *particular* da Alice

Assinatura criptográfica da Alice

(128 bits)



RSA

Qualquer seq. de bits

x

São Paulo, nn de dezembro de 1999.

Prezado Sr. Silva

Conforme … autorizo o pagamento de 10 milhões de reais …

Cordialmente,

Alice Cabral

Hashing(x) ***Passo 1***

78E829301FA44BA71228D3753AB2

Verificação da assinatura, *sem* a chave *particular* da Alice

$f_p(x)$ ***Passo 2***

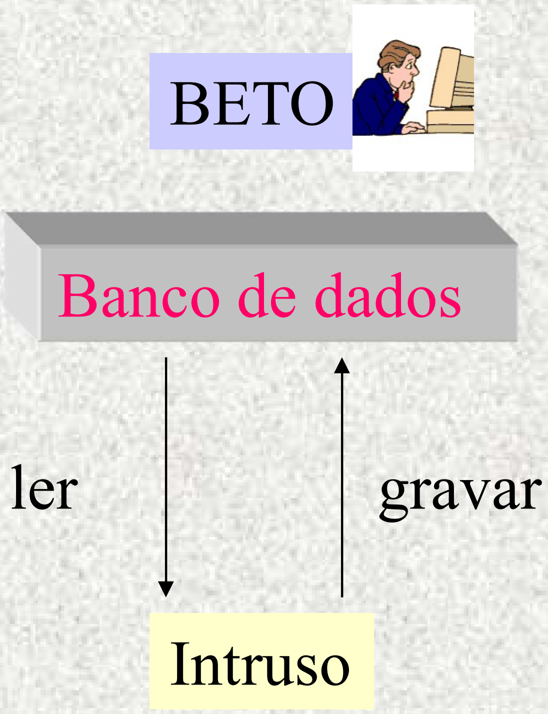
A7762BFF9201BDEEB115294A88D

p é a chave *pública* da Alice

Assinatura criptográfica da Alice

(128 bits)

RSA



BETO

Banco de dados

ler

gravar

Intruso

(por ex, loja virtual)

Objetivo 1: garantir sigilo. Solução: criptografar

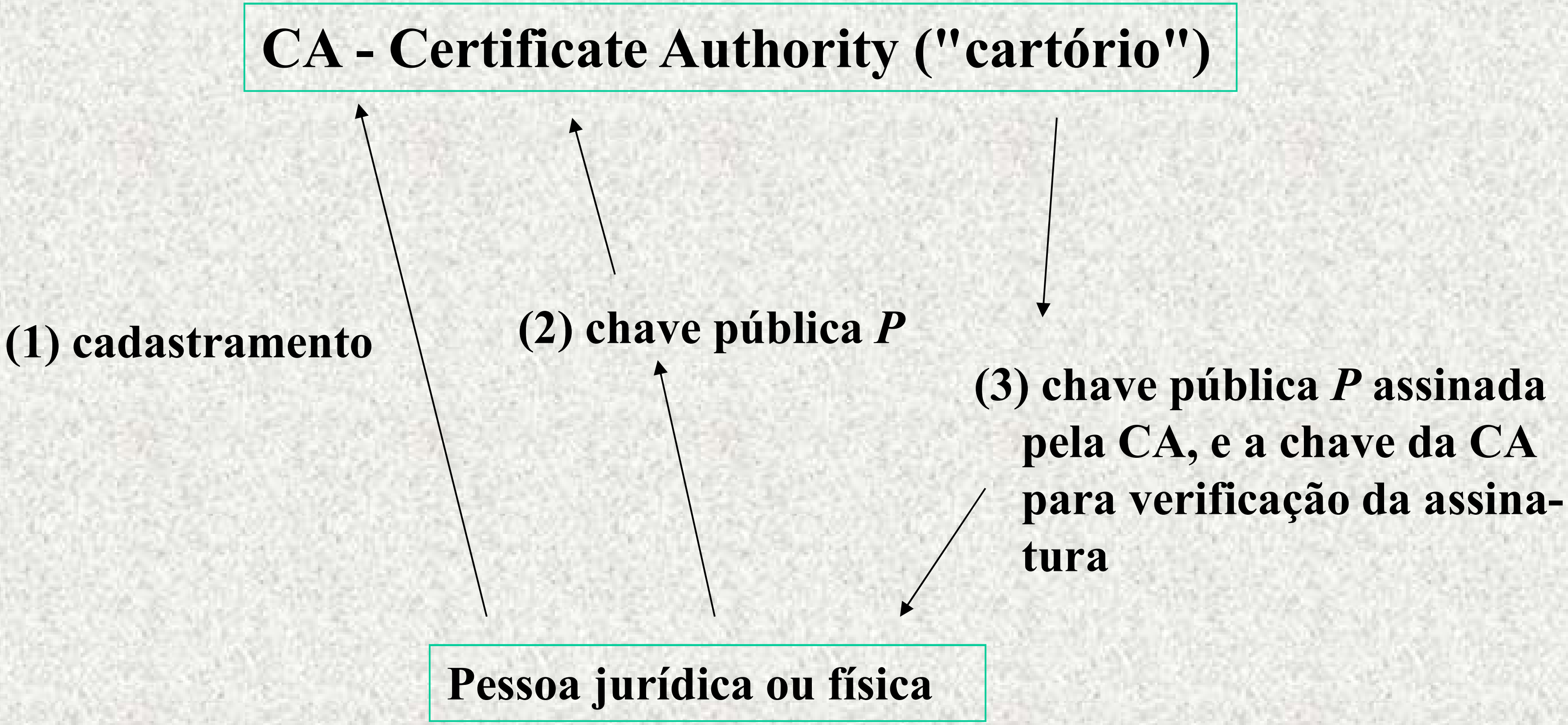
Objetivo 2: garantir integridade de info. Solução: assinatura criptográfica

Como saber se aquela chave pública é de fato do legítimo dono?

A chave deve ser assinada por uma autoridade idônea

PKI - Public Key Infrastructure

ICP – Infraestrutura de Chave Pública



CA - Certificate Authority ("cartório")

(1) cadastramento

(2) chave pública *P*

(3) chave pública *P* assinada pela CA, e a chave da CA para verificação da assinatura

Pessoa jurídica ou física

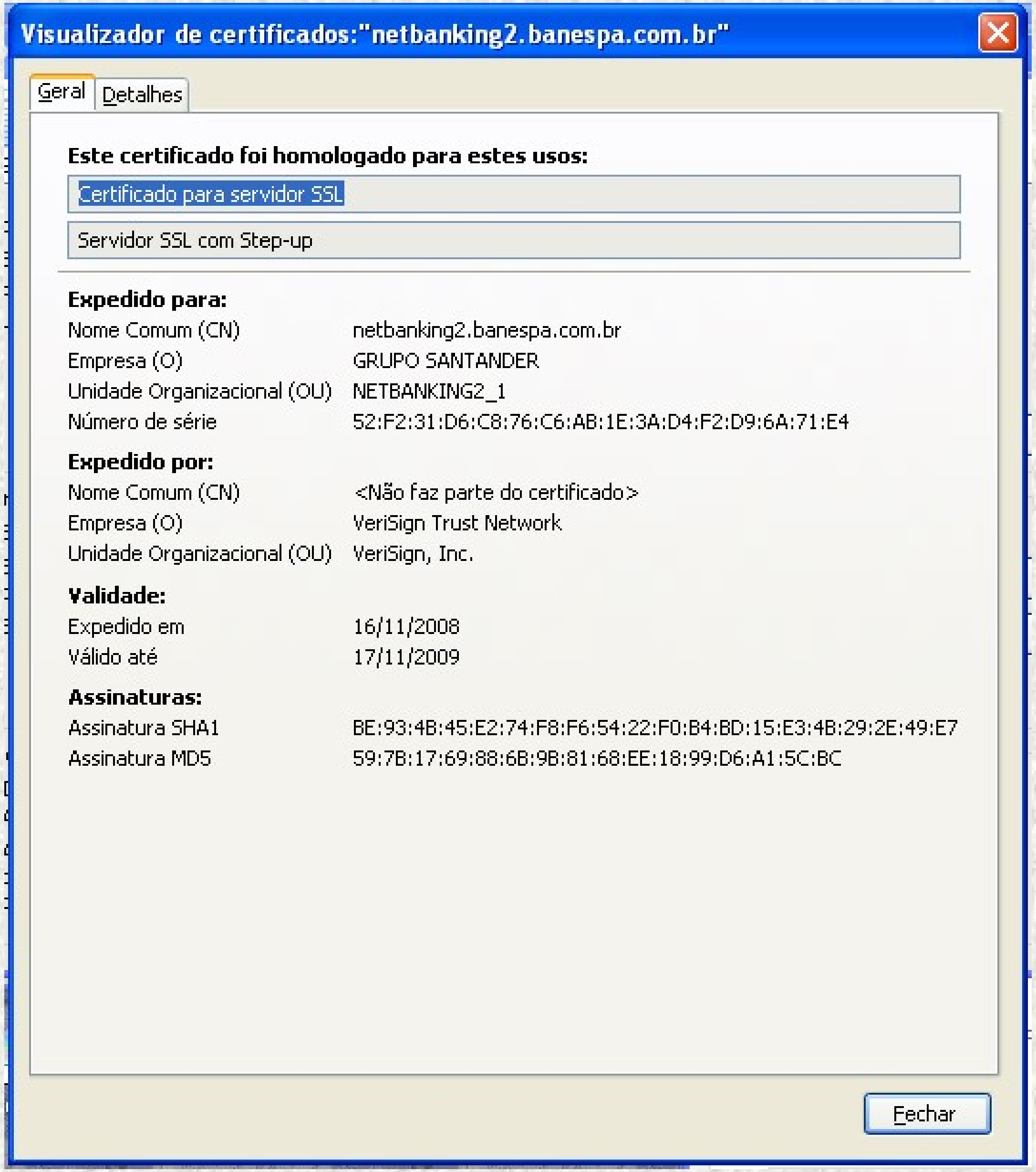
Exemplo fictício de certificado

Serial Number: 102251
Certificate for: Roberto Cabral
Company: Oops Consultoria Ltda.
Issued by: LeftSign Certificates
Email address: beto@oops.com.br
Activation: 29/01/2002
Expiration: 29/01/2005
Policy: Gold, contract signing
Public key: a44ff100c5 628ab4481
1baa171792 51bafec123
c441b182ab cc29123451
b237628767 26bba177af

---

LeftSign's digital signature:
3a72b18aab c2c4f1ff1
9aa6366876 172563ba66
a6a66273 9471448ba 2
28dc6ca1 f1228ab233

Certificado



Este certificado foi homologado para estes usos:

Certificado para servidor SSL

Servidor SSL com Step-up

Expedido para:

Nome Comum (CN)	netbanking2.banespa.com.br
Empresa (O)	GRUPO SANTANDER
Unidade Organizacional (OU)	NETBANKING2_1
Número de série	52:F2:31:D6:C8:76:C6:AB:1E:3A:D4:F2:D9:6A:71:E4

Expedido por:

Nome Comum (CN)	<Não faz parte do certificado>
Empresa (O)	VeriSign Trust Network
Unidade Organizacional (OU)	VeriSign, Inc.

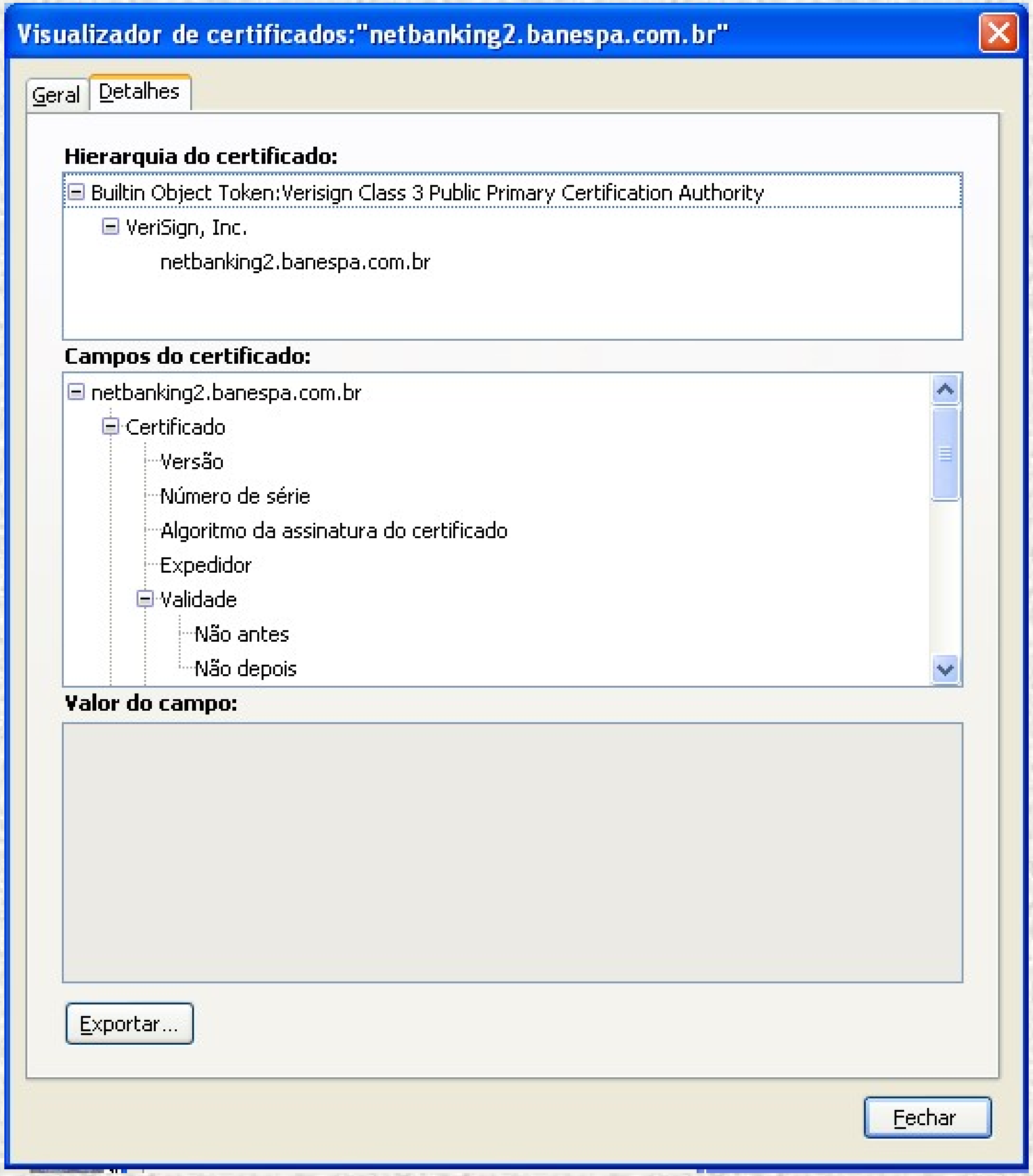
Validade:

Expedido em	16/11/2008
Válido até	17/11/2009

Assinaturas:

Assinatura SHA1	BE:93:4B:45:E2:74:F8:F6:54:22:F0:B4:BD:15:E3:4B:29:2E:49:E7
Assinatura MD5	59:7B:17:69:88:6B:9B:81:68:EE:18:99:D6:A1:5C:BC

Certificado



Visualizador de certificados:"netbanking2.banespa.com.br"

Hierarquia do certificado:

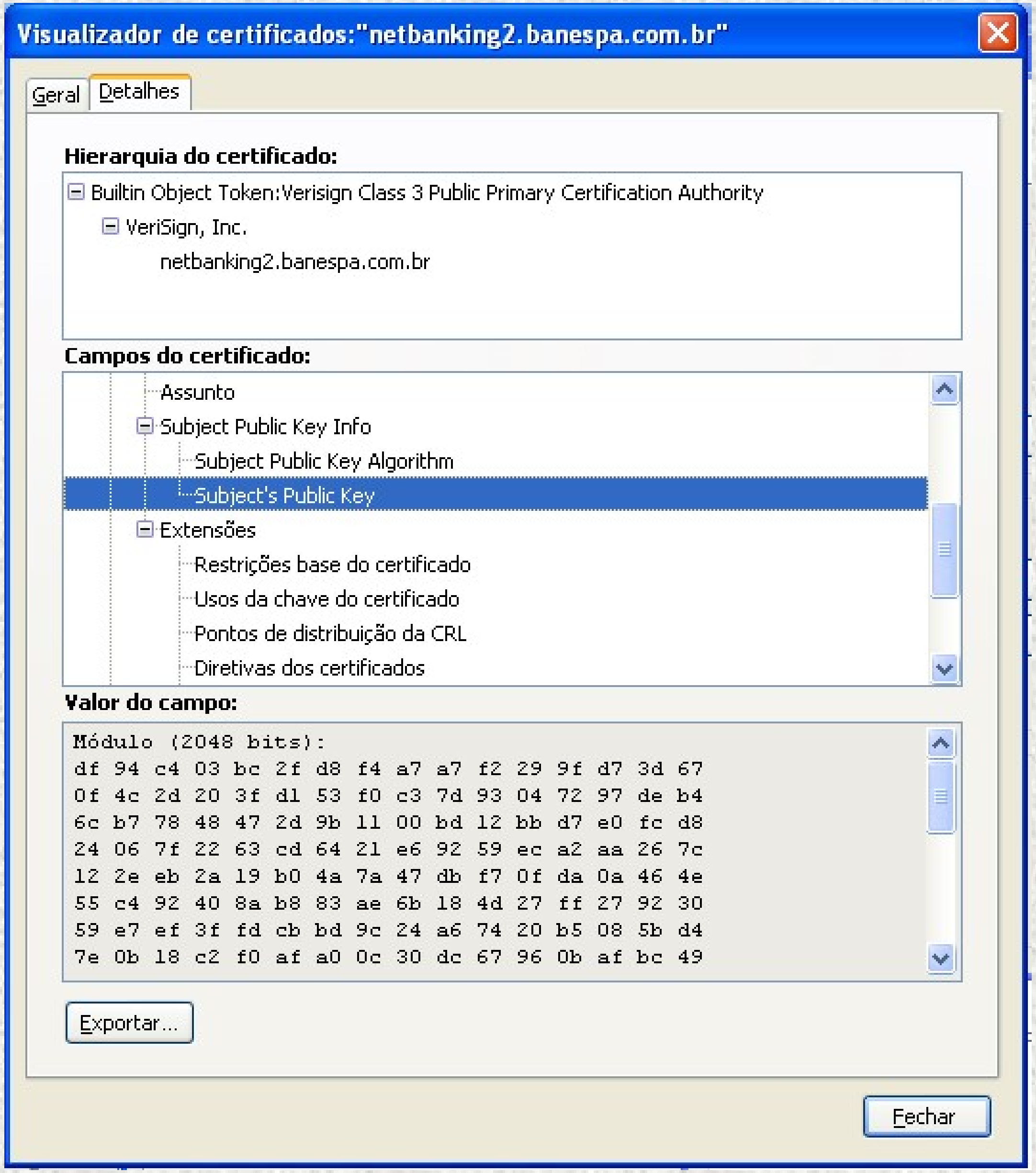
- Builtin Object Token:Verisign Class 3 Public Primary Certification Authority
  - VeriSign, Inc.
    - netbanking2.banespa.com.br

Campos do certificado:

- netbanking2.banespa.com.br
  - Certificado
    - Versão
    - Número de série
    - Algoritmo da assinatura do certificado
    - Expedidor
    - Validade
      - Não antes
      - Não depois

Valor do campo:

Certificado



Visualizador de certificados:"netbanking2.banespa.com.br"

Hierarquia do certificado:

- Builtin Object Token:Verisign Class 3 Public Primary Certification Authority
  - VeriSign, Inc.
    - netbanking2.banespa.com.br

Campos do certificado:

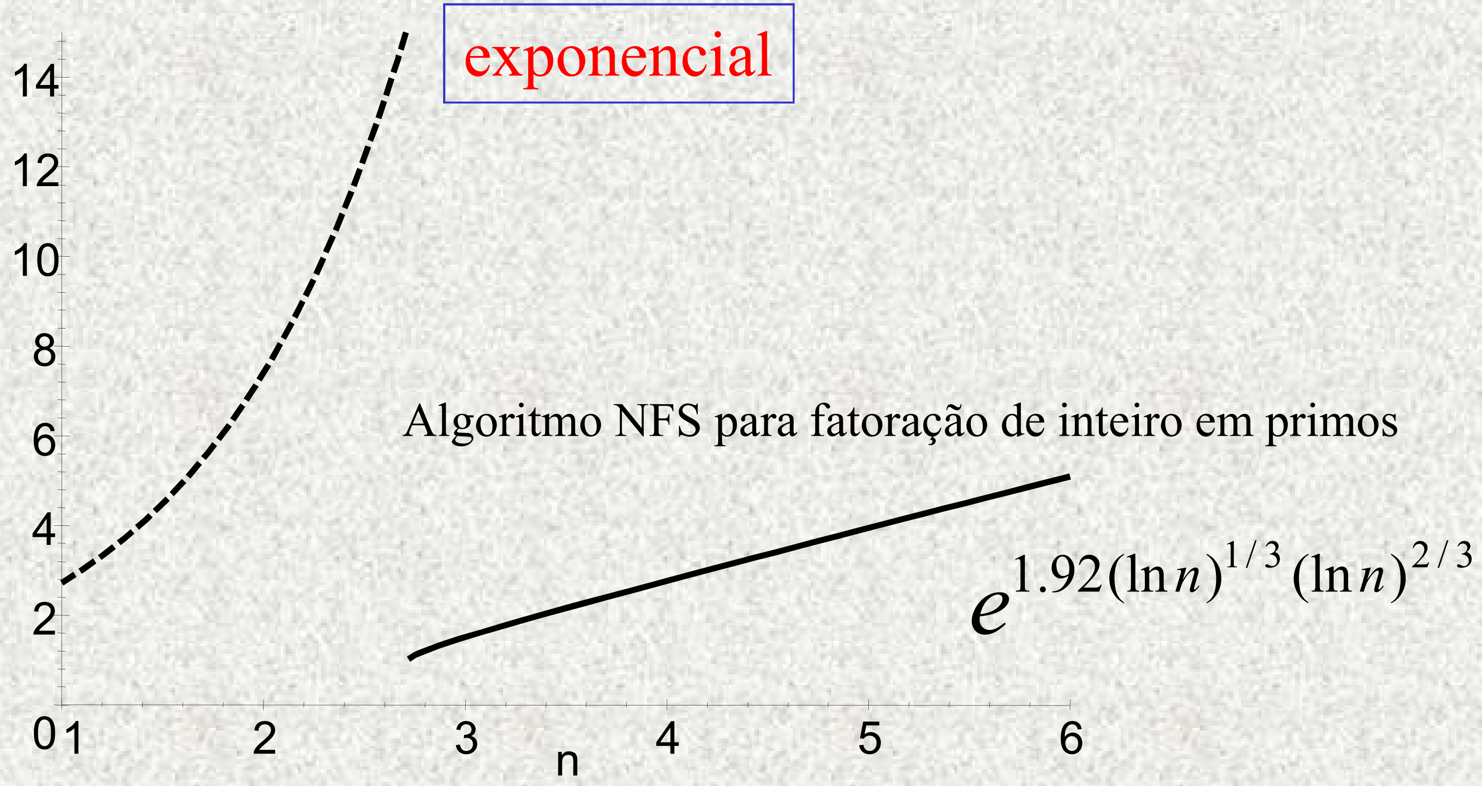
- Assunto
- Subject Public Key Info
  - Subject Public Key Algorithm
  - Subject's Public Key
- Extensões
  - Restrições base do certificado
  - Usos da chave do certificado
  - Pontos de distribuição da CRL
  - Diretivas dos certificados

Valor do campo:

```
Módulo (2048 bits):
df 94 c4 03 bc 2f d8 f4 a7 a7 f2 29 9f d7 3d 67
0f 4c 2d 20 3f d1 53 f0 c3 7d 93 04 72 97 de b4
6c b7 78 48 47 2d 9b 11 00 bd 12 bb d7 e0 fc d8
24 06 7f 22 63 cd 64 21 e6 92 59 ec a2 aa 26 7c
12 2e eb 2a 19 b0 4a 7a 47 db f7 0f da 0a 46 4e
55 c4 92 40 8a b8 83 ae 6b 18 4d 27 ff 27 92 30
59 e7 ef 3f fd cb bd 9c 24 a6 74 20 b5 08 5b d4
7e 0b 18 c2 f0 af a0 0c 30 dc 67 96 0b af bc 49
```

Quebra do Algoritmo RSA

Dificuldade de fatoração de n=q.r



Chave RSA 428 bits -- 5 mil MIPS-anos

Atualmente: recomenda-se mínimo de 768 bits em *n*

AES versus RSA

1. AES não permite assinatura criptográfica
2. RSA é cerca de 70 vezes mais lento

Em geral:

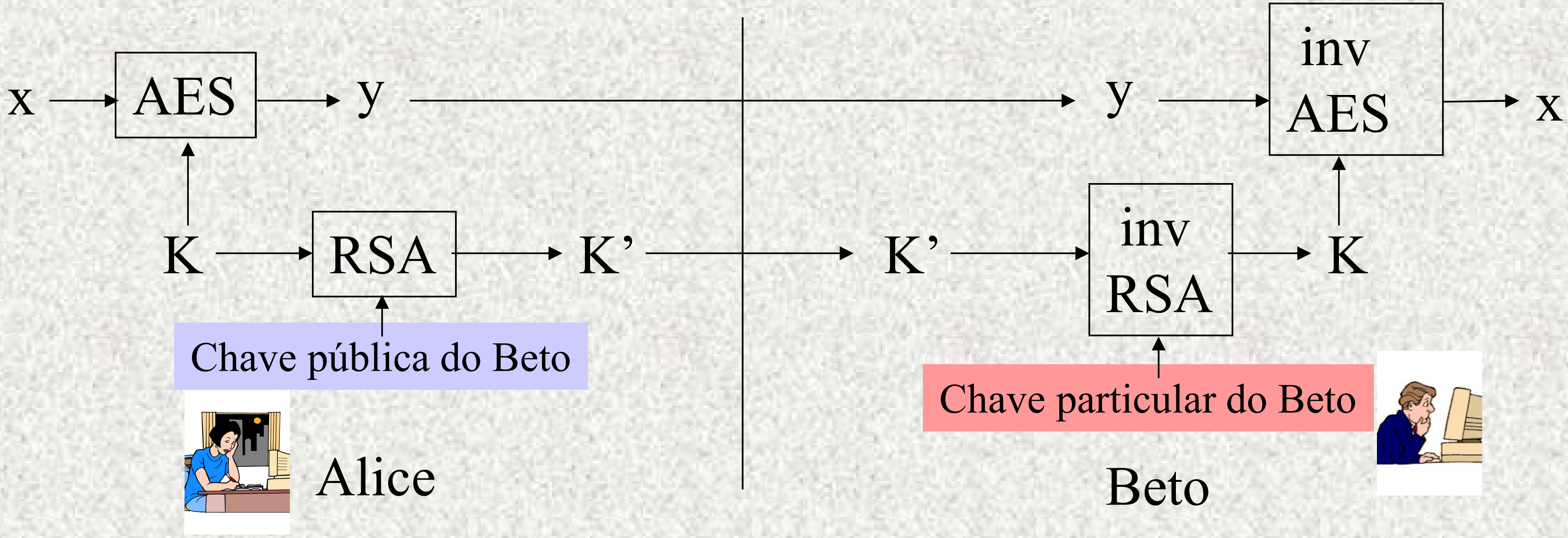
1. Cripto de chave secreta não permite assinatura criptográfica
2. Cripto de chave pública é dezenas de vezes mais lento

Recomenda-se sistema híbrido como PGP (a seguir)

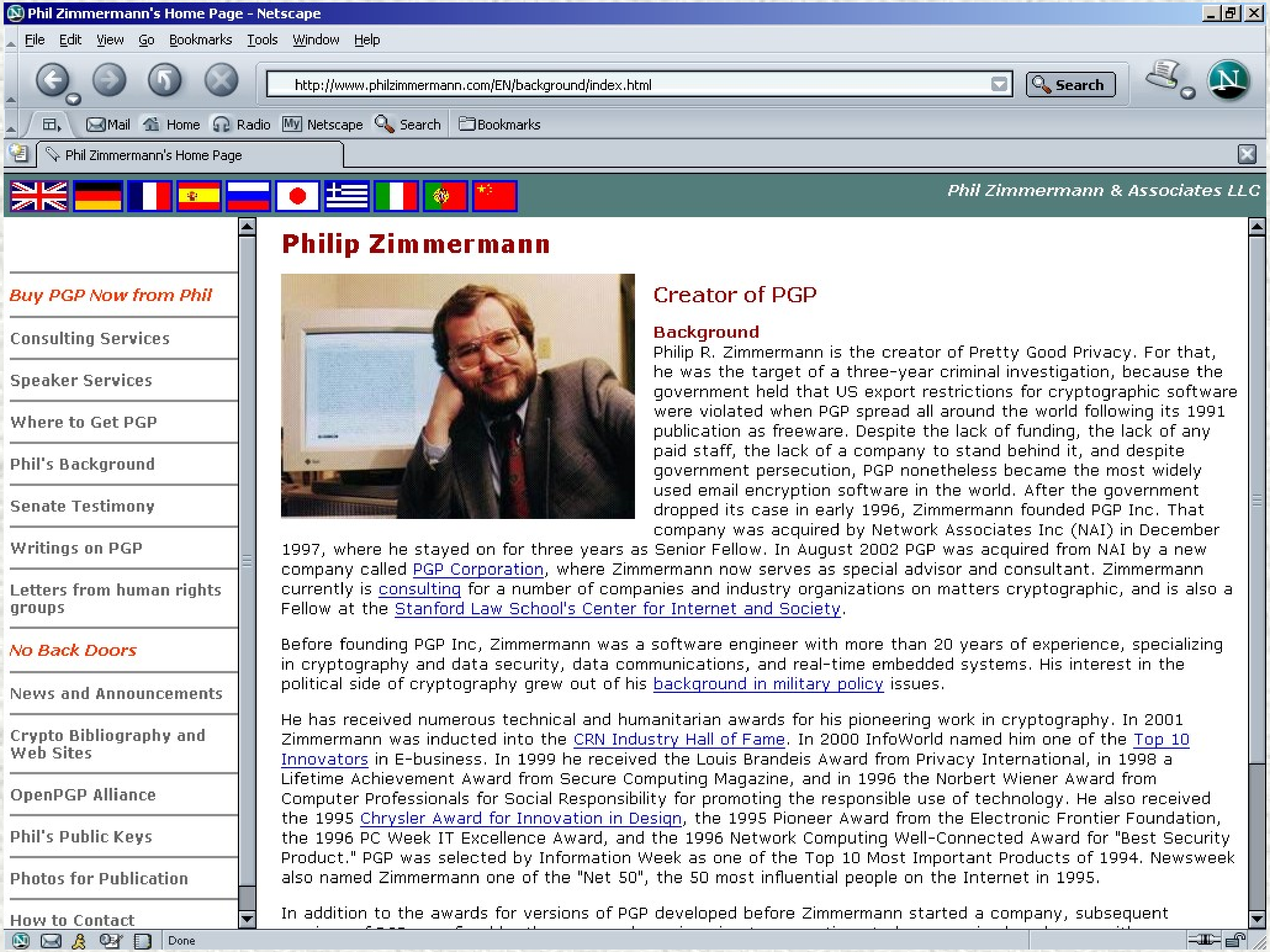
GPG → Open Source do Gnu equivalente a PGP

PGP – Pretty Good Privacy (Phil Zimmermann)

Sistema híbrido



1. Chave K é gerada p/ Alice
2. x é criptografado por IDEA, com K, e y é enviado
3. K é criptografado por RSA com chave pública do Beto (retirado do certificado do Beto) e K’ é enviado também
4. Beto decriptografa K’ com sua chave particular
5. Com K, Beto decriptografa y’ por IDEA


Phil Zimmermann's Home Page - Netscape
File Edit View Go Bookmarks Tools Window Help
http://www.philzimmermann.com/EN/background/index.html
Search
Mail Home Radio My Netscape Search Bookmarks
Phil Zimmermann's Home Page
Phil Zimmermann & Associates LLC
Buy PGP Now from Phil
Consulting Services
Speaker Services
Where to Get PGP
Phil's Background
Senate Testimony
Writings on PGP
Letters from human rights groups
No Back Doors
News and Announcements
Crypto Bibliography and Web Sites
OpenPGP Alliance
Phil's Public Keys
Photos for Publication
How to Contact
Done

Philip Zimmermann

Creator of PGP

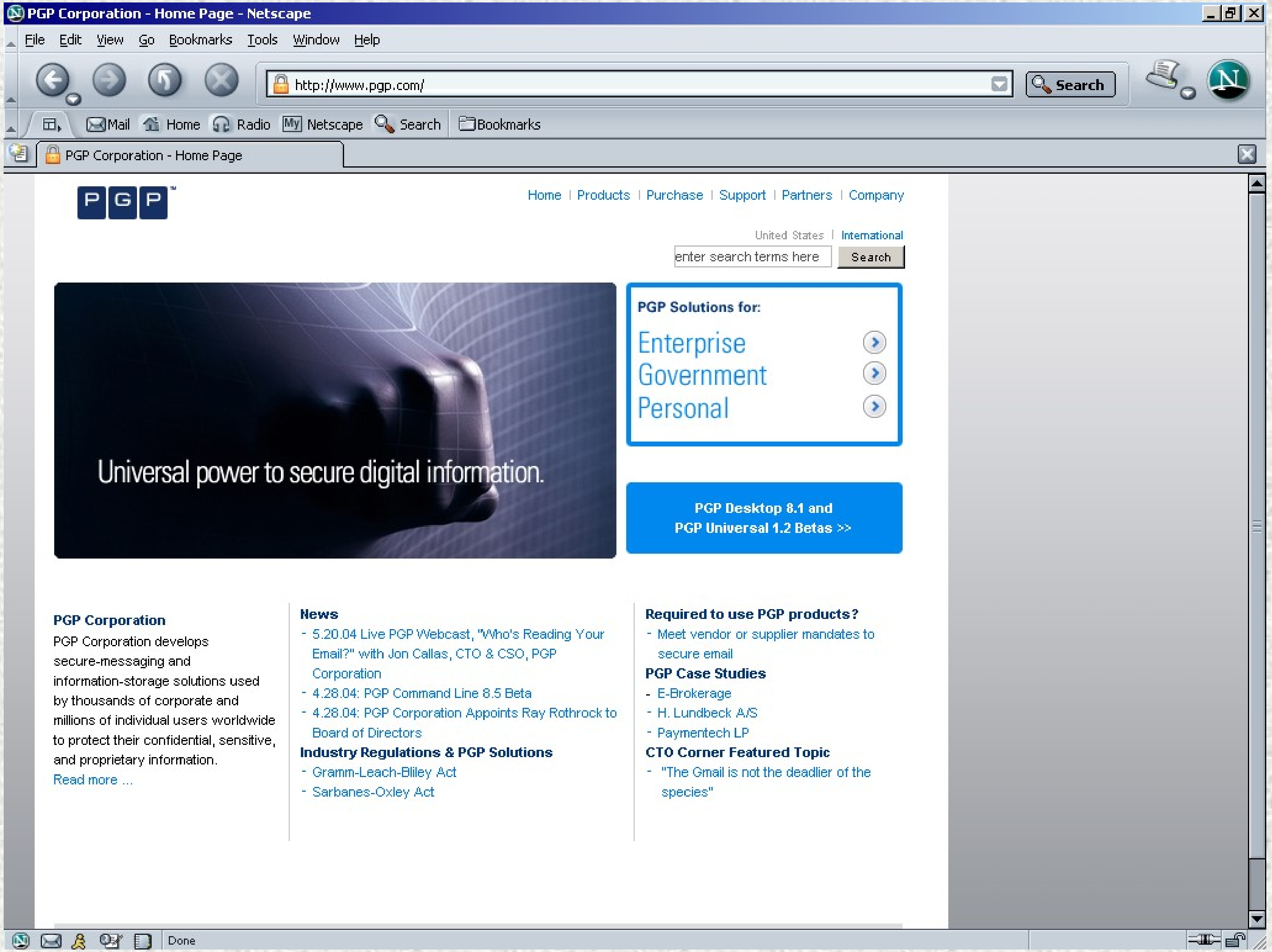
Background

Philip R. Zimmermann is the creator of Pretty Good Privacy. For that, he was the target of a three-year criminal investigation, because the government held that US export restrictions for cryptographic software were violated when PGP spread all around the world following its 1991 publication as freeware. Despite the lack of funding, the lack of any paid staff, the lack of a company to stand behind it, and despite government persecution, PGP nonetheless became the most widely used email encryption software in the world. After the government dropped its case in early 1996, Zimmermann founded PGP Inc. That company was acquired by Network Associates Inc (NAI) in December 1997, where he stayed on for three years as Senior Fellow. In August 2002 PGP was acquired from NAI by a new company called PGP Corporation, where Zimmermann now serves as special advisor and consultant. Zimmermann currently is consulting for a number of companies and industry organizations on matters cryptographic, and is also a Fellow at the Stanford Law School's Center for Internet and Society.

Before founding PGP Inc, Zimmermann was a software engineer with more than 20 years of experience, specializing in cryptography and data security, data communications, and real-time embedded systems. His interest in the political side of cryptography grew out of his background in military policy issues.

He has received numerous technical and humanitarian awards for his pioneering work in cryptography. In 2001 Zimmermann was inducted into the CRN Industry Hall of Fame. In 2000 InfoWorld named him one of the Top 10 Innovators in E-business. In 1999 he received the Louis Brandeis Award from Privacy International, in 1998 a Lifetime Achievement Award from Secure Computing Magazine, and in 1996 the Norbert Wiener Award from Computer Professionals for Social Responsibility for promoting the responsible use of technology. He also received the 1995 Chrysler Award for Innovation in Design, the 1995 Pioneer Award from the Electronic Frontier Foundation, the 1996 PC Week IT Excellence Award, and the 1996 Network Computing Well-Connected Award for "Best Security Product." PGP was selected by Information Week as one of the Top 10 Most Important Products of 1994. Newsweek also named Zimmermann one of the "Net 50", the 50 most influential people on the Internet in 1995.

In addition to the awards for versions of PGP developed before Zimmermann started a company, subsequent



PGP Corporation - Home Page - Netscape
File Edit View Go Bookmarks Tools Window Help
http://www.pgp.com/
Search
Mail Home Radio Netscape Search Bookmarks
PGP Corporation - Home Page
Home | Products | Purchase | Support | Partners | Company
United States | International
enter search terms here
Search
Done

Universal power to secure digital information.

PGP Solutions for:

- Enterprise
- Government
- Personal

PGP Desktop 8.1 and PGP Universal 1.2 Betas >>

PGP Corporation

PGP Corporation develops secure-messaging and information-storage solutions used by thousands of corporate and millions of individual users worldwide to protect their confidential, sensitive, and proprietary information.

Read more ...

News

- 5.20.04 Live PGP Webcast, "Who's Reading Your Email?" with Jon Callas, CTO & CSO, PGP Corporation
- 4.28.04: PGP Command Line 8.5 Beta
- 4.28.04: PGP Corporation Appoints Ray Rothrock to Board of Directors

Industry Regulations & PGP Solutions

- Gramm-Leach-Bliley Act
- Sarbanes-Oxley Act

Required to use PGP products?

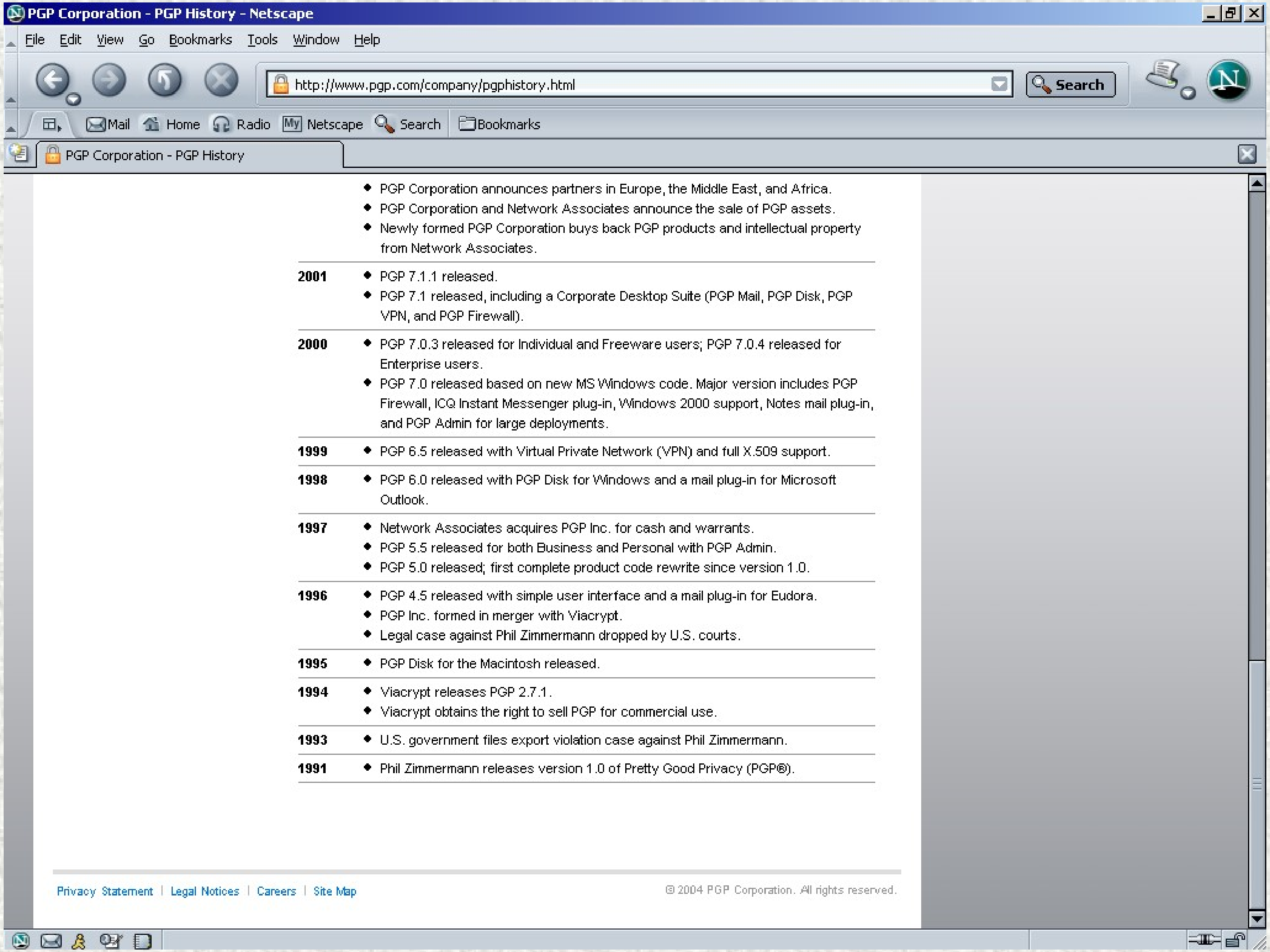
- Meet vendor or supplier mandates to secure email

PGP Case Studies

- E-Brokerage
- H. Lundbeck A/S
- Paymentech LP

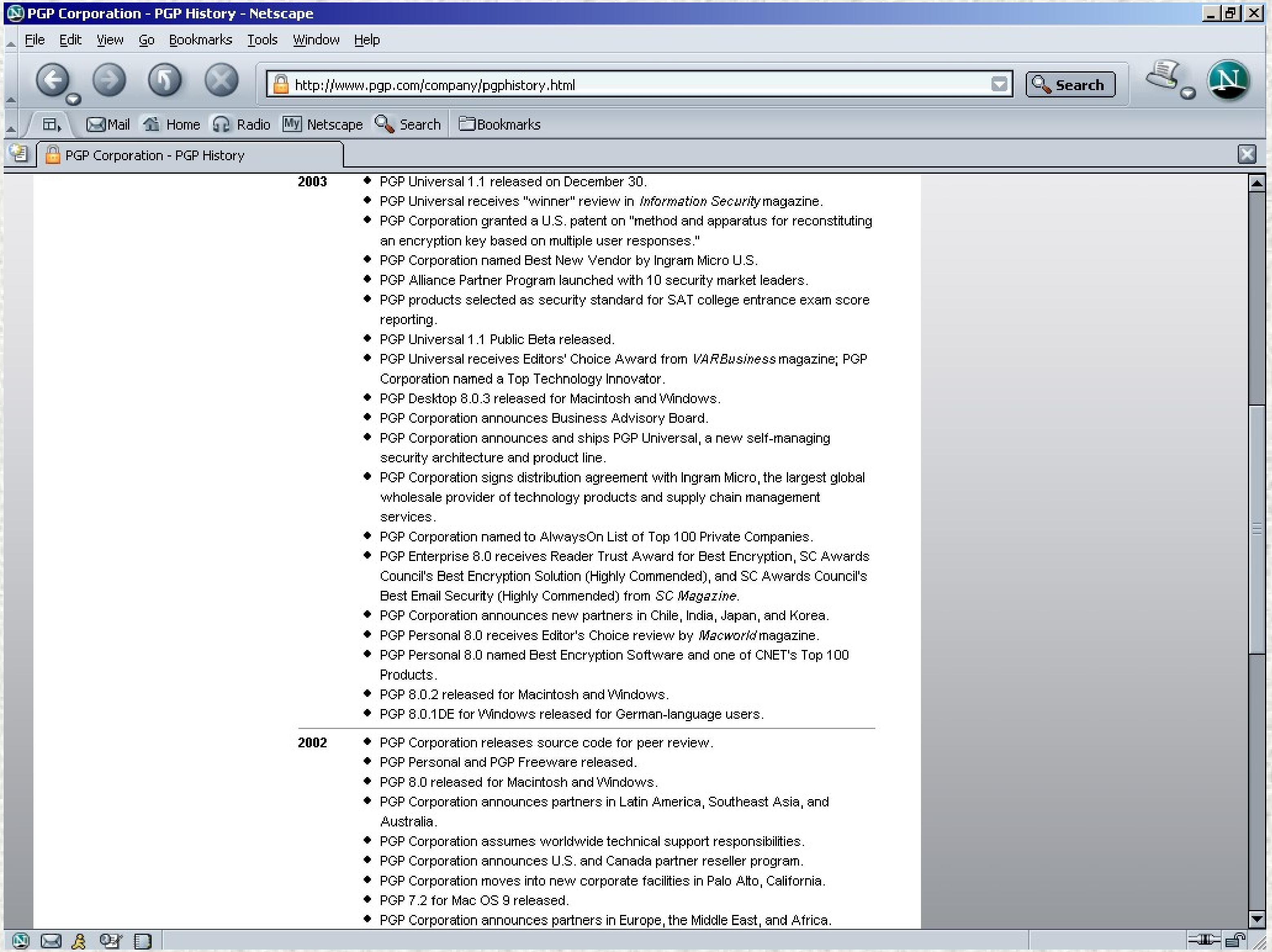
CTO Corner Featured Topic

- "The Gmail is not the deadlier of the species"


PGP Corporation - PGP History - Netscape
File Edit View Go Bookmarks Tools Window Help
http://www.pgp.com/company/pgphistory.html
Search
Mail Home Radio Netscape Search Bookmarks
PGP Corporation - PGP History

	◆ PGP Corporation announces partners in Europe, the Middle East, and Africa. ◆ PGP Corporation and Network Associates announce the sale of PGP assets. ◆ Newly formed PGP Corporation buys back PGP products and intellectual property from Network Associates.
2001	◆ PGP 7.1.1 released. ◆ PGP 7.1 released, including a Corporate Desktop Suite (PGP Mail, PGP Disk, PGP VPN, and PGP Firewall).
2000	◆ PGP 7.0.3 released for Individual and Freeware users; PGP 7.0.4 released for Enterprise users. ◆ PGP 7.0 released based on new MS Windows code. Major version includes PGP Firewall, ICQ Instant Messenger plug-in, Windows 2000 support, Notes mail plug-in, and PGP Admin for large deployments.
1999	◆ PGP 6.5 released with Virtual Private Network (VPN) and full X.509 support.
1998	◆ PGP 6.0 released with PGP Disk for Windows and a mail plug-in for Microsoft Outlook.
1997	◆ Network Associates acquires PGP Inc. for cash and warrants. ◆ PGP 5.5 released for both Business and Personal with PGP Admin. ◆ PGP 5.0 released; first complete product code rewrite since version 1.0.
1996	◆ PGP 4.5 released with simple user interface and a mail plug-in for Eudora. ◆ PGP Inc. formed in merger with Viacrypt. ◆ Legal case against Phil Zimmermann dropped by U.S. courts.
1995	◆ PGP Disk for the Macintosh released.
1994	◆ Viacrypt releases PGP 2.7.1. ◆ Viacrypt obtains the right to sell PGP for commercial use.
1993	◆ U.S. government files export violation case against Phil Zimmermann.
1991	◆ Phil Zimmermann releases version 1.0 of Pretty Good Privacy (PGP®).

Privacy Statement | Legal Notices | Careers | Site Map

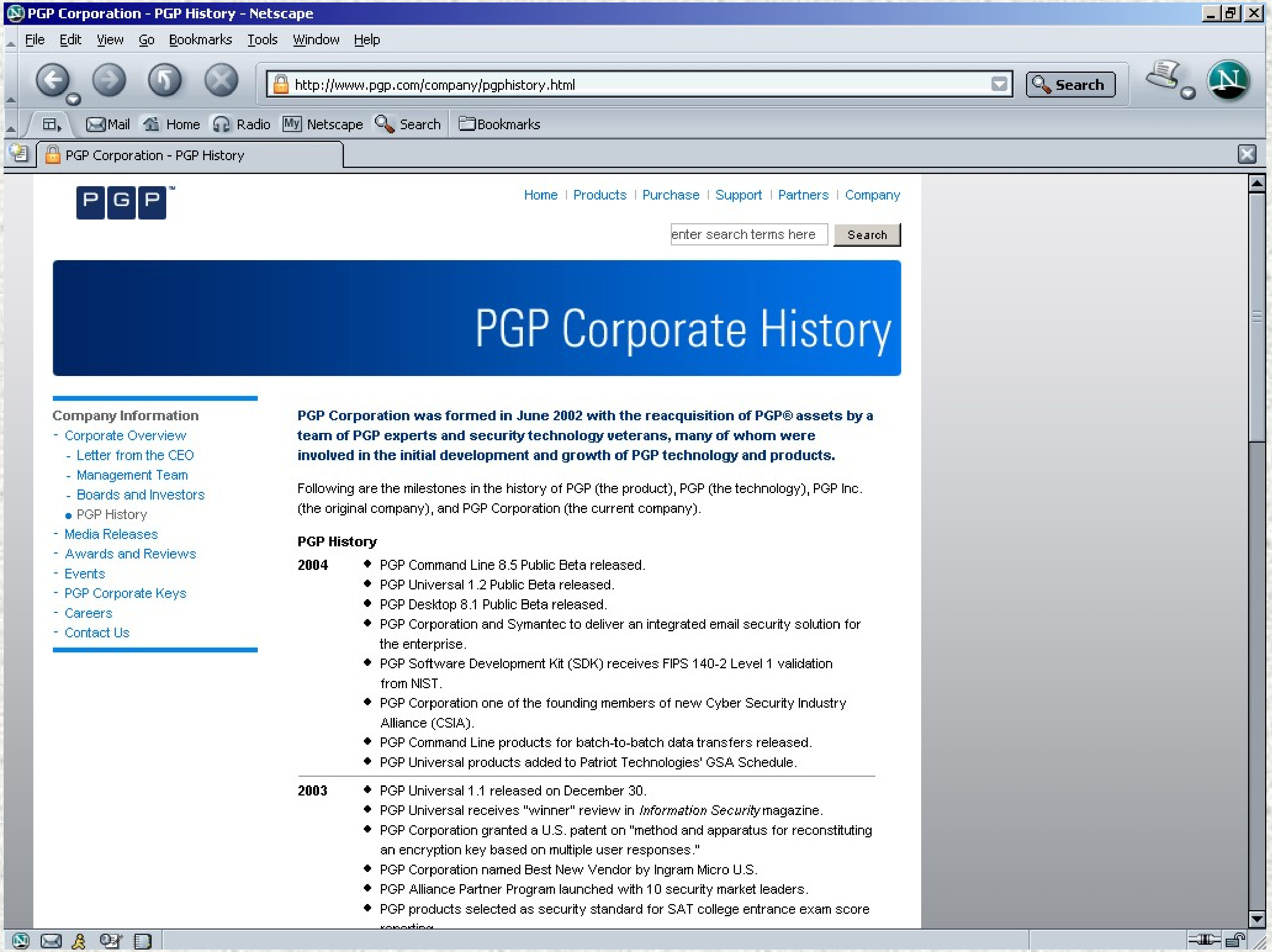

PGP Corporation - PGP History - Netscape
File Edit View Go Bookmarks Tools Window Help
http://www.pgp.com/company/pgphistory.html
Search
Mail Home Radio Netscape Search Bookmarks
PGP Corporation - PGP History

2003

- PGP Universal 1.1 released on December 30.
- PGP Universal receives "winner" review in *Information Security* magazine.
- PGP Corporation granted a U.S. patent on "method and apparatus for reconstituting an encryption key based on multiple user responses."
- PGP Corporation named Best New Vendor by Ingram Micro U.S.
- PGP Alliance Partner Program launched with 10 security market leaders.
- PGP products selected as security standard for SAT college entrance exam score reporting.
- PGP Universal 1.1 Public Beta released.
- PGP Universal receives Editors' Choice Award from *VARBusiness* magazine; PGP Corporation named a Top Technology Innovator.
- PGP Desktop 8.0.3 released for Macintosh and Windows.
- PGP Corporation announces Business Advisory Board.
- PGP Corporation announces and ships PGP Universal, a new self-managing security architecture and product line.
- PGP Corporation signs distribution agreement with Ingram Micro, the largest global wholesale provider of technology products and supply chain management services.
- PGP Corporation named to AlwaysOn List of Top 100 Private Companies.
- PGP Enterprise 8.0 receives Reader Trust Award for Best Encryption, SC Awards Council's Best Encryption Solution (Highly Commended), and SC Awards Council's Best Email Security (Highly Commended) from *SC Magazine*.
- PGP Corporation announces new partners in Chile, India, Japan, and Korea.
- PGP Personal 8.0 receives Editor's Choice review by *Macworld* magazine.
- PGP Personal 8.0 named Best Encryption Software and one of CNET's Top 100 Products.
- PGP 8.0.2 released for Macintosh and Windows.
- PGP 8.0.1DE for Windows released for German-language users.

2002

- PGP Corporation releases source code for peer review.
- PGP Personal and PGP Freeware released.
- PGP 8.0 released for Macintosh and Windows.
- PGP Corporation announces partners in Latin America, Southeast Asia, and Australia.
- PGP Corporation assumes worldwide technical support responsibilities.
- PGP Corporation announces U.S. and Canada partner reseller program.
- PGP Corporation moves into new corporate facilities in Palo Alto, California.
- PGP 7.2 for Mac OS 9 released.
- PGP Corporation announces partners in Europe, the Middle East, and Africa.


PGP Corporation - PGP History - Netscape
File Edit View Go Bookmarks Tools Window Help
http://www.pgp.com/company/pgphistory.html
Search
Mail Home Radio Netscape Search Bookmarks
PGP Corporation - PGP History
PGP
Home | Products | Purchase | Support | Partners | Company
enter search terms here
Search

PGP Corporate History

Company Information
- Corporate Overview
  - Letter from the CEO
  - Management Team
  - Boards and Investors
  - PGP History
- Media Releases
- Awards and Reviews
- Events
- PGP Corporate Keys
- Careers
- Contact Us

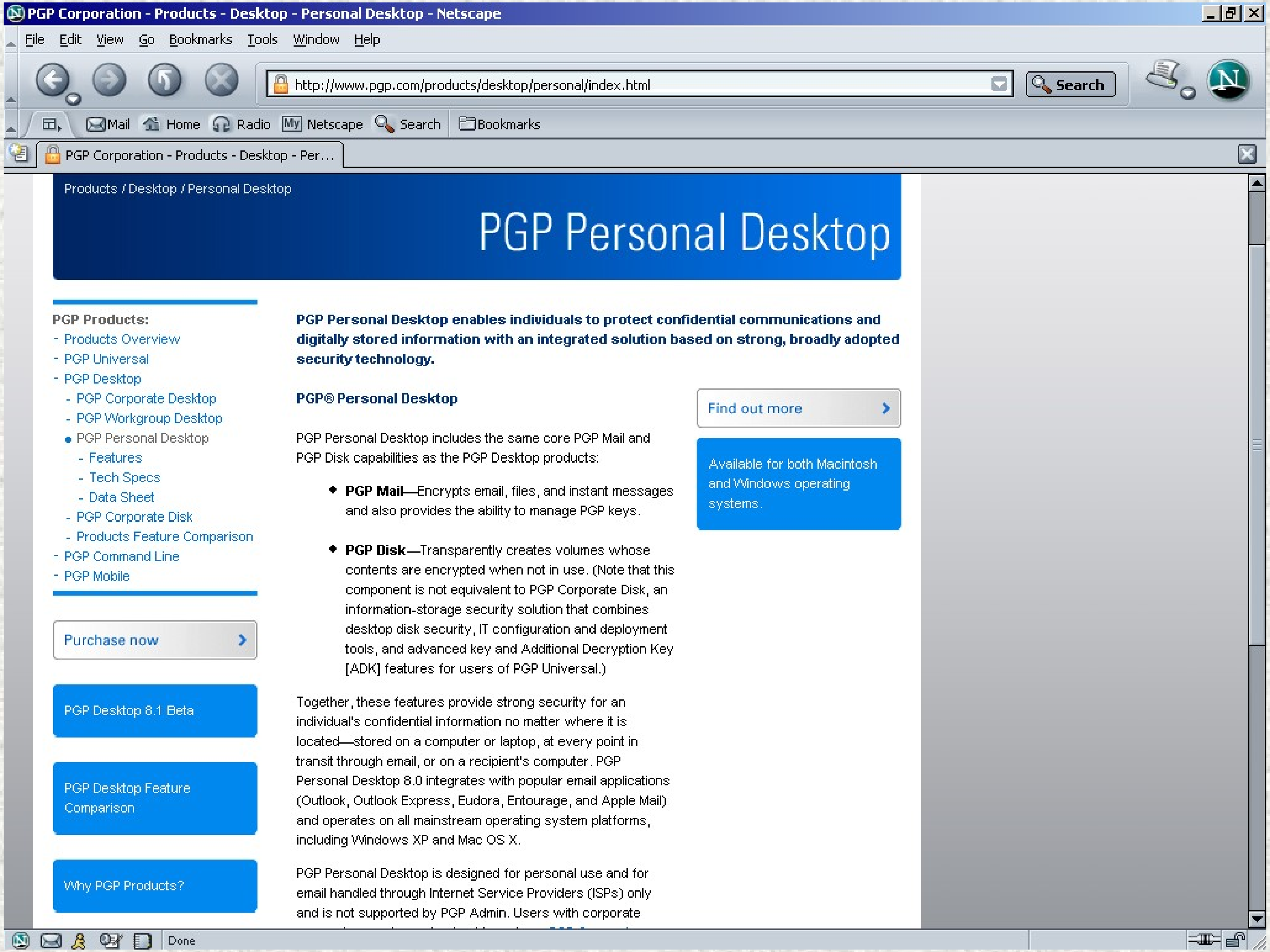
PGP Corporation was formed in June 2002 with the reacquisition of PGP® assets by a team of PGP experts and security technology veterans, many of whom were involved in the initial development and growth of PGP technology and products.

Following are the milestones in the history of PGP (the product), PGP (the technology), PGP Inc. (the original company), and PGP Corporation (the current company).

PGP History

2004
- PGP Command Line 8.5 Public Beta released.
- PGP Universal 1.2 Public Beta released.
- PGP Desktop 8.1 Public Beta released.
- PGP Corporation and Symantec to deliver an integrated email security solution for the enterprise.
- PGP Software Development Kit (SDK) receives FIPS 140-2 Level 1 validation from NIST.
- PGP Corporation one of the founding members of new Cyber Security Industry Alliance (CSIA).
- PGP Command Line products for batch-to-batch data transfers released.
- PGP Universal products added to Patriot Technologies' GSA Schedule.

2003
- PGP Universal 1.1 released on December 30.
- PGP Universal receives "winner" review in *Information Security* magazine.
- PGP Corporation granted a U.S. patent on "method and apparatus for reconstituting an encryption key based on multiple user responses."
- PGP Corporation named Best New Vendor by Ingram Micro U.S.
- PGP Alliance Partner Program launched with 10 security market leaders.
- PGP products selected as security standard for SAT college entrance exam score reporting


PGP Corporation - Products - Desktop - Personal Desktop - Netscape
File Edit View Go Bookmarks Tools Window Help
http://www.pgp.com/products/desktop/personal/index.html
Search
Mail Home Radio Netscape Search Bookmarks
PGP Corporation - Products - Desktop - Per…
Done

Products / Desktop / Personal Desktop

PGP Personal Desktop

PGP Products:

- Products Overview
- PGP Universal
- PGP Desktop
  - PGP Corporate Desktop
  - PGP Workgroup Desktop
  - PGP Personal Desktop
    - Features
    - Tech Specs
    - Data Sheet
  - PGP Corporate Disk
  - Products Feature Comparison
- PGP Command Line
- PGP Mobile

Purchase now ›

PGP Desktop 8.1 Beta

PGP Desktop Feature Comparison

Why PGP Products?

PGP Personal Desktop enables individuals to protect confidential communications and digitally stored information with an integrated solution based on strong, broadly adopted security technology.

PGP® Personal Desktop

PGP Personal Desktop includes the same core PGP Mail and PGP Disk capabilities as the PGP Desktop products:

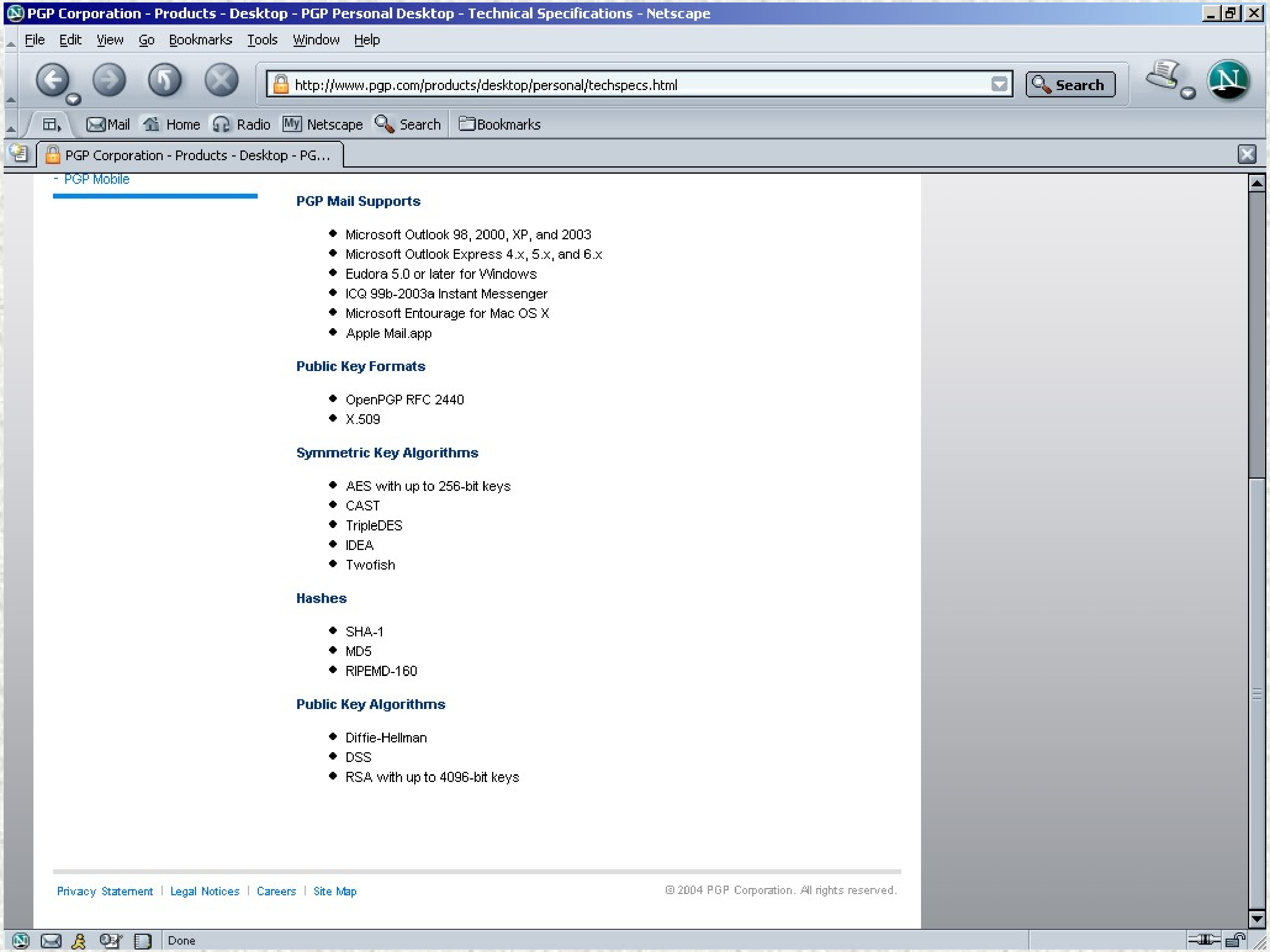
- **PGP Mail**—Encrypts email, files, and instant messages and also provides the ability to manage PGP keys.
- **PGP Disk**—Transparently creates volumes whose contents are encrypted when not in use. (Note that this component is not equivalent to PGP Corporate Disk, an information-storage security solution that combines desktop disk security, IT configuration and deployment tools, and advanced key and Additional Decryption Key [ADK] features for users of PGP Universal.)

Together, these features provide strong security for an individual's confidential information no matter where it is located—stored on a computer or laptop, at every point in transit through email, or on a recipient's computer. PGP Personal Desktop 8.0 integrates with popular email applications (Outlook, Outlook Express, Eudora, Entourage, and Apple Mail) and operates on all mainstream operating system platforms, including Windows XP and Mac OS X.

PGP Personal Desktop is designed for personal use and for email handled through Internet Service Providers (ISPs) only and is not supported by PGP Admin. Users with corporate

Find out more ›

Available for both Macintosh and Windows operating systems.


PGP Corporation - Products - Desktop - PGP Personal Desktop - Technical Specifications - Netscape
File Edit View Go Bookmarks Tools Window Help
http://www.pgp.com/products/desktop/personal/techspecs.html
Search
Mail Home Radio Netscape Search Bookmarks
PGP Corporation - Products - Desktop - PG...
- PGP Mobile
Done

PGP Mail Supports

- Microsoft Outlook 98, 2000, XP, and 2003
- Microsoft Outlook Express 4.x, 5.x, and 6.x
- Eudora 5.0 or later for Windows
- ICQ 99b-2003a Instant Messenger
- Microsoft Entourage for Mac OS X
- Apple Mail.app

Public Key Formats

- OpenPGP RFC 2440
- X.509

Symmetric Key Algorithms

- AES with up to 256-bit keys
- CAST
- TripleDES
- IDEA
- Twofish

Hashes

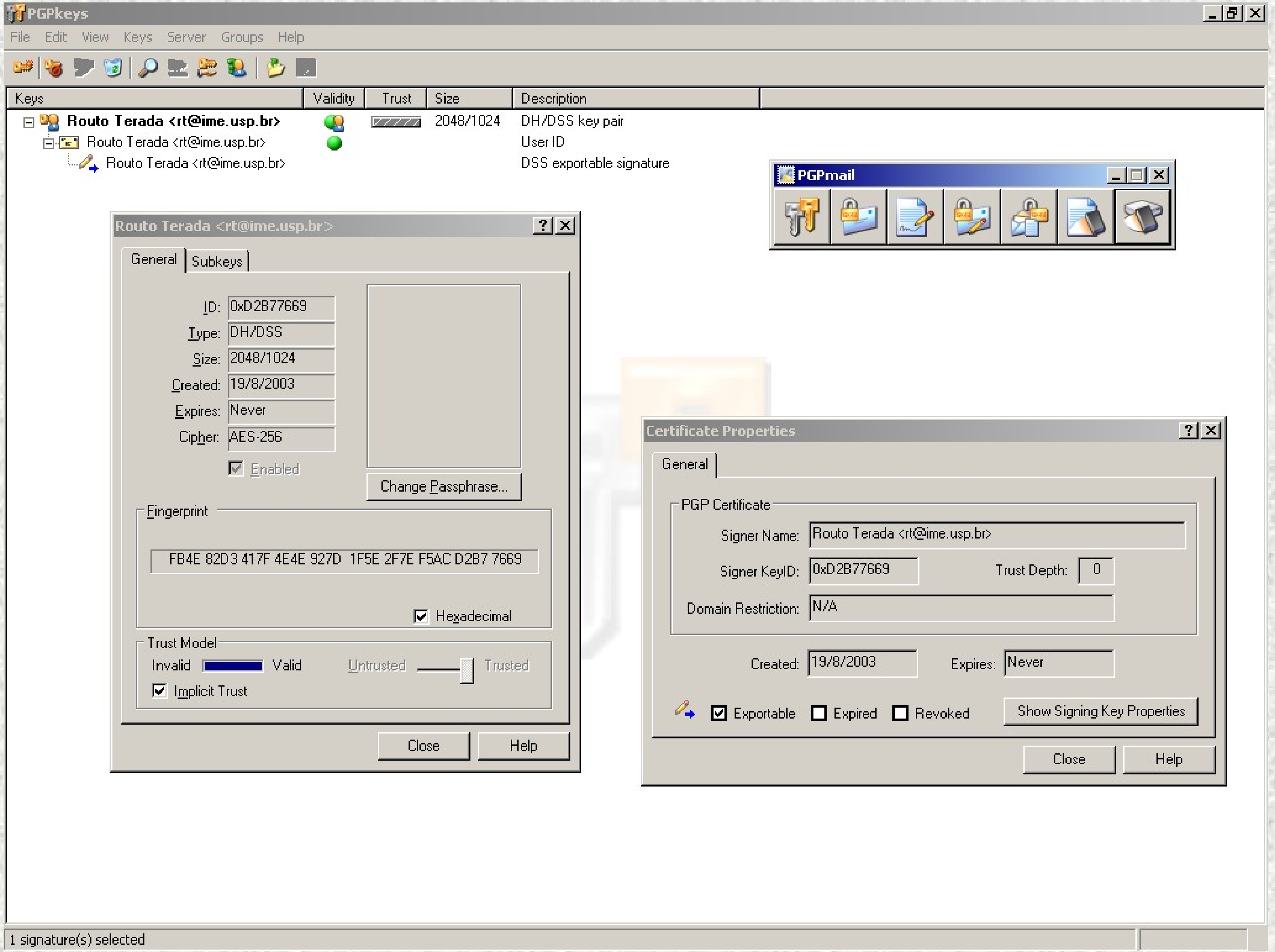
- SHA-1
- MD5
- RIPEMD-160

Public Key Algorithms

- Diffie-Hellman
- DSS
- RSA with up to 4096-bit keys

Privacy Statement | Legal Notices | Careers | Site Map

© 2004 PGP Corporation. All rights reserved.



Keys	Validity	Trust	Size	Description
Routo Terada <rt@ime.usp.br>	●	▨	2048/1024	DH/DSS key pair
Routo Terada <rt@ime.usp.br>	●			User ID
Routo Terada <rt@ime.usp.br>				DSS exportable signature

Routo Terada <rt@ime.usp.br>

General | Subkeys

ID: 0xD2B77669
Type: DH/DSS
Size: 2048/1024
Created: 19/8/2003
Expires: Never
Cipher: AES-256
☑ Enabled

Change Passphrase...

Fingerprint
FB4E 82D3 417F 4E4E 927D 1F5E 2F7E F5AC D2B7 7669
☑ Hexadecimal

Trust Model
Invalid Valid Untrusted Trusted
☑ Implicit Trust

Close Help

Certificate Properties

General

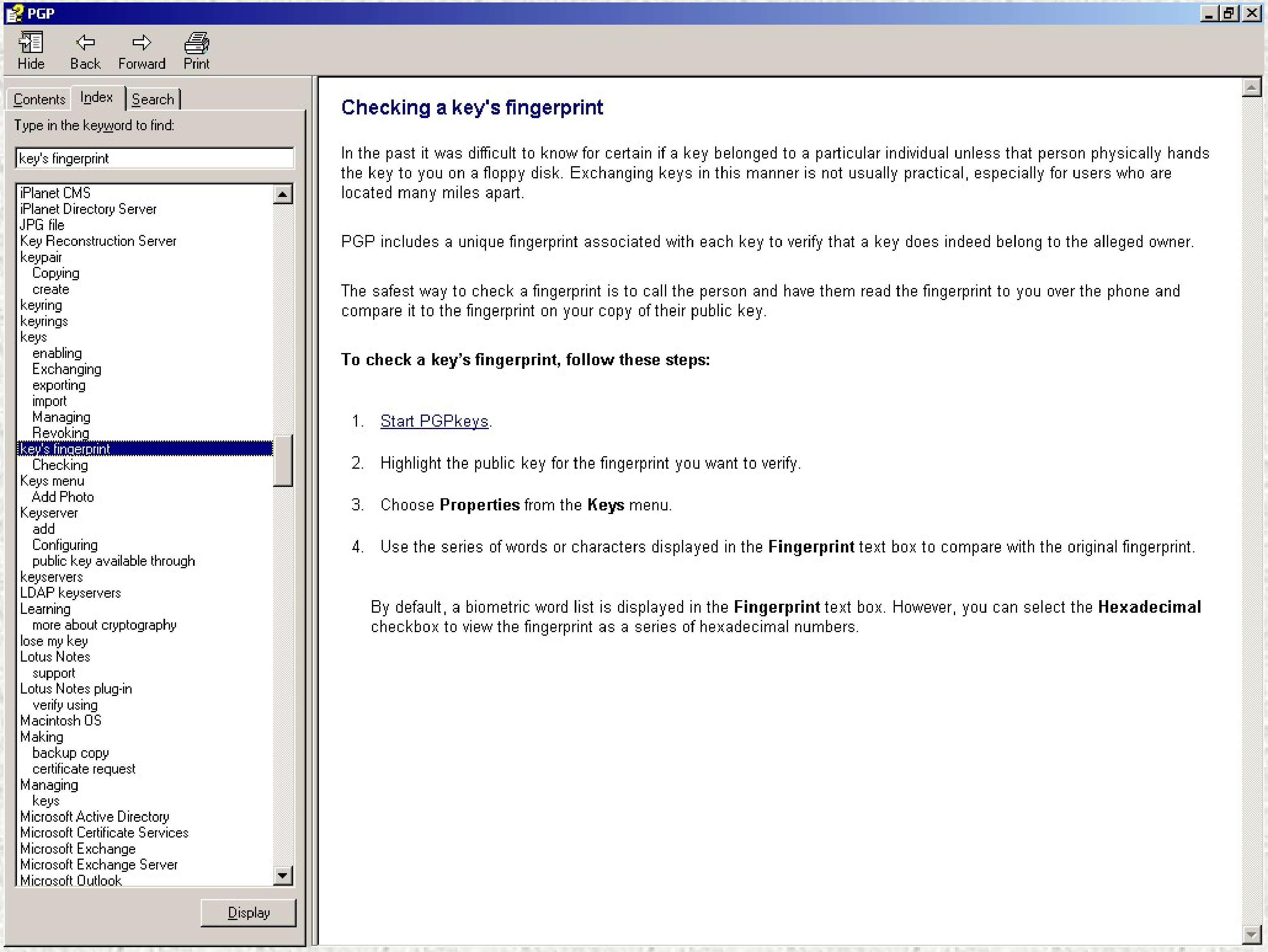
PGP Certificate
Signer Name: Routo Terada <rt@ime.usp.br>
Signer KeyID: 0xD2B77669 Trust Depth: 0
Domain Restriction: N/A

Created: 19/8/2003 Expires: Never

☑ Exportable ☐ Expired ☐ Revoked Show Signing Key Properties

Close Help

1 signature(s) selected



Checking a key's fingerprint

In the past it was difficult to know for certain if a key belonged to a particular individual unless that person physically hands the key to you on a floppy disk. Exchanging keys in this manner is not usually practical, especially for users who are located many miles apart.

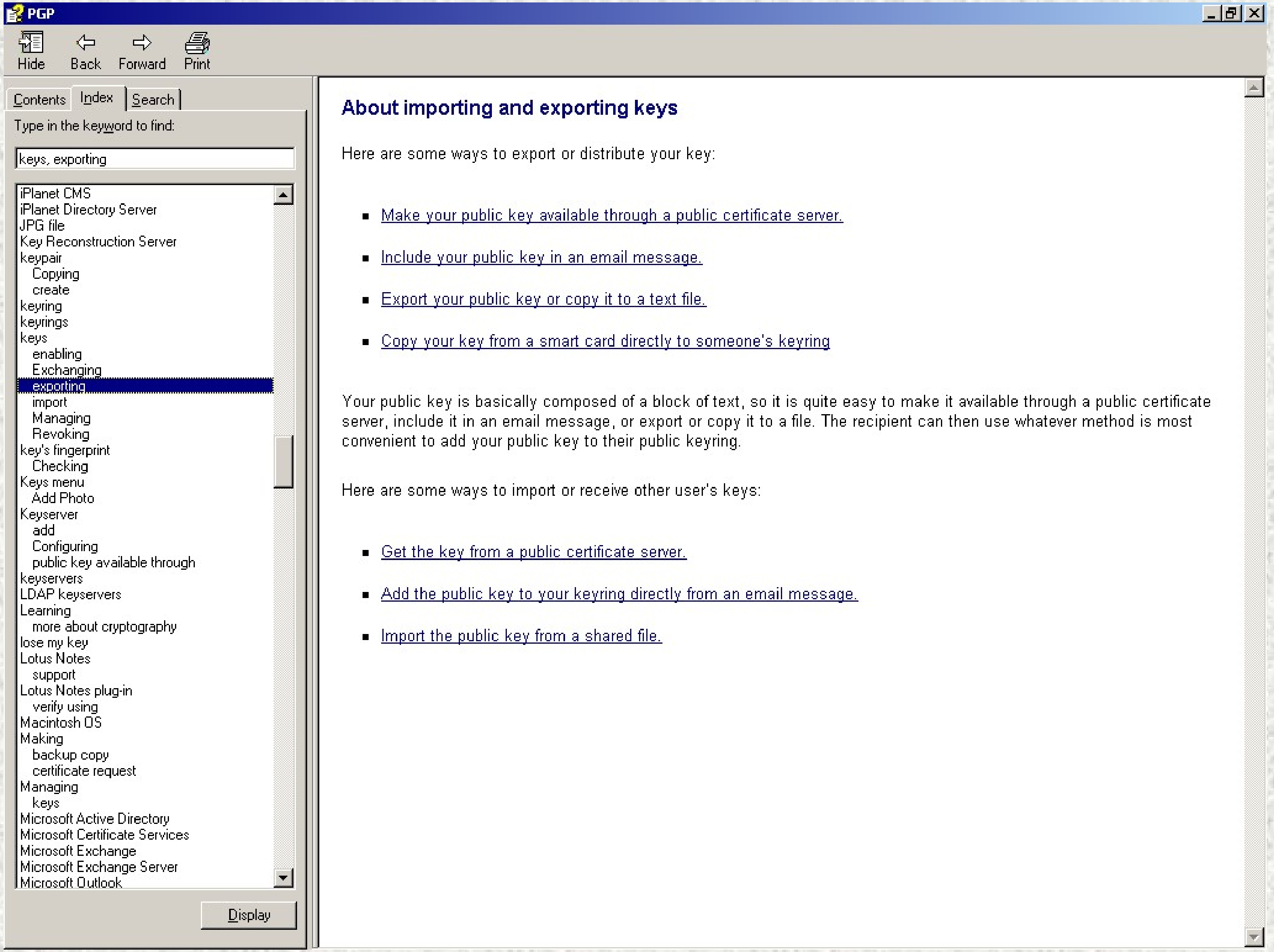
PGP includes a unique fingerprint associated with each key to verify that a key does indeed belong to the alleged owner.

The safest way to check a fingerprint is to call the person and have them read the fingerprint to you over the phone and compare it to the fingerprint on your copy of their public key.

To check a key's fingerprint, follow these steps:

1. Start PGPkeys.
2. Highlight the public key for the fingerprint you want to verify.
3. Choose **Properties** from the **Keys** menu.
4. Use the series of words or characters displayed in the **Fingerprint** text box to compare with the original fingerprint.

   By default, a biometric word list is displayed in the **Fingerprint** text box. However, you can select the **Hexadecimal** checkbox to view the fingerprint as a series of hexadecimal numbers.



About importing and exporting keys

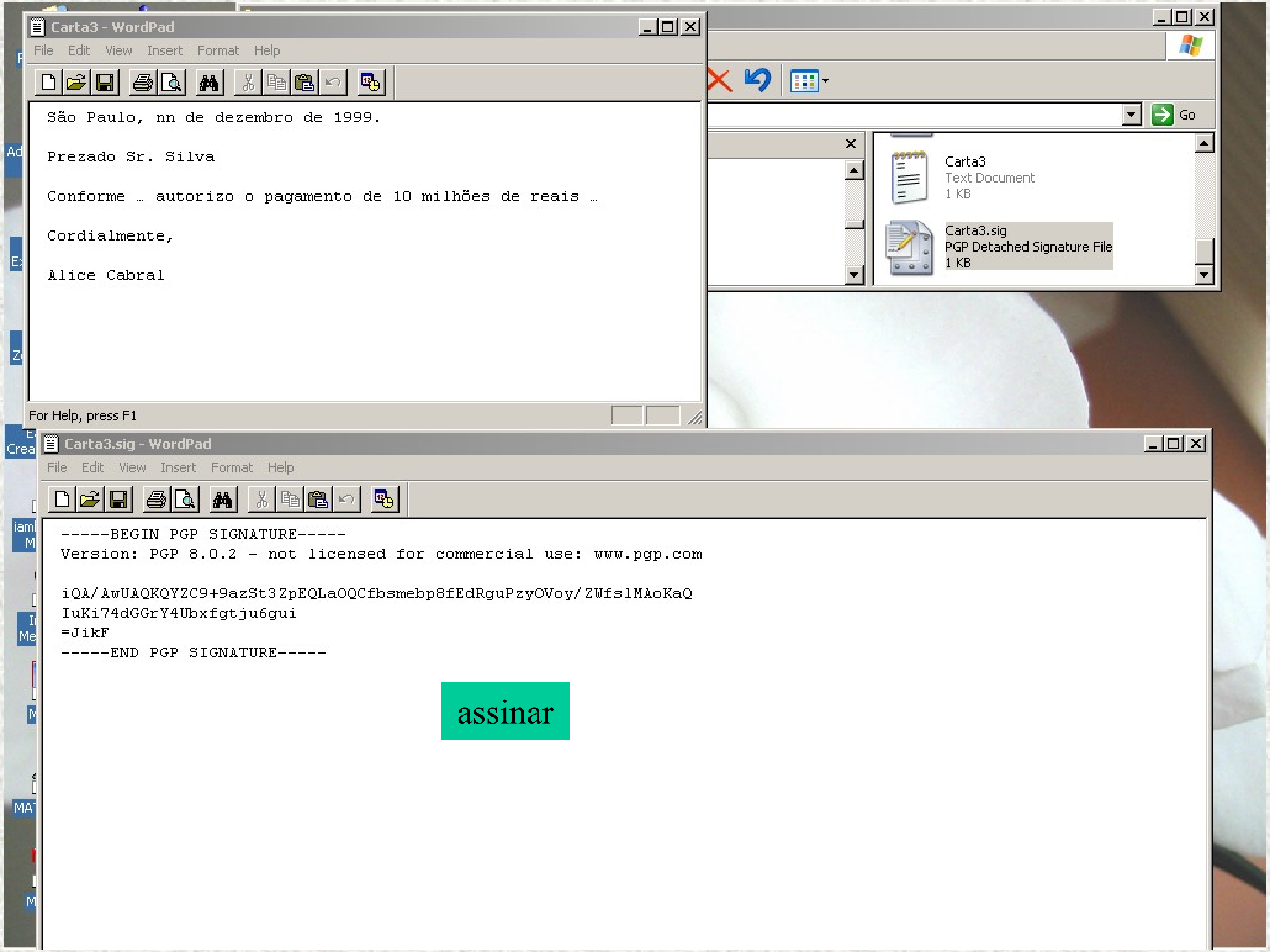
Here are some ways to export or distribute your key:

- Make your public key available through a public certificate server.
- Include your public key in an email message.
- Export your public key or copy it to a text file.
- Copy your key from a smart card directly to someone's keyring

Your public key is basically composed of a block of text, so it is quite easy to make it available through a public certificate server, include it in an email message, or export or copy it to a file. The recipient can then use whatever method is most convenient to add your public key to their public keyring.

Here are some ways to import or receive other user's keys:

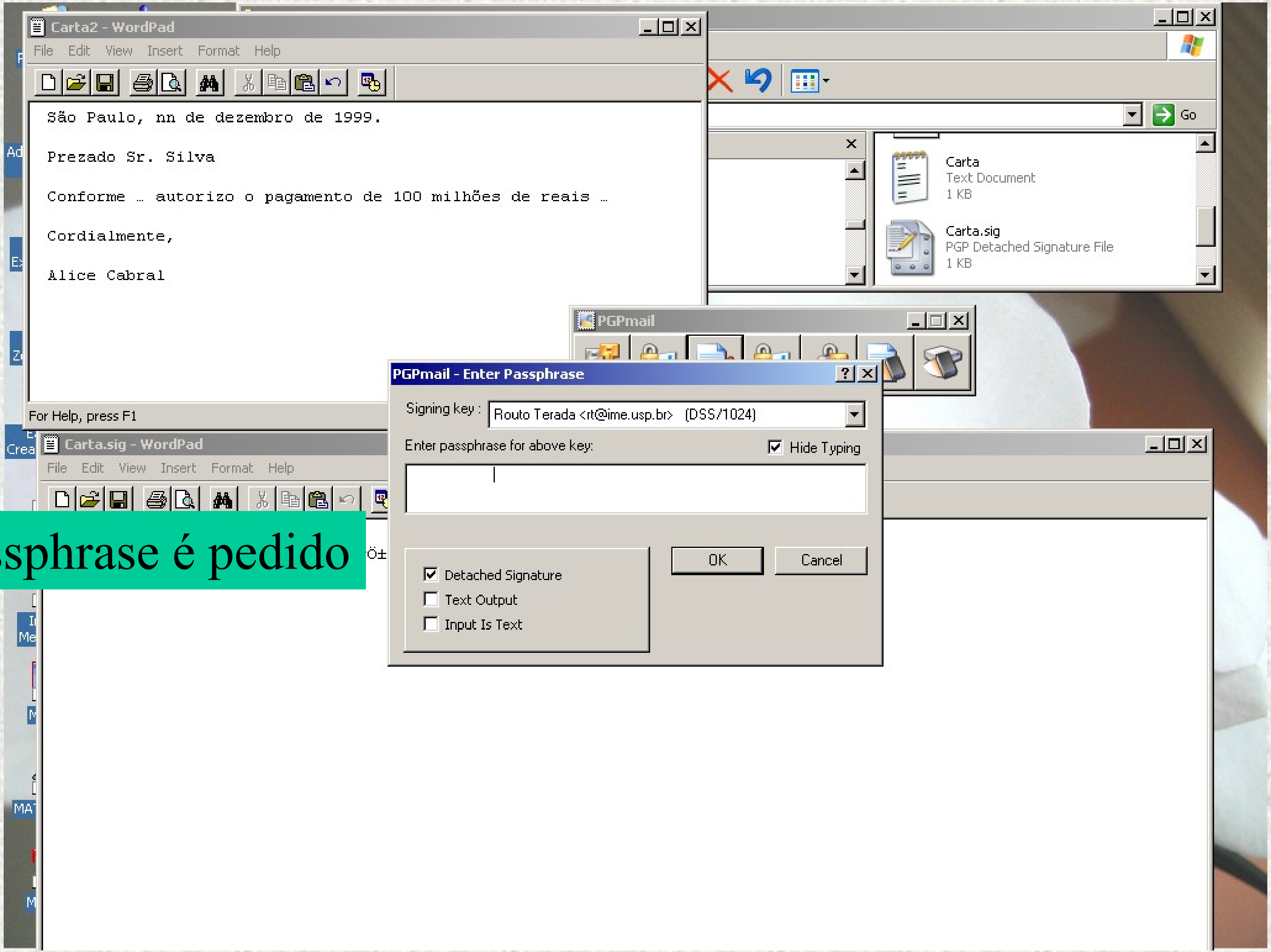
- Get the key from a public certificate server.
- Add the public key to your keyring directly from an email message.
- Import the public key from a shared file.


Carta3 - WordPad
File Edit View Insert Format Help
For Help, press F1
Go
Carta3
Text Document
1 KB
Carta3.sig
PGP Detached Signature File
1 KB
Carta3.sig - WordPad
File Edit View Insert Format Help

```
São Paulo, nn de dezembro de 1999.

Prezado Sr. Silva

Conforme … autorizo o pagamento de 10 milhões de reais …

Cordialmente,

Alice Cabral
```

```
-----BEGIN PGP SIGNATURE-----
Version: PGP 8.0.2 - not licensed for commercial use: www.pgp.com

iQA/AwUAQKQYZC9+9azSt3ZpEQLaOQCfbsmebp8fEdRguPzyOVoy/ZWfslMAoKaQ
IuKi74dGGrY4Ubxfgtju6gui
=JikF
-----END PGP SIGNATURE-----
```

assinar



Carta2 - WordPad
File Edit View Insert Format Help

```
São Paulo, nn de dezembro de 1999.

Prezado Sr. Silva

Conforme … autorizo o pagamento de 100 milhões de reais …

Cordialmente,

Alice Cabral
```

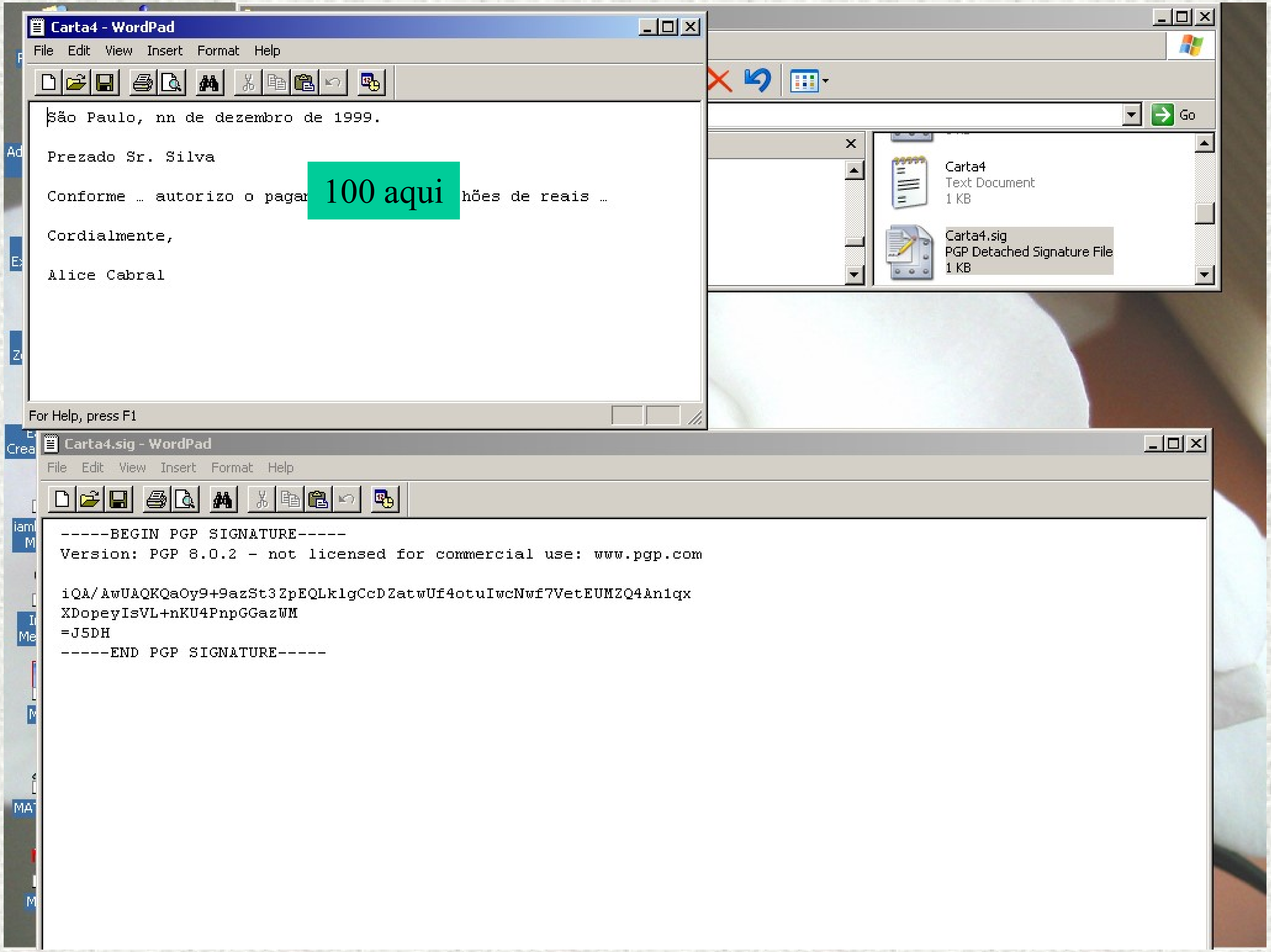
For Help, press F1
Carta
Text Document
1 KB
Carta.sig
PGP Detached Signature File
1 KB
Go
PGPmail
Carta.sig - WordPad
File Edit View Insert Format Help
PGPmail - Enter Passphrase

Signing key : Routo Terada <rt@ime.usp.br> (DSS/1024)

Enter passphrase for above key: ☑ Hide Typing

☑ Detached Signature
☐ Text Output
☐ Input Is Text

Passphrase é pedido


Carta4 - WordPad
File Edit View Insert Format Help
For Help, press F1
Carta4
Text Document
1 KB
Carta4.sig
PGP Detached Signature File
1 KB
Go
Carta4.sig - WordPad
File Edit View Insert Format Help

São Paulo, nn de dezembro de 1999.

Prezado Sr. Silva

Conforme … autorizo o pagar 100 aqui hões de reais …

Cordialmente,

Alice Cabral

```
-----BEGIN PGP SIGNATURE-----
Version: PGP 8.0.2 - not licensed for commercial use: www.pgp.com

iQA/AwUAQKQaOy9+9azSt3ZpEQLklgCcDZatwUf4otuIwcNwf7VetEUMZQ4An1qx
XDopeyIsVL+nKU4PnpGGazWM
=J5DH
-----END PGP SIGNATURE-----
```

São Paulo, nn de dezembro de 1999.

Prezado Sr. Silva

Conforme … autorizo o pagamento de 10 milhões de reais …

Cordialmente,

Alice Cabral

```
-----BEGIN PGP SIGNATURE-----
Version: PGP 8.0.2 - not licensed for commercial use: www.pgp.com
iQA/AwUAQKQYZC9+9azSt3ZpEQLaOQCfbsmebp8fEdRguPzyOVoy/ZWfslMAoKaQ
IuKi74dGGrY4Ubxfgtju6gui
=JikF
-----END PGP SIGNATURE-----
```

10

São Paulo, nn de dezembro de 1999.

Prezado Sr. Silva

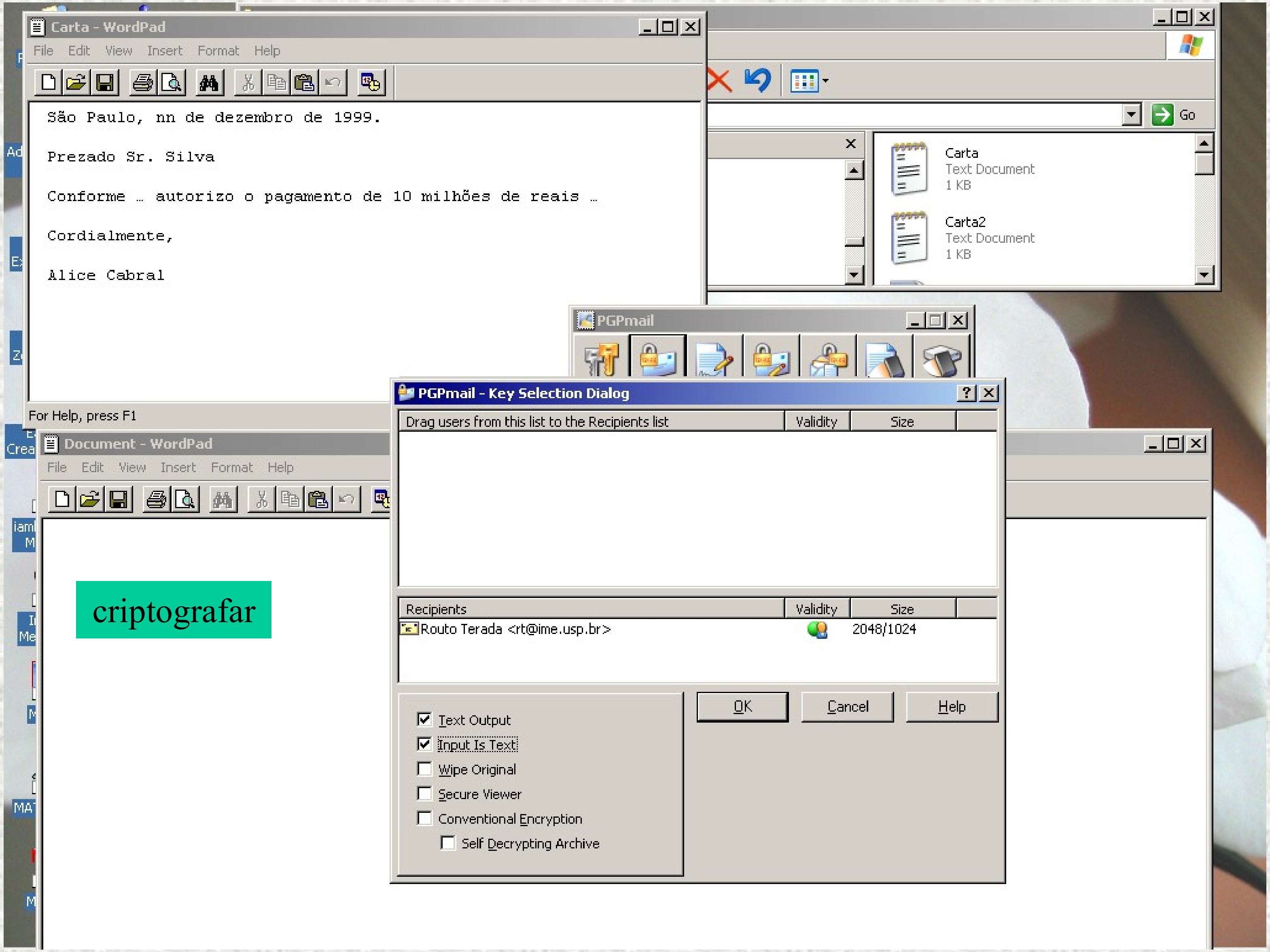
Conforme … autorizo o pagamento de 100 milhões de reais …

Cordialmente,

Alice Cabral

```
-----BEGIN PGP SIGNATURE-----
Version: PGP 8.0.2 - not licensed for commercial use: www.pgp.com

iQA/AwUAQKQaOy9+9azSt3ZpEQLklgCcDZatwUf4otuIwcNwf7VetEUMZQ4An1qx
XDopeyIsVL+nKU4PnpGGazWM
=J5DH
-----END PGP SIGNATURE-----
```

100



São Paulo, nn de dezembro de 1999.

Prezado Sr. Silva

Conforme … autorizo o pagamento de 10 milhões de reais …

Cordialmente,

Alice Cabral

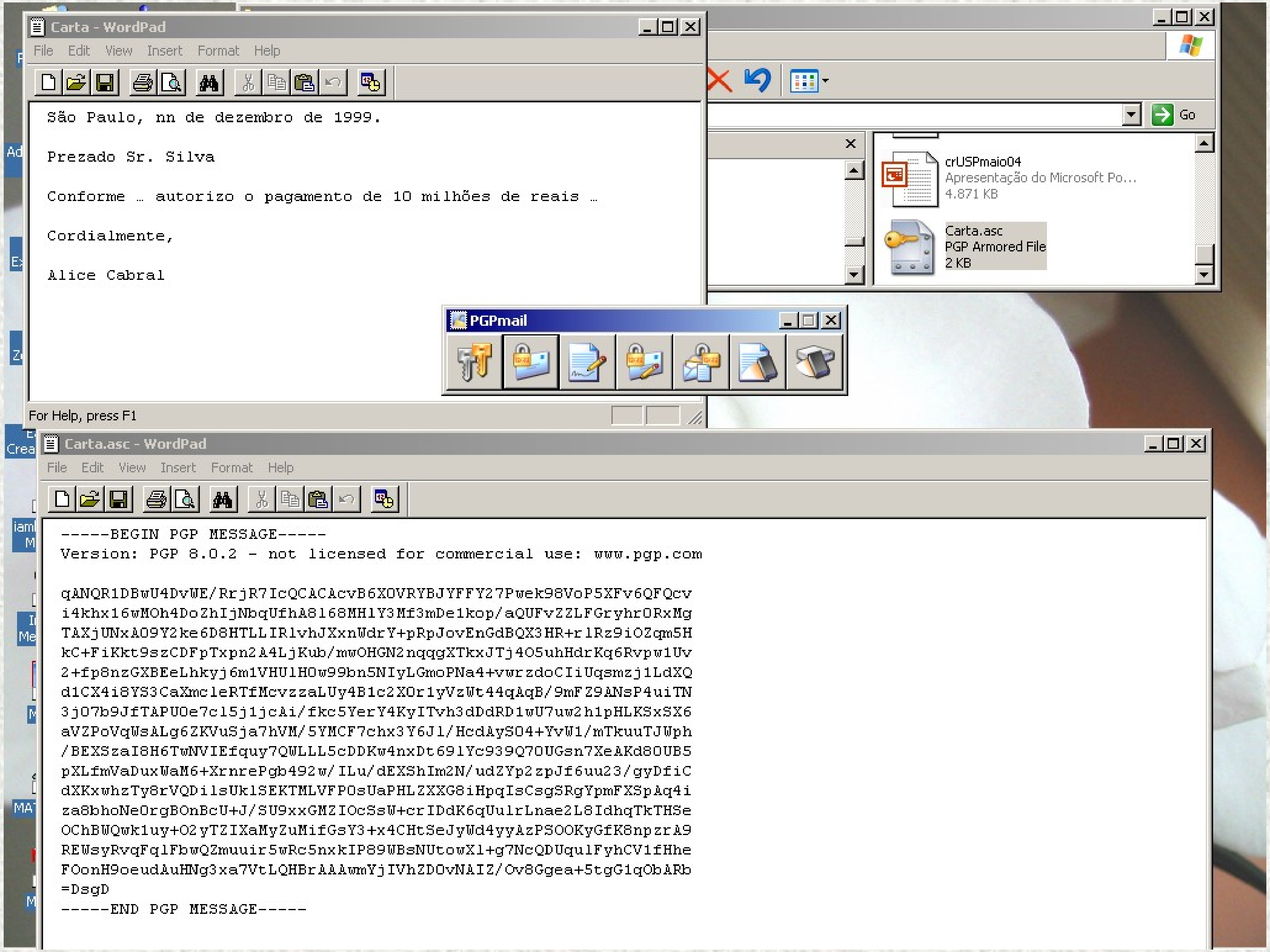
criptografar

PGPmail - Key Selection Dialog

Drag users from this list to the Recipients list	Validity	Size

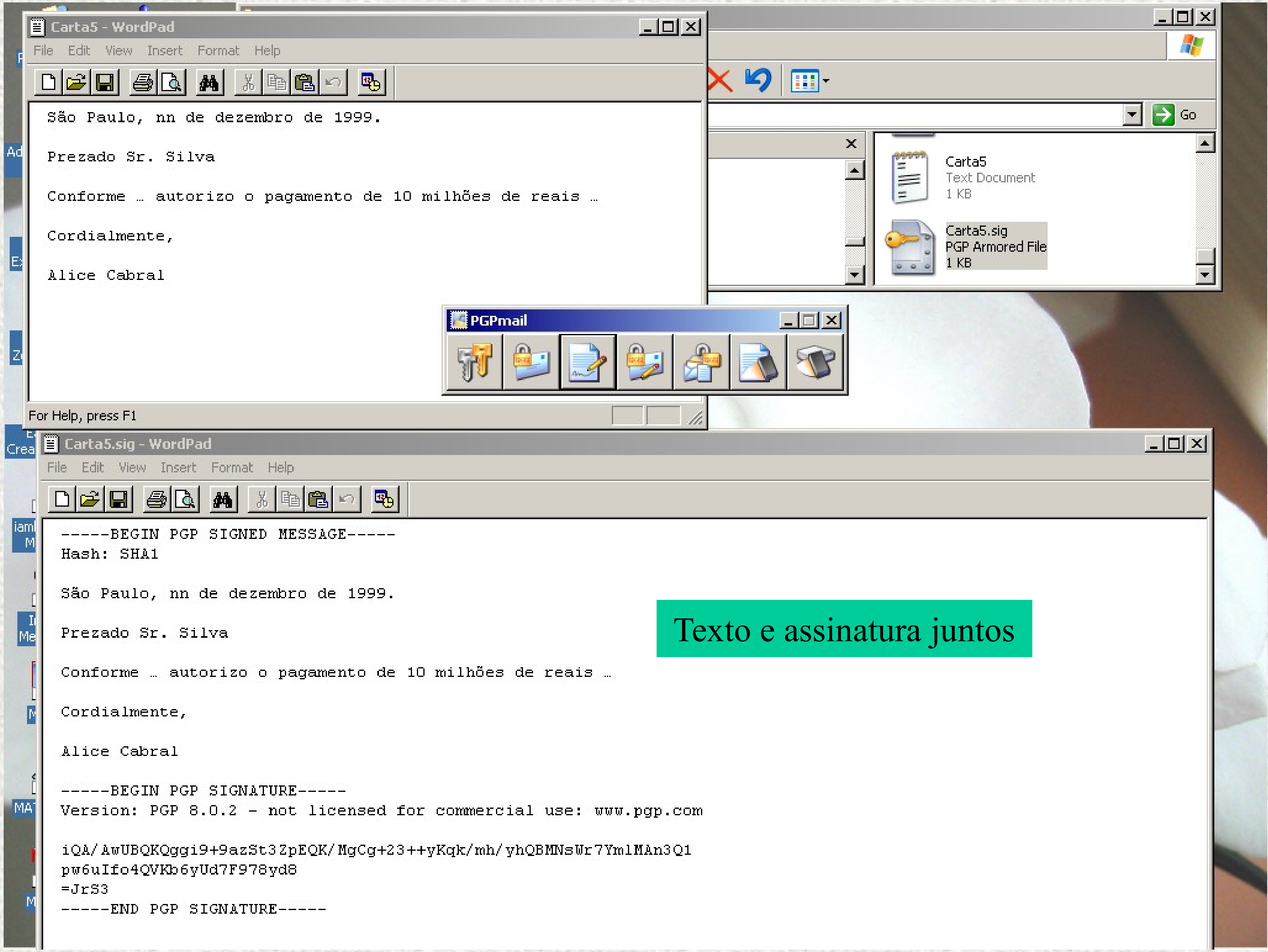
Recipients	Validity	Size
Routo Terada <rt@ime.usp.br>	●	2048/1024

☑ Text Output
☑ Input Is Text
☐ Wipe Original
☐ Secure Viewer
☐ Conventional Encryption
☐ Self Decrypting Archive



```
São Paulo, nn de dezembro de 1999.

Prezado Sr. Silva

Conforme … autorizo o pagamento de 10 milhões de reais …

Cordialmente,

Alice Cabral
```

```
-----BEGIN PGP MESSAGE-----
Version: PGP 8.0.2 - not licensed for commercial use: www.pgp.com

qANQR1DBwU4DvWE/RrjR7IcQCACAcvB6XOVRYBJYFFY27Pwek98VoP5XFv6QFQcv
i4khx16wMOh4DoZhIjNbqUfhA8168MHlY3Mf3mDe1kop/aQUFvZZLFGryhrORxMg
TAXjUNxA09Y2ke6D8HTLLIRlvhJXxnWdrY+pRpJovEnGdBQX3HR+r1Rz9iOZqm5H
kC+FiKkt9szCDFpTxpn2A4LjKub/mwOHGN2nqqgXTkxJTj4O5uhHdrKq6Rvpw1Uv
2+fp8nzGXBEeLhkyj6m1VHUlHOw99bn5NIyLGmoPNa4+vwrzdoCIiUqsmzj1LdXQ
d1CX4i8YS3CaXmcleRTfMcvzzaLUy4B1c2XOr1yVzWt44qAqB/9mFZ9ANsP4uiTN
3jO7b9JfTAPU0e7cl5j1jcAi/fkc5YerY4KyITvh3dDdRD1wU7uw2h1pHLKSxSX6
aVZPoVqWsALg6ZKVuSja7hVM/5YMCF7chx3Y6Jl/HcdAySO4+YvW1/mTkuuTJWph
/BEXSzaI8H6TwNVIEfquy7QWLLL5cDDKw4nxDt691Yc939Q7OUGsn7XeAKd8OUB5
pXLfmVaDuxWaM6+XrnrePgb492w/ILu/dEXShIm2N/udZYp2zpJf6uu23/gyDfiC
dXKxwhzTy8rVQDilsUklSEKTMLVFPOsUaPHLZXXG8iHpqIsCsgSRgYpmFXSpAq4i
za8bhoNeOrgBOnBcU+J/SU9xxGMZIOcSsW+crIDdK6qUulrLnae2L8IdhqTkTHSe
OChBWQwk1uy+O2yTZIXaMyZuMifGsY3+x4CHtSeJyWd4yyAzPSOOKyGfK8npzrA9
REWsyRvqFqlFbwQZmuuir5wRc5nxkIP89WBsNUtowXl+g7NcQDUqulFyhCV1fHhe
FOonH9oeudAuHNg3xa7VtLQHBrAAAwmYjIVhZDOvNAIZ/Ov8Ggea+5tgG1qObARb
=DsgD
-----END PGP MESSAGE-----
```

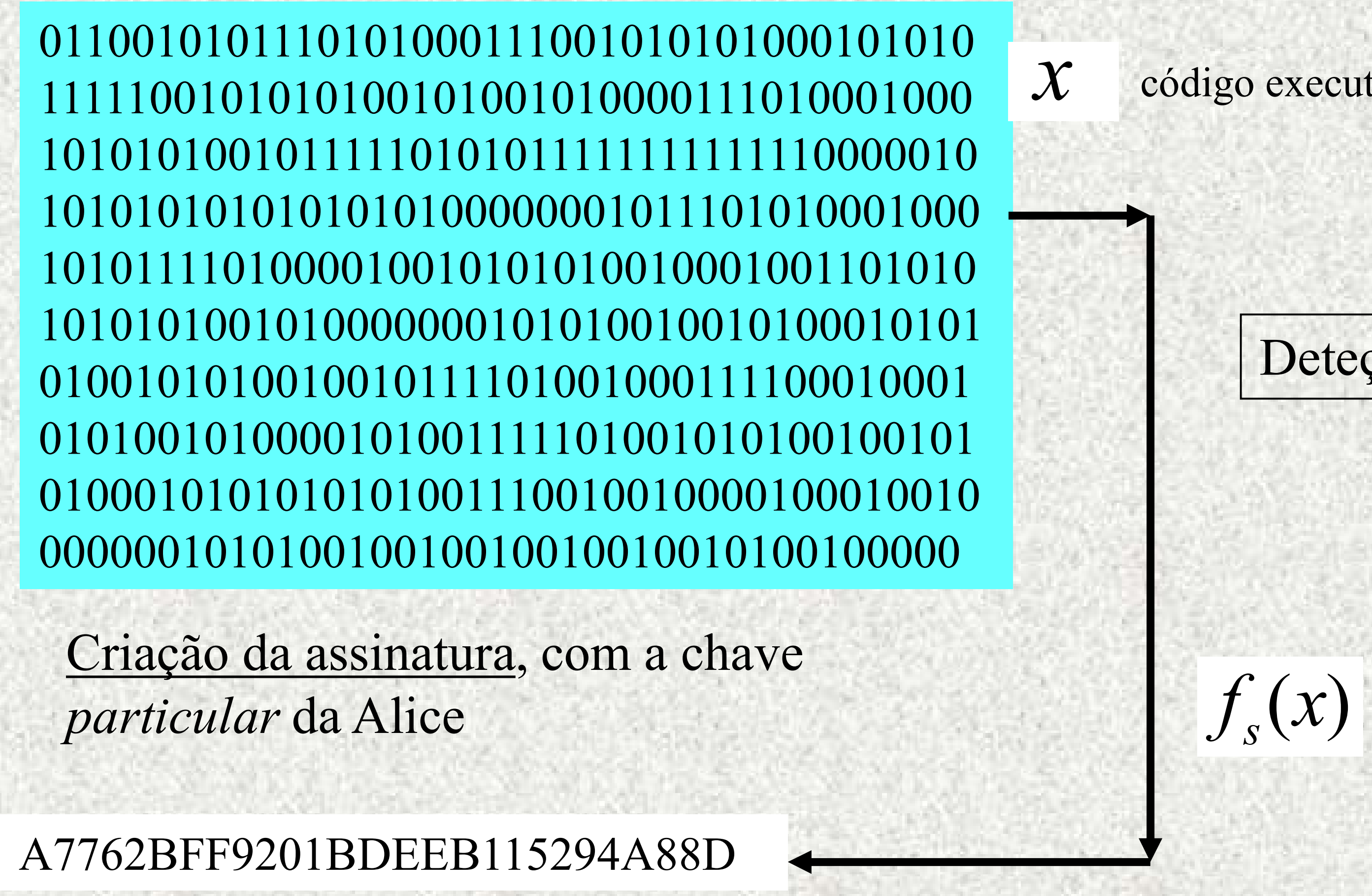


```
São Paulo, nn de dezembro de 1999.

Prezado Sr. Silva

Conforme … autorizo o pagamento de 10 milhões de reais …

Cordialmente,

Alice Cabral
```

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

São Paulo, nn de dezembro de 1999.

Prezado Sr. Silva

Conforme … autorizo o pagamento de 10 milhões de reais …

Cordialmente,

Alice Cabral

-----BEGIN PGP SIGNATURE-----
Version: PGP 8.0.2 - not licensed for commercial use: www.pgp.com

iQA/AwUBQKQggi9+9azSt3ZpEQK/MgCg+23++yKqk/mh/yhQBMNsWr7YmlMAn3Q1
pw6uIfo4QVKb6yUd7F978yd8
=JrS3
-----END PGP SIGNATURE-----
```

Texto e assinatura juntos

Vírus



```
0110010101110101000111001010101000101010
1111100101010100101001010000111010001000
1010101001011111010101111111111110000010
1010101010101010100000001011101010001000
1010111101000010010101010010001001101010
1010101001010000000101010010010100010101
0100101010010010111101001000111100010001
0101001010000101001111101001010100100101
0100010101010101001110010010000100010010
0000001010100100100100100100101001000000
```

x código executável

Deteção de vírus

$f_s(x)$

A7762BFF9201BDEEB115294A88D

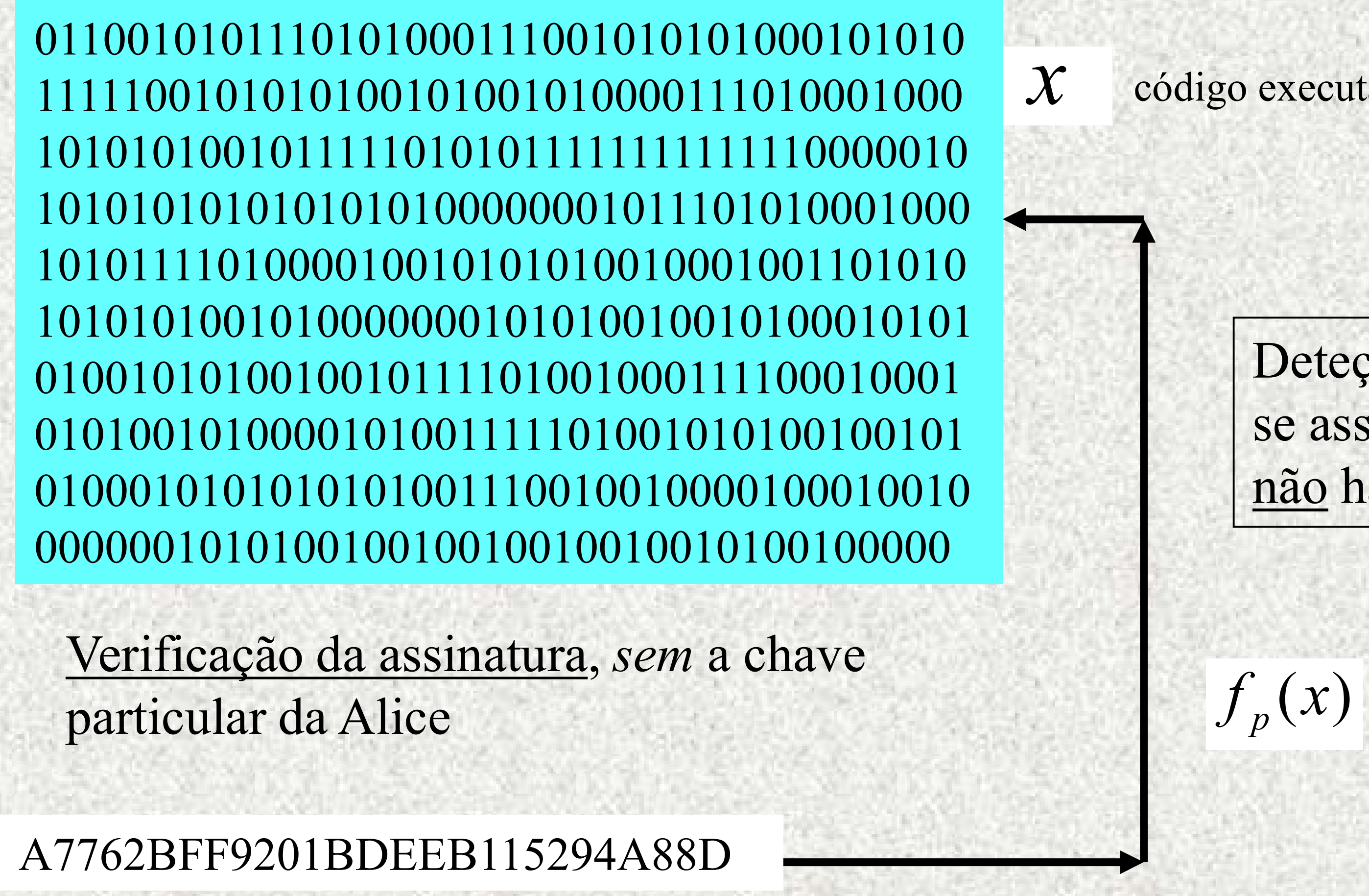
Criação da assinatura, com a chave *particular* da Alice

Assinatura criptográfica da Alice

(128 bits)

s é a chave particular da Alice

“vacinar”, “inocular”, etc..



```
0110010101110101000111001010101000101010
1111100101010100101001010000111010001000
1010101001011111010101111111111110000010
10101010101010101000000001011101010001000
1010111101000010010101010010001001101010
1010101001010000000101010010010100010101
0100101010010010111101001000111100010001
0101001010000101001111101001010100100101
0100010101010101001110010010000100010010
0000001010100100100100100100101001000000
```

x código executável

Vírus

Deteção de vírus:
se assinatura OK,
não há vírus em x

Verificação da assinatura, *sem* a chave particular da Alice

$f_p(x)$

A7762BFF9201BDEEB115294A88D

Assinatura criptográfica da Alice

(128 bits)

p é a chave pública da Alice

"vacinado", "inoculado", etc..

Pesquisas Recentes

- Identity Based Encryption: chave pública pode ser, por exemplo, o no. CPF
- Certificateless Public Key Encryption: chave pública pode ser o endereço Email
- Computador quântico
- Criptografia quântica
- Criptografia pós-quântica

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, 2008