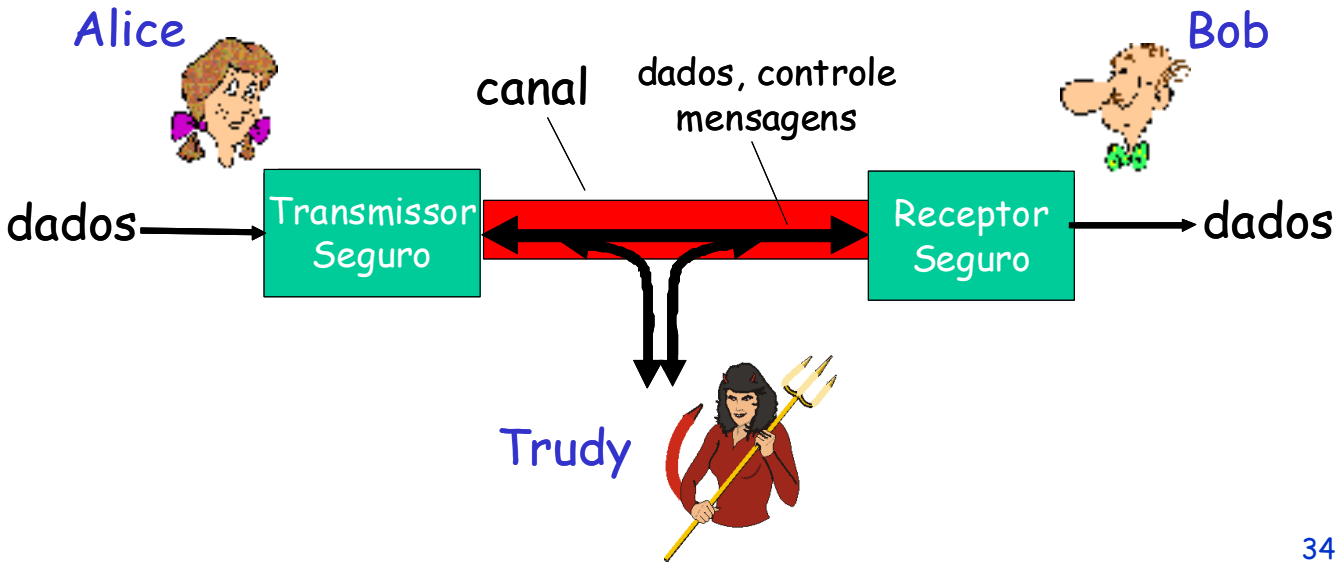
Unidade 2
Criptografia e Certificação Digital

Amigos e inimigos: Alice, Bob e Trudy

- ✓ Bob e Alice querem se comunicar "de forma segura".
- ✓ Trudy (intruso) pode interceptar, apagar e adicionar mensagens falsas.



Quem são Bob e Alice de fato?

Bobs e Alices!

- ✓ Web browser/servidor de transações eletrônicas (p.ex., compras on-line).
- ✓ Cliente/servidor de transações bancárias.
- ✓ Servidores DNS (Domain Name System).
- ✓ Roteadores atualizando tabelas de roteamento.

Quem é Trudy?

Adversário	Objetivo
Estudante	Divertir-se bisbilhotando as mensagens de correio eletrônico de outras pessoas
Hacker	Testar o sistema de segurança de alguém; roubar dados
Executivo	Descobrir estratégias de marketing do concorrente
Ex-funcionário	Vingar-se por ter sido demitido
Contador	Desfalcar dinheiro da empresa
Corretor de valores	Negar promessa feita a um cliente através de uma mensagem de correio eletrônico
Vigarista	Roubar número de cartões de crédito
Espião	Descobrir segredos militares do inimigo
Terrorista	Roubar segredos de armas bacteriológicas

Fonte: Tanenbaum

Tipos de Ataque

Grampo: interceptação de mensagens.

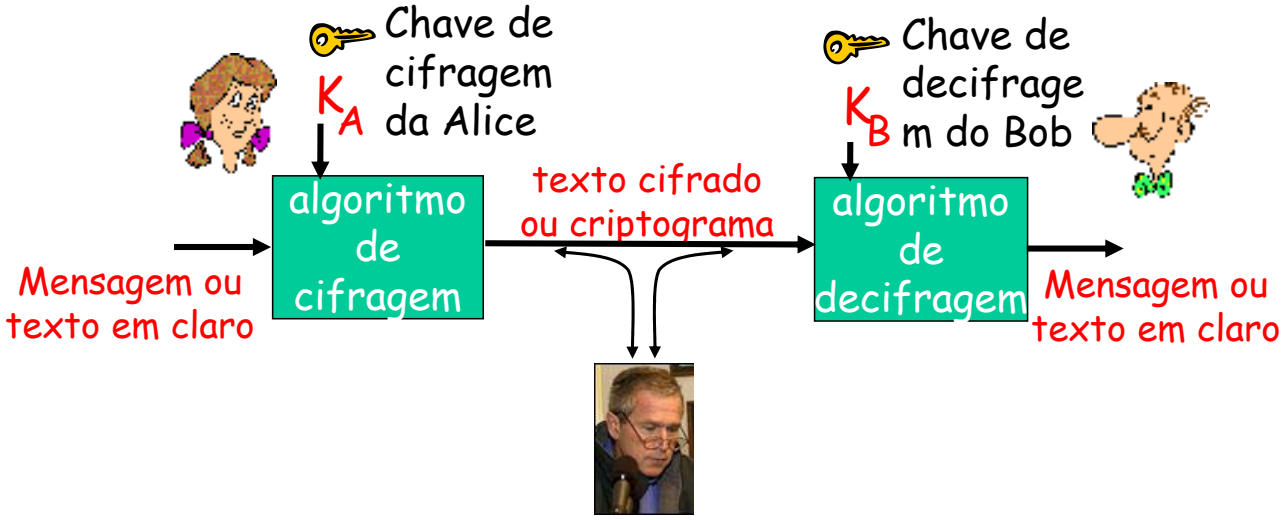
Inserção: envio de mensagens falsas.

Personalização: troca do endereço do remetente de um pacote (ou qualquer campo do pacote).

Sequestro: remoção do remetente ou do destinatário de uma conexão, inserindo-se no seu lugar.

Destruição de serviço: restrição ou negação de acesso a um serviço (ex. sobrecarga de recursos).

A nomenclatura em criptografia



Criptografia de chave simétrica: chaves de cifragem e decifragem *idênticas*.

Criptografia de chave assimétrica: chave de cifragem *pública*, chave de decifragem *secreta* (privada).

Criptografia de chave simétrica

Cifra de substituição: substitui-se uma coisa por outra.

- ✓ cifra monoalfabética: substitui-se um caractere por outro.
- ✓ cifra polialfabética: utiliza-se um conjunto de regras monoalfabéticas, de acordo com uma chave.

Exemplo: Chave simétrica monoalfabética

Mensagem: **bob, eu te amo. alice**

Chave: **M**

Criptograma: **nan, qg fq mya. mxuoq**

P: É difícil quebrar esta cifra simples?

Inatel
Instituto Nacional de Telecomunicações
Criptografia e Certificação Digital – Unid. 2

Cifra de Substituicão

Texto claro

Chave	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Cifra de Substituição
Exemplos:

1: Usando a Cifra de César (k=3), cifrar a mensagem: "Curso de Segurança em Redes"

2: Usando a cifra polialbabética com chave CPQ, cifrar a mensagem "Curso de Segurança em Redes"

Criptografia de chave simétrica

Cifra de transposição: reordena-se os caracteres sem, no entanto, substituí-los.

Ex.:

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Mensagem:

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

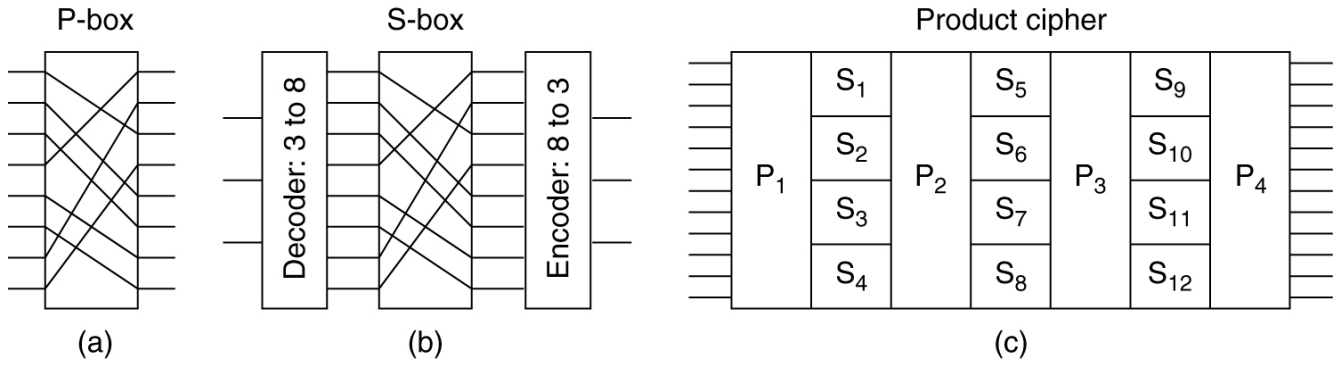
Criptograma:

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

Fonte: Tanenbaum

Criptografia de chave simétrica

Cifra de produto: mescla as técnicas de substituição e permutação.



Elementos básicos: (a) P-box. (b) S-box. (c) Produto.

Fonte: Tanenbaum

Inatel
Instituto Nacional de Telecomunicações
Criptografia e Certificação Digital – Unid. 2

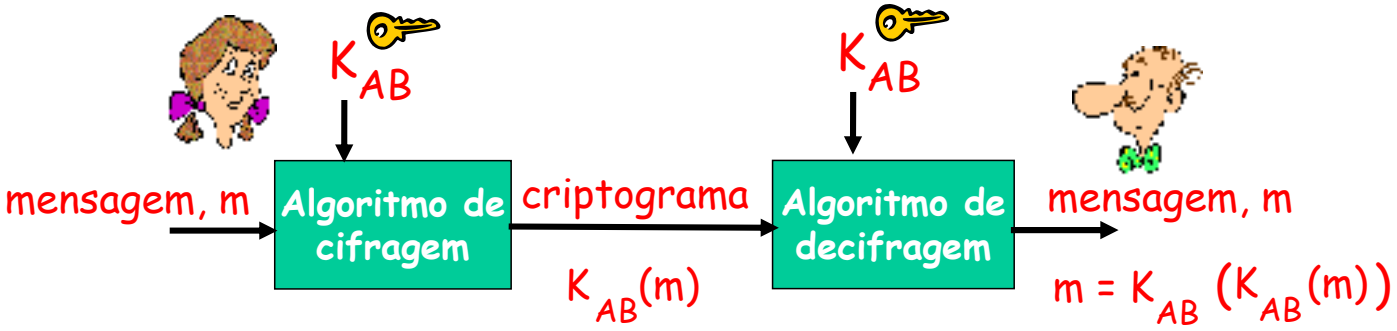
Cifra de Produto
Exemplos:

a) Caixa P
- entrada 0 1 2 3 4 5 6 7 → saída 3 6 0 7 1 2 4 5

b) Caixa S
- Entrada dos números octais 0 1 2 3 4 5 6 7.
- Saída dos valores octais 2 4 5 0 6 7 1 3.

c) Cifra de Produto
- Combinação de caixas P e S

Criptografia de chave simétrica



Criptografia simétrica: Bob e Alice compartilham a mesma chave: K_{AB}

- ✓ p.ex., a chave é o padrão de substituição na cifragem monoalfabética.
- ✓ P: Como Bob e Alice combinam uma chave em comum?

Inatel
Instituto Nacional de Telecomunicações
Criptografia e Certificação Digital – Unid. 2

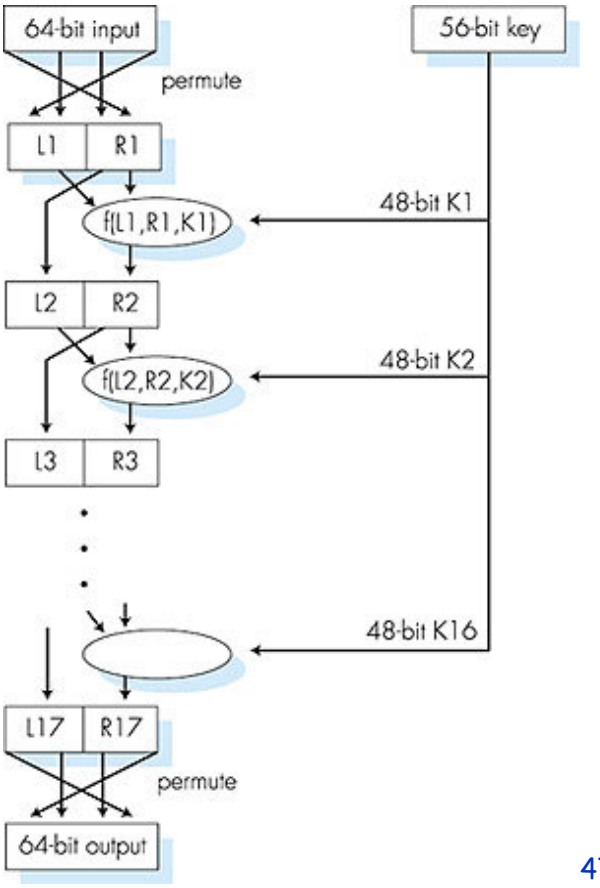
DES: Data Encryption Standard

- ✓ Versão refinada do algoritmo LUCIFER
  - Algoritmo concluído em 1971 pela IBM e vendido ao Lloyd´s Bank de Londres para uso em sistemas de caixa eletrônico. Chave de 128 bits.
- ✓ Os dados também são codificados em blocos de 64 bits, porém fazendo uso de uma chave de 56 bits.
- ✓ Adotado pelo NIST (National Institute of Standards and Technology) em 1977, como FIPS PUB 46 (Federal Information Processing Standard 46).

DES: visão geral

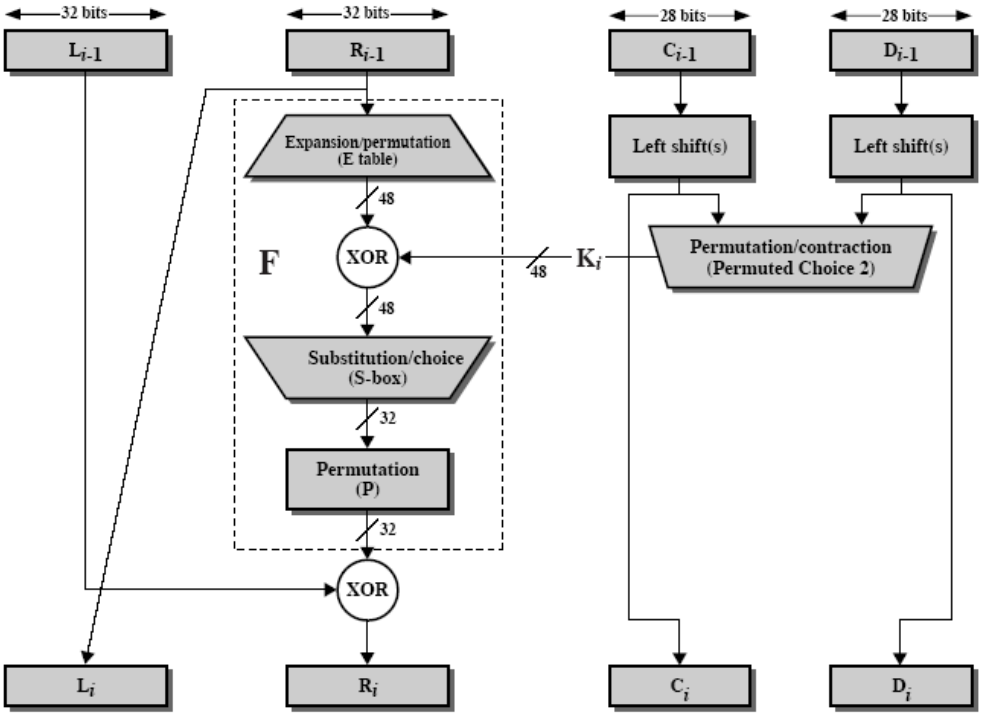
Operação DES

- permutação inicial.
- 16 "rounds" idênticos de cifragem de produto, usando sub-chaves diferentes de 48 bits.
- permutação final.
- decifragem: chaves em ordem inversa.



Inatel
Instituto Nacional de Telecomunicações
Criptografia e Certificação Digital – Unid. 2

DES: detalhe de cada *round*



Quão seguro é o DES

- ✓ Chave de 56 bits: existem 2^56 ≅ 7,2x10^16 chaves possíveis.

Fonte: Stallings

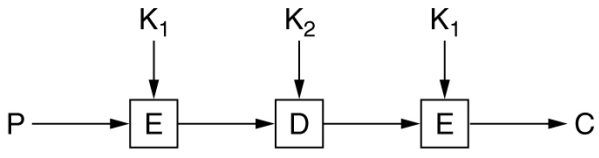
Tamanho da chave (bits)	No de Chaves	Tempo necessário para 1 decriptografia/μs	Tempo necessário para 10^6 decriptografias/μs
32	2^32 = 4,3x10^9	2^31 μs = 35,8 min	2,15 ms
56	2^56 = 7,2x10^16	2^55 μs = 1142 anos	10,01 horas
128	2^128 = 3,4x10^38	2^127 μs = 5,4x10^24 anos	5,4x10^18 anos
168	2^168 = 3,7X10^50	2^167 μs = 5,9x10^36 anos	5,9x10^30 anos
26 caracteres (permutação)	26! = 4x10^26	2x10^26 μs = 6,4x10x12 anos	6,4x10^6 anos

- ✓ Desafio DES (RSA Data Security Inc - 1997): frase cifrada com chave de 56 bits ("Strong cryptography makes the world a safer place") foi decifrada por força bruta em menos de 4 meses, após testado $\frac{1}{4}$ do espaço de chaves (cerca de 18 quatrilhões de chaves)

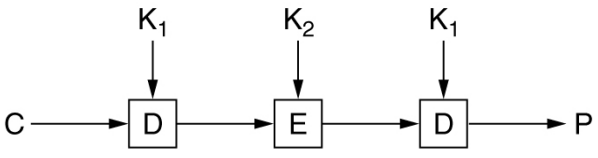
Inatel
Instituto Nacional de Telecomunicações
Criptografia e Certificação Digital – Unid. 2

Quão seguro é o DES

Em 1999, o NIST emitiu uma nova versão do padrão (FIPS PUB 46-3), onde o DES só deveria ser usado em sistemas legado; nos demais sistemas, deveria ser usado o 3-DES



cifragem



decifragem

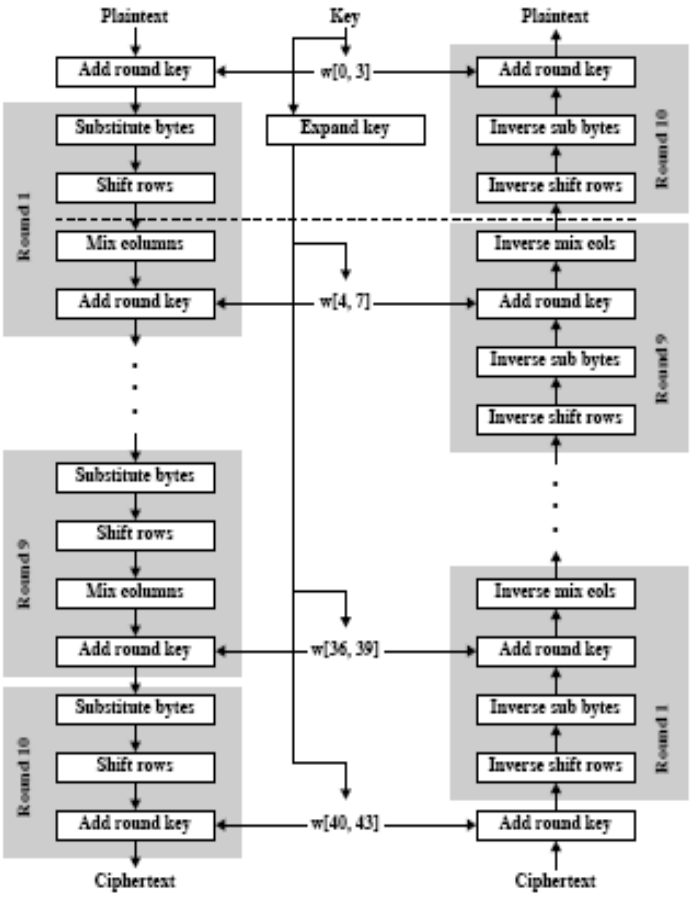
AES: Advanced Encryption Standard

- ✓ Em 1997, o NIST requisitou propostas para um novo padrão de criptografia, com grau de segurança igual ou superior ao 3-DES e uma eficiência melhorada (maior tamanho de bloco e processamento mais rápido)
- ✓ Algoritmo *Rijndael* (J. Daemen & V. Rijmen) foi selecionado dentre 15 concorrentes:
  - Processa os dados em blocos de 128 bits.
  - Chaves de 128, 192 ou 256 bits.
- ✓ Novo padrão foi publicado pelo NIST em novembro de 2001 (FIPS PUB 197).

AES: visão geral

Operação AES

- adição inicial.
- 10 "rounds" de cifragem, usando sub-chaves diferentes de 128 bits.
- não há mixagem no round final.
- Decifragem usa funções inversas.



Exemplos de algoritmos de chave simétrica

Cifra	Autor	Tamanho da Chave (bits)	Comentários
Blowfish	Bruce Schneier	1 a 448	Velho e lento
DES	IBM	56	Muito fraco para usar agora
IDEA	Massey e Xuejia	128	Bom, mas patenteado
RC4	Ronald Rivest	1 a 1024	Algumas chaves são fracas
RC5	Ronald Rivest	128 a 256	Bom, mas patenteado
Rijndael	Daemen e Rijmen	128 a 256	Melhor escolha
Serpent	Anderson, Biham, Knudsen	128 a 256	Muito forte
DES triplo	IBM	168	Segunda melhor escolha
Twofish	Bruce Schneier	128 a 256	Muito forte, amplamente utilizado

Fonte: Tanenbaum

Inatel
Instituto Nacional de Telecomunicações
Criptografia e Certificação Digital – Unid. 2

Criptografia de Chave Pública

Cripto. de chave *simétrica*

Requer que o remetente e o destinatário compartilhem uma chave secreta.

P: como estabelecer uma chave, a primeira vez (particularmente se nunca se "reuniram")?

Cripto. de chave *pública*

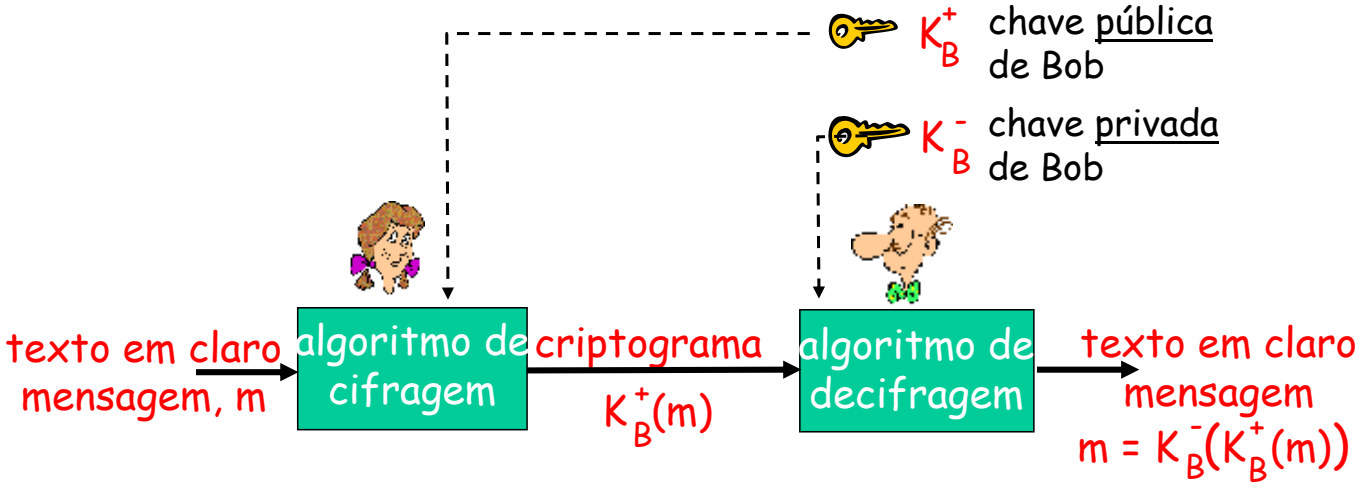
Enfoque radicalmente diferente [Diffie-Hellman 76, RSA 78].

O remetente e o destinatário não compartilham uma chave secreta.

Chave *pública* de cifragem é conhecida por *todos*.

Chave *privada* de decifragem é conhecida somente pelo destinatário.

Criptografia de Chave Pública



Algoritmos de chave pública

Requisitos (Diffie e Hellman, 1976):

1. funções $K_B^+(\cdot)$ e $K_B^-(\cdot)$ tais que

$$K_B^-(K_B^+(m)) = m$$

2. dada uma chave pública K_B^+, deve ser impraticável computar-se a chave privada K_B^-.

Algoritmo RSA: Rivest, Shamir, Adelson (1978)

RSA: Escolha das chaves

1. Selecione dois números primos grandes *p*, *q*.
2. Compute $n = pq$, $z = (p-1)(q-1)$.
3. Escolha e (com $e<n$) que não tenha fatores em comum com z. (e, z são "primos entre si").
4. Escolha d tal que $ed-1$ é divisível por z. (isto é: $ed \bmod z = 1$.)
5. A chave *pública* é o par $\underbrace{(n,e)}_{K_B^+}$. A chave *privada* é $\underbrace{(n,d)}_{K_B^-}$.

RSA: Cifragem e decifragem

0. Dados (n,e) e (n,d) conforme computado anteriormente,
1. Para cifrar a mensagem m, compute
   $c = m^e \bmod n$ (i.e., resto da divisão de m^e por n)
2. Para decifrar o criptograma, c, compute
   $m = c^d \bmod n$ (i.e., resto da divisão de c^d por n)

$$m = (\underbrace{m^e \bmod n}_{c})^d \bmod n$$

RSA: Exemplo

Bob escolhe *p=3*, *q=11*. Então, *n=33*, *z=20*.
e=3 (logo, *e* & *z* são primos entre si).
d=7 (logo, *ed-1* é divisível por z.)

	letra	m	m^e	$c = m^e \bmod n$
cifragem:	E	05	125	26

	c	c^d	$m = c^d \bmod n$	letra
decifragem:	26	8031810176	05	E

RSA: Exercício

Letra	m	m^e	$c = m^e \bmod n$	c^d	$m = c^d \bmod n$	Letra
I						
N						
A						
T						
E						
L						

cifragem decifragem

RSA: Por que $m = (m^e \bmod n)^d \bmod n$?

Teorema de Euler: Se p, q são primos e $n = pq$, então:

$$x^y \bmod n = x^{y \bmod (p-1)(q-1)} \bmod n$$

$$(m^e \bmod n)^d \bmod n = m^{ed} \bmod n$$

$$= m^{ed \bmod (p-1)(q-1)} \bmod n$$

(usando o teorema acima)

$$= m^1 \bmod n$$

(já que escolhemos ed divisível por $(p-1)(q-1)$ com resto 1)

$$= m$$

RSA: outra propriedade importante

A seguinte propriedade será *muito* útil adiante:

$$\underbrace{K_B^-(K_B^+(m))}_{\text{usa a chave pública antes, seguida da chave privada}} = m = \underbrace{K_B^+(K_B^-(m))}_{\text{usa a chave privada antes, seguida da chave pública}}$$

O resultado é o mesmo!

RSA: Segurança

- ✓ A segurança do RSA se baseia na dificuldade em se fatorar grandes números rapidamente.
- ✓ Em 1977, Rivest lançou um desafio pela revista Scientific American, usando uma chave (n) de 129 dígitos (≈ 428 bits), que na época levaria 40 quatrilhões de anos para ser fatorado.
- ✓ Em 1994 Lenstra anunciou a quebra do RSA-129. Para conseguir essa proeza, ele recrutou 600 voluntários pela Internet.
- ✓ O número RSA-129 e seus dois fatores:

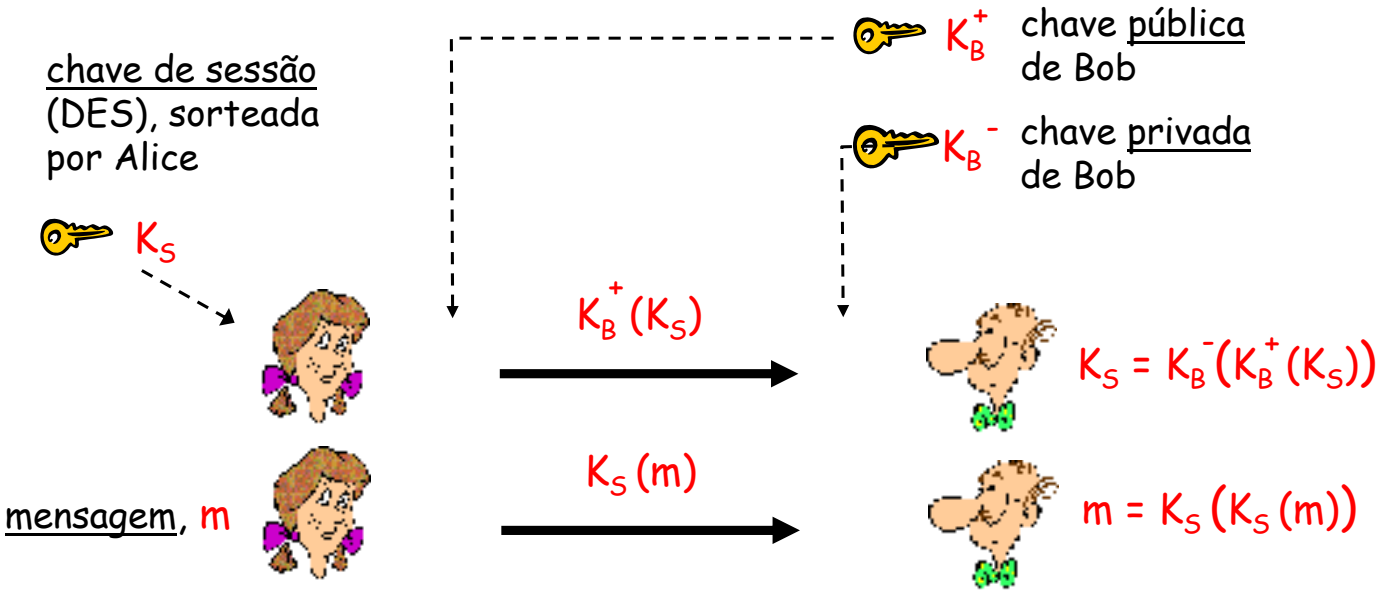
```
114381625757888867669235779976146612010218296721242362562561842935706935
245733897830597123563958705058989075147599290026879543541 =

349052951084765094914784961990389813341776463849338784399082057 7

                                  ×

327691329932667095499619881908344614131776429679929425397982885 33
```


RSA: Desempenho

- ✓ Atualmente, considera-se que o RSA é seguro se *n* é da ordem de 768 bits para *aplicações domésticas*, e 1024 bits para *aplicações corporativas*.
- ✓ As operações de exponenciação de números de centenas de bits requeridas pelo RSA demandam muito tempo de processamento. Tipicamente, para computadores pessoais obtém-se taxas de algumas dezenas de kilobits por segundo.
- ✓ Os algoritmos simétricos DES ou AES permitem a operação centenas ou milhares de vezes mais rápida.
- ✓ É comum se adotar um sistema misto RSA + DES.

Sistema Misto RSA/DES

Objetivo: Alice quer enviar uma grande quantidade de dados cifrados para Bob.



Inatel
Instituto Nacional de Telecomunicações
Criptografia e Certificação Digital – Unid. 2

Autenticação

Objetivo: Bob quer que Alice "prove" sua identidade para ele.

Protocolo ap1.0: Alice diz "Eu sou Alice".

Falha na segurança??

Autenticação

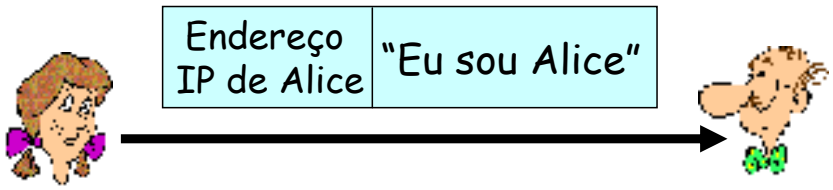
Objetivo: Bob quer que Alice "prove" sua identidade para ele.

Protocolo ap1.0: Alice diz "Eu sou Alice".

Identidade falsa: - Numa rede de dados, Bob não pode "ver" Alice, assim Trudy simplesmente se declara como sendo Alice!

Autenticação: outra tentativa

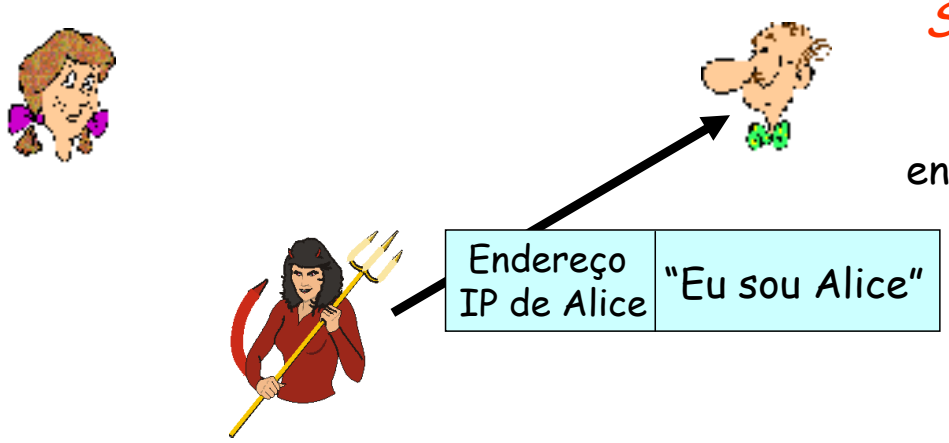
Protocolo ap2.0: Alice diz "Eu sou Alice" em um pacote IP contendo seu endereço IP.



Falha na segurança??

Autenticação: outra tentativa

Protocolo ap2.0: Alice diz "Eu sou Alice" em um pacote IP contendo seu endereço IP.

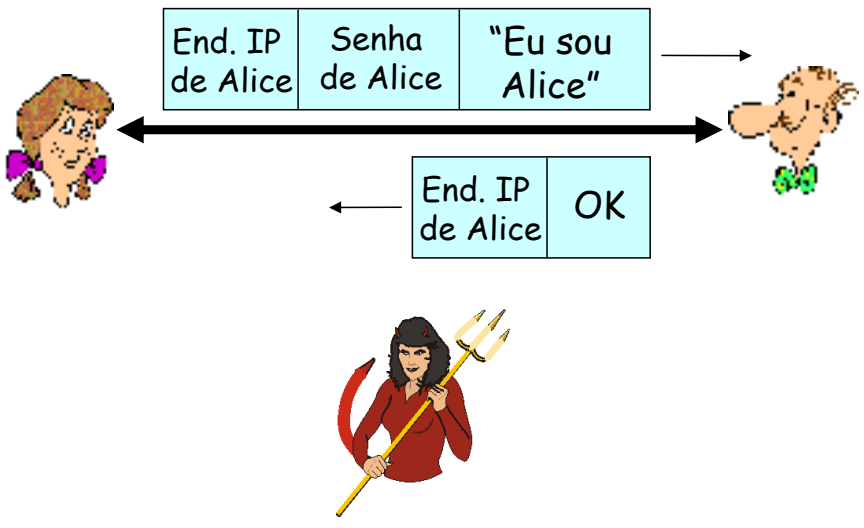


Spoofing: - Trudy pode criar um pacote com o endereço IP de Alice.

Inatel
Instituto Nacional de Telecomunicações
Criptografia e Certificação Digital – Unid. 2

Autenticação: outra tentativa

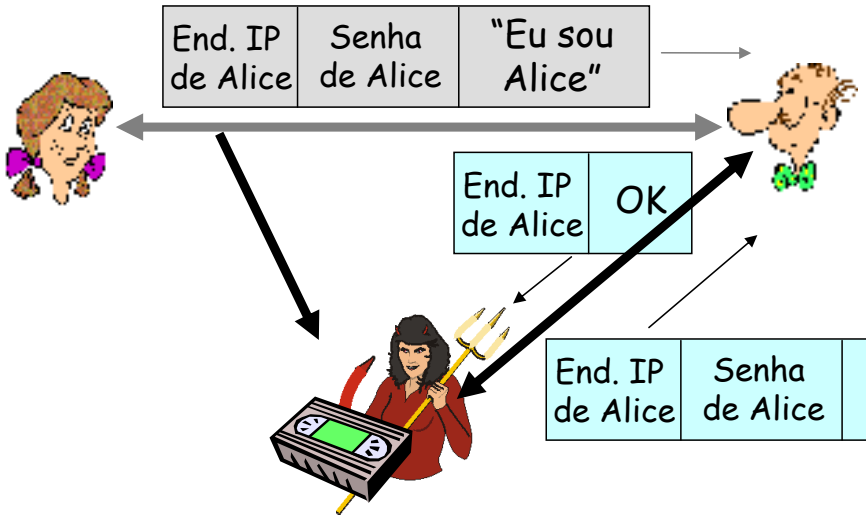
Protocolo ap3.0: Alice diz "Eu sou Alice" e envia sua senha secreta para "prová-lo".



Falha na segurança??

Autenticação: outra tentativa

Protocolo ap3.0: Alice diz "Eu sou Alice" e envia sua senha secreta para "prová-lo".

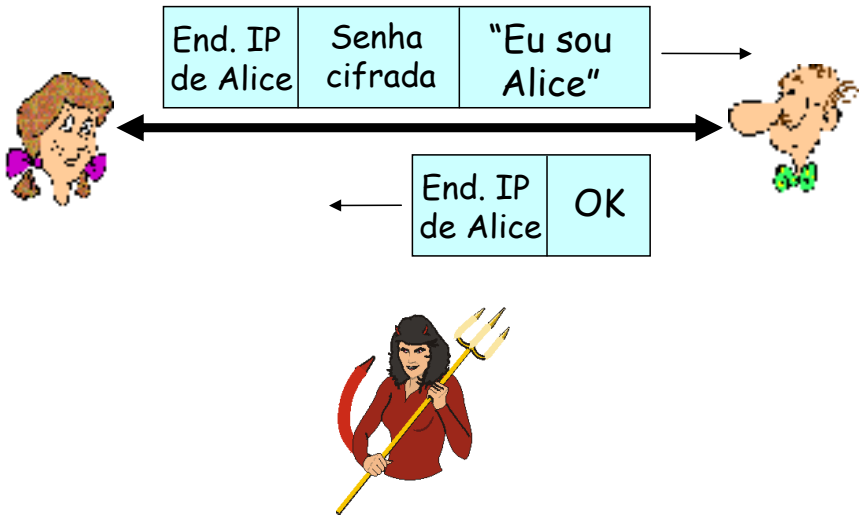


Ataque playback:
- Trudy grava o pacote de Alice e o envia para Bob mais tarde.

Inatel
Instituto Nacional de Telecomunicações
Criptografia e Certificação Digital – Unid. 2

Autenticação: ainda outra tentativa

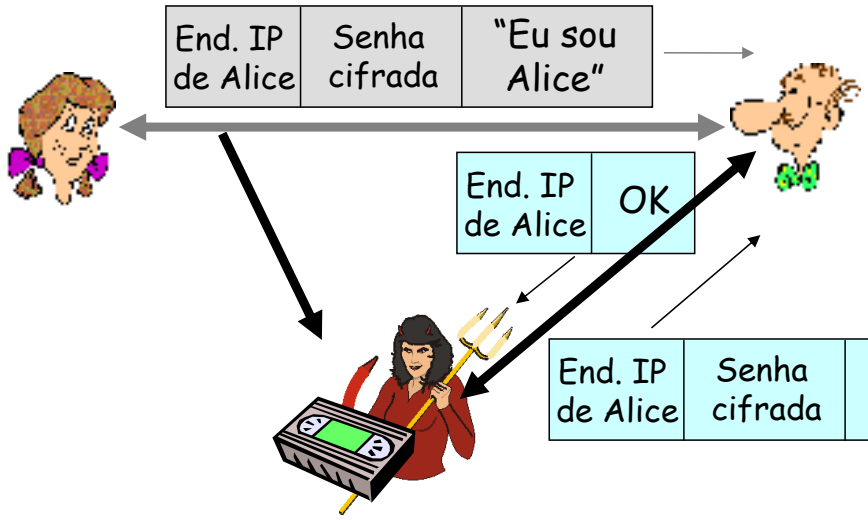
Protocolo ap3.1: Alice diz "Eu sou Alice" e envia sua senha secreta *criptografada* para "prová-lo".



Falha na segurança??

Autenticação: ainda outra tentativa

Protocolo ap3.1: Alice diz "Eu sou Alice" e envia sua senha secreta *criptografada* para "prová-lo".



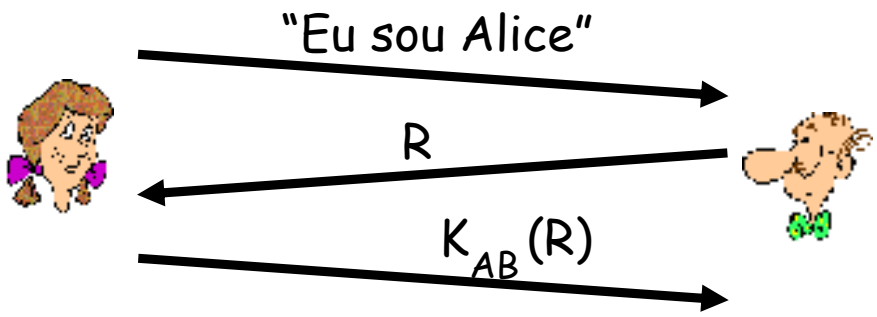
Ataque de *playback* ainda funciona!

Autenticação: mais outra tentativa

Objetivo: evitar o ataque de playback.

Nonce: número (R) usado só *uma vez na vida.*

ap4.0: para provar que Alice está "viva", Bob envia para Alice um nonce (R). Alice deve retornar R, cifrado com a chave secreta conhecida apenas por eles.



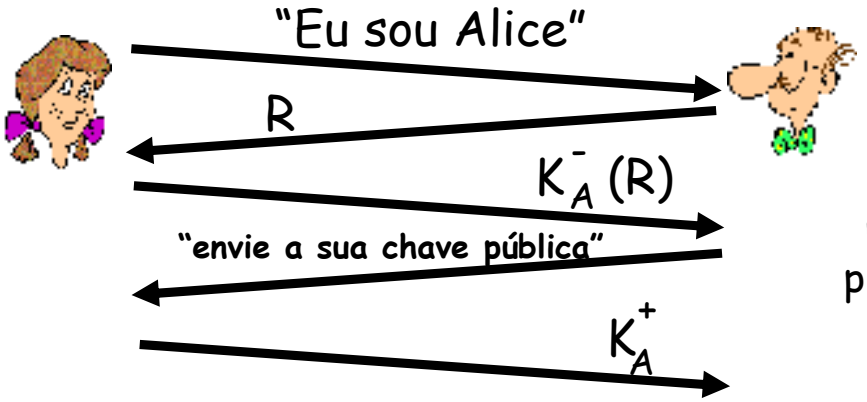
Alice está viva, e só ela conhece a chave para cifrar o nonce, logo ela deve ser Alice!

Autenticação: mais outra tentativa

ap4.0 requer chave simétrica compartilhada.

É possível efetuar autenticação usando técnicas de chave pública?

ap5.0: usa nonce e criptografia de chave pública.

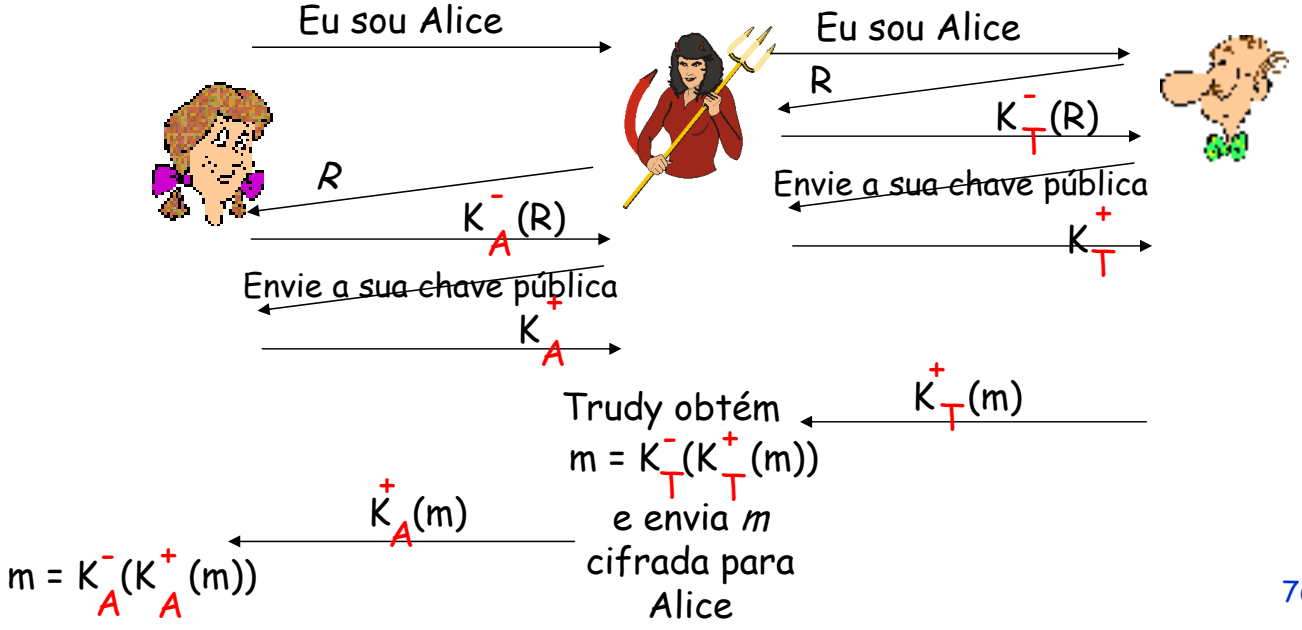


Bob computa
$K_A^+(K_A^-(R)) = R$
e sabe que só Alice poderia ter a chave privada que cifraria R tal que
$K_A^+(K_A^-(R)) = R$

Inatel
Instituto Nacional de Telecomunicações
Criptografia e Certificação Digital – Unid. 2

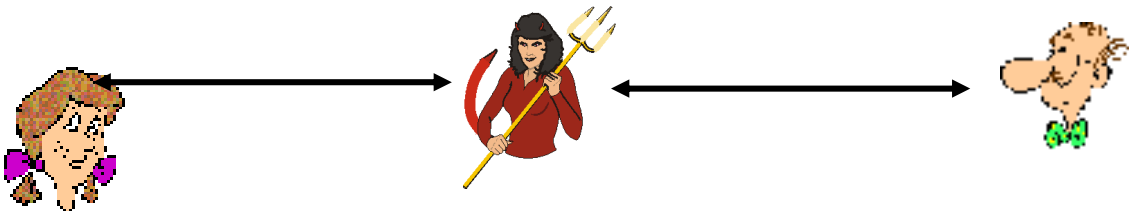
ap5.0: furo na segurança

Ataque "homem no meio": Trudy se passa por Alice (para Bob) e como Bob (para Alice).



ap5.0: furo na segurança

Ataque "homem no meio": Trudy se passa por Alice (para Bob) e como Bob (para Alice).



Difícil de detectar:

- ✓ Bob recebe tudo que Alice transmite, e vice-versa. (i.e., Bob e Alice podem se encontrar uma semana mais tarde e lembrar da conversa.
- ✓O problema é que Trudy recebe todas as mensagens também!

Inatel
Instituto Nacional de Telecomunicações
Criptografia e Certificação Digital – Unid. 2

Assinaturas Digitais

Técnica criptográfica análoga às assinaturas a mão livre.

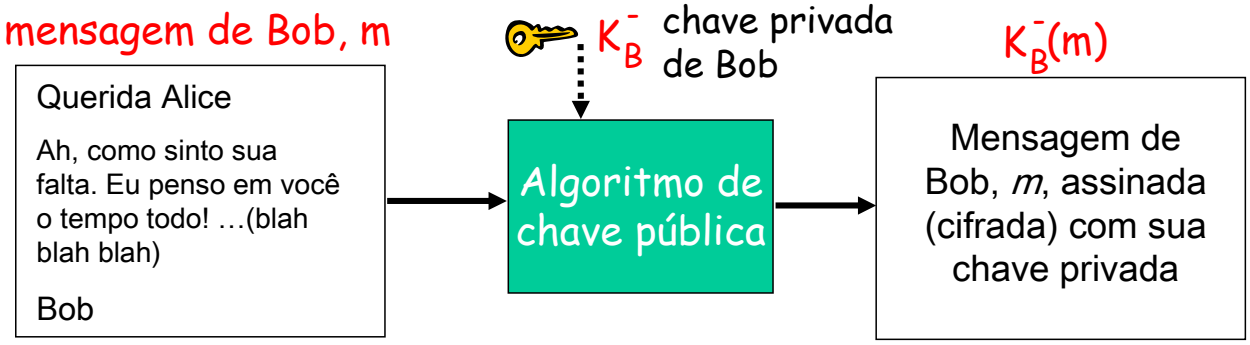
O remetente (Bob) assina digitalmente o documento, estabelecendo que ele é o autor/proprietário do mesmo.

O destinatário (Alice) pode provar que Bob, e ninguém mais (inclusive Alice), deve ter assinado o documento.

Assinaturas Digitais

Assinatura digital simples da mensagem *m*:

Bob assina *m* cifrando-a com sua chave privada K_B^-, criando a mensagem "assinada", $K_B^-(m)$.



Inatel
Instituto Nacional de Telecomunicações
Criptografia e Certificação Digital – Unid. 2

Assinaturas Digitais

Suponha que Alice receba a mensagem *m* e a correspondente assinatura digital $K_B^-(m)$.

Alice verifica se *m* está assinada por Bob aplicando a chave pública de Bob e verificando se $K_B^+(K_B^-(m)) = m$.

Alice verifica que:

- ✓ Bob assinou *m*.
- ✓ Ninguém mais assinou *m*.
- ✓ Bob assinou *m* e não *m'*.

Bob não pode negar:

- ✓ Alice pode apresentar *m*, e a assinatura $K_B^-(m)$ em juízo e provar que Bob assinou *m*.

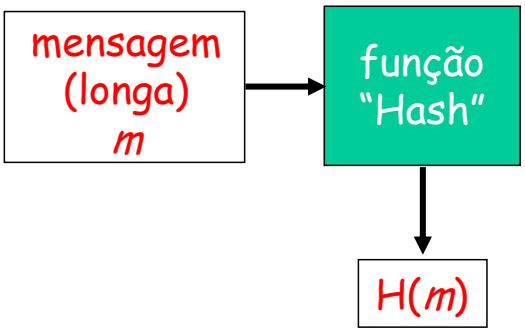
Resumo de mensagem

Cifragem de mensagens longas com algoritmo de chave pública é ineficiente.

Objetivo:

Obter uma "impressão digital" da mensagem, de tamanho fixo e de cômputo simples.

Aplica-se a função "hash" H em *m*, obtendo-se o resumo da mensagem, H(*m*).



Propriedades funções Hash:

Função *muitos-para-um*,

produzem resumos de mensagens de tamanho fixo (*impressão digital*)

Dado o resumo *x*, é impra-ticável encontrar *m* tal que *x* = H(*m*).

Inatel
Instituto Nacional de Telecomunicações
Criptografia e Certificação Digital – Unid. 2

Checksum: uma função hash fraca

O *checksum*, muito usado na Internet, tem algumas propriedades de uma função hash:

- ✓ produz resumos de mensagens de tamanho fixo (soma de 16-bit).
- ✓ Função do tipo "muitos-para-um".

Mas, dada uma mensagem com um certo checksum, é fácil encontrar outra mensagem com o mesmo checksum:

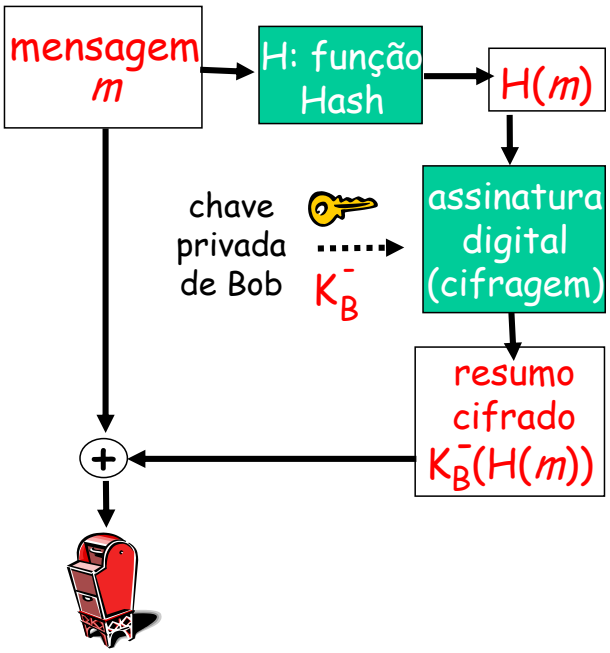
mensagem	formato ASCII
I O U 1	49 4F 55 31
0 0 . 9	30 30 2E 39
9 B O B	39 42 4F 42
	B2 C1 D2 AC

mensagem	formato ASCII
I O U 9	49 4F 55 39
0 0 . 1	30 30 2E 31
9 B O B	39 42 4F 42
	B2 C1 D2 AC

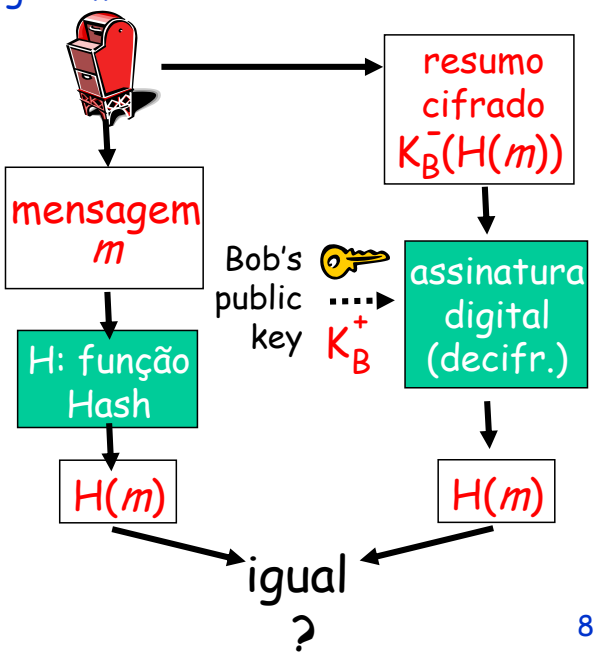
mensagens diferentes com checksum idênticos!

Assinatura digital = resumo da mens. assinado

Bob envia uma mensagem assinada digitalmente:



Alice verifica a assinatura e a integridade da mensagem assinada digitalmente:



Inatel
Instituto Nacional de Telecomunicações
Criptografia e Certificação Digital – Unid. 2

Algoritmos de Funções Hash

MD5 (RFC 1321):

- ✓ Fornece resumos de 128 bits computados em quatro passos.
- ✓ Dada uma seqüência arbitrária de 128 bits x, é difícil construir uma mensagem m cujo hash MD5 seja igual a x.

SHA-1:

- ✓ Padrão nos EUA [NIST, FIPS PUB 180-1].
- ✓ Resumos de 160 bits.

Intermediários Confiáveis

Problema chave simétrica:

Como duas entidades estabelecem uma chave secreta compartilhada pela rede?

Problema chave pública:

Quando Alice obtém a chave pública de Bob (a partir de um *web site*, e-mail, disquete), qual é a garantia que essa é realmente a chave pública de Bob, não a de Trudy?

Solução:

Centro de distribuição de chaves confiável (KDC - Key Distribution Center) atuando como intermediário entre as entidades.

Solução :

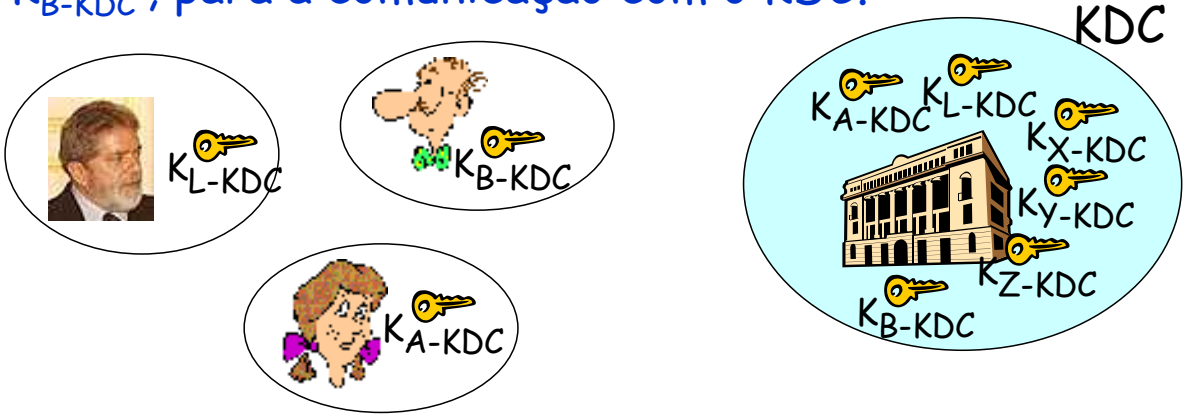
Autoridade de certificação confiável (CA - Certification Authority)

Centro de Distribuição de Chaves (KDC)

Alice e Bob necessitam de uma chave simétrica.

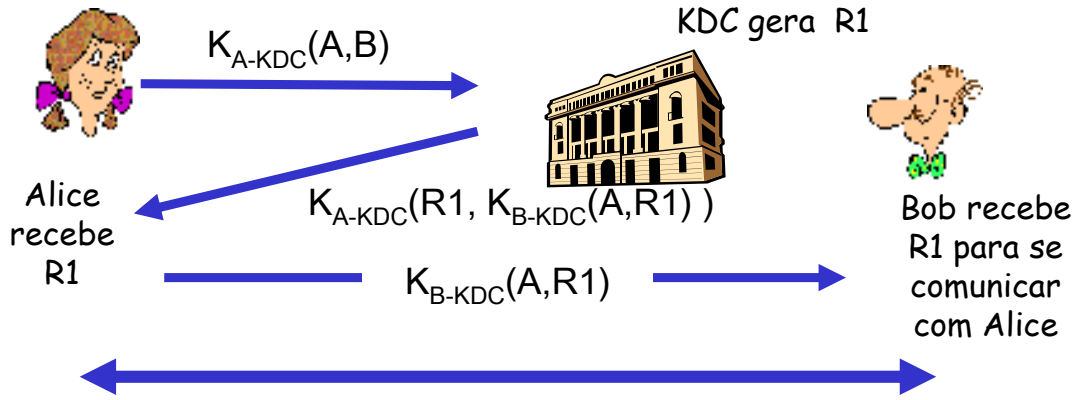
KDC: servidor compartilha diferentes chaves secretas com *cada* usuário registrado (muitos usuários).

Alice e Bob têm chaves simétricas individuais, $K_{A\text{-}KDC}$ e $K_{B\text{-}KDC}$, para a comunicação com o KDC.



Centro de Distribuição de Chaves (KDC)

Como o KDC permite que Bob e Alice estabeleçam uma chave simétrica para que eles se comuniquem com segurança?

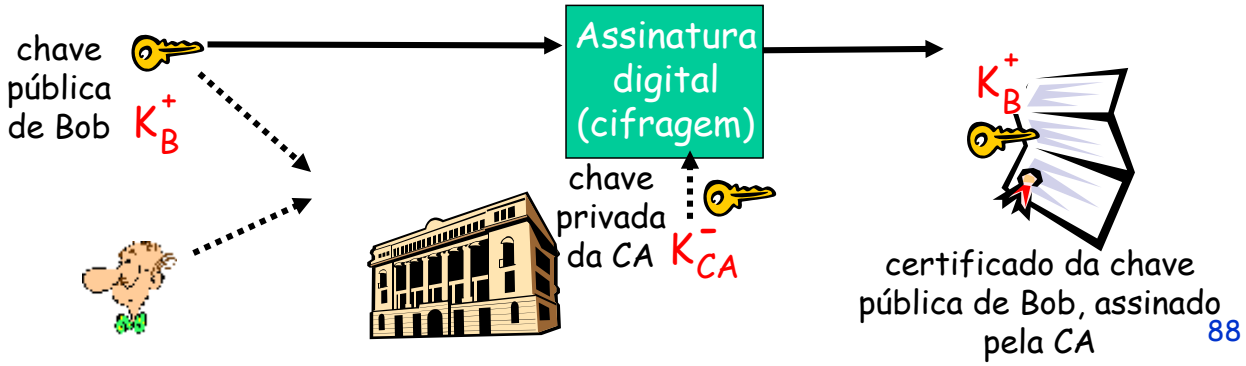


Alice e Bob utilizam R1 como *chave de sessão* compartilhada para a cifragem simétrica dos dados.

Autoridades Certificadoras (CA)

Autoridade certificadora (CA): guarda e certifica a chave pública de uma identidade particular, *E*.

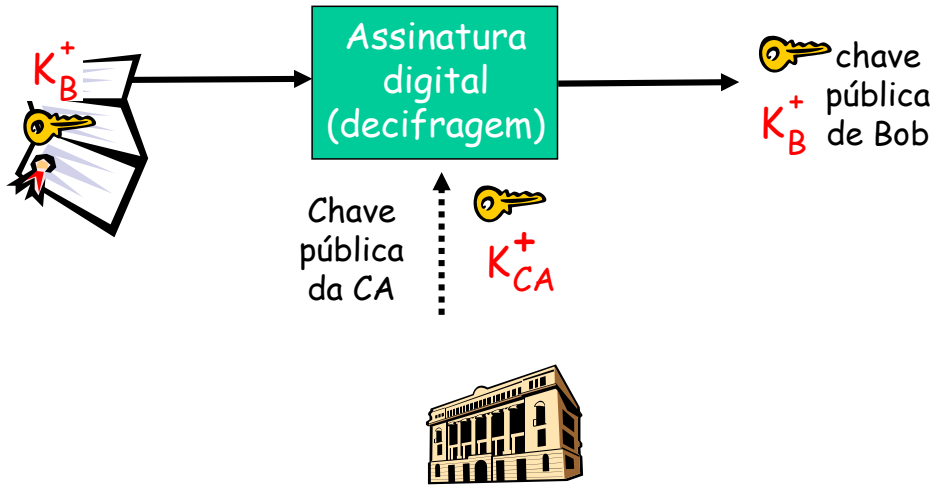
- ✓ Usuário *E* registra sua chave pública junto ao CA.
  - *E* fornece uma "prova de identidade" ao CA.
  - CA cria um certificado digital ligando *E* à sua chave pública.
  - O certificado contém a chave pública de *E* assinada digitalmente pela CA. (CA garante: "esta é a chave pública de *E*").



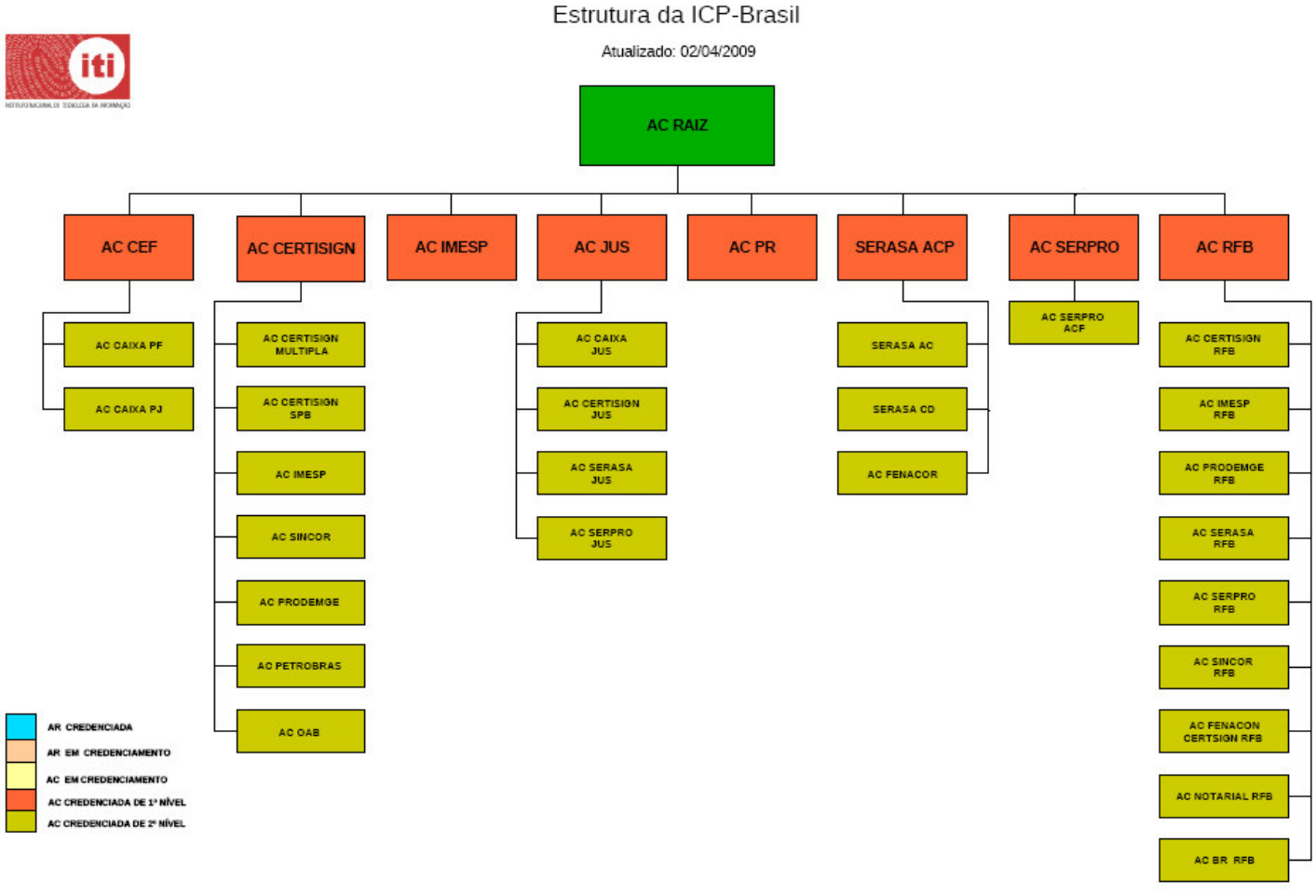
Autoridades Certificadoras (CA)

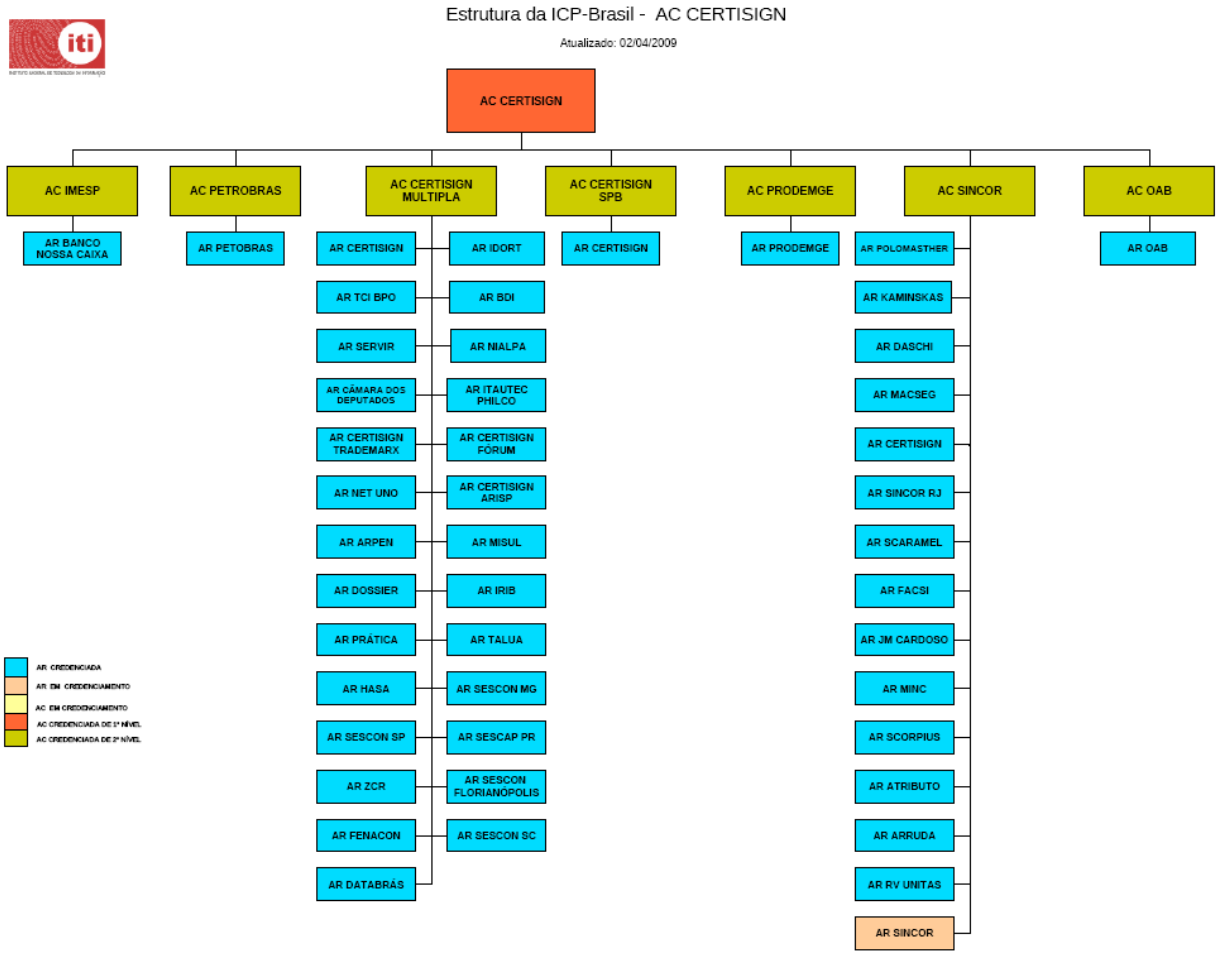
Quando Alice necessita da chave pública de Bob:

- ✓ acessa o certificado digital de Bob,
- ✓ aplica a chave pública da CA sobre o certificado de Bob e obtém a chave pública de Bob.



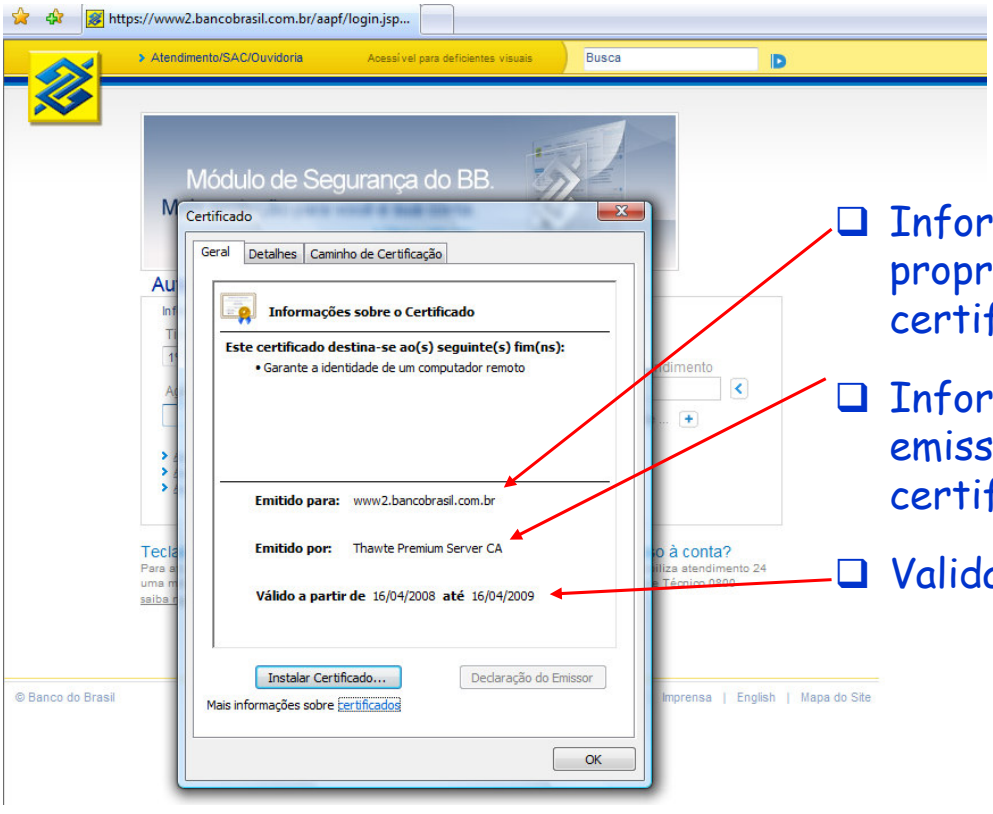
Inatel
Instituto Nacional de Telecomunicações
Criptografia e Certificação Digital – Unid. 2





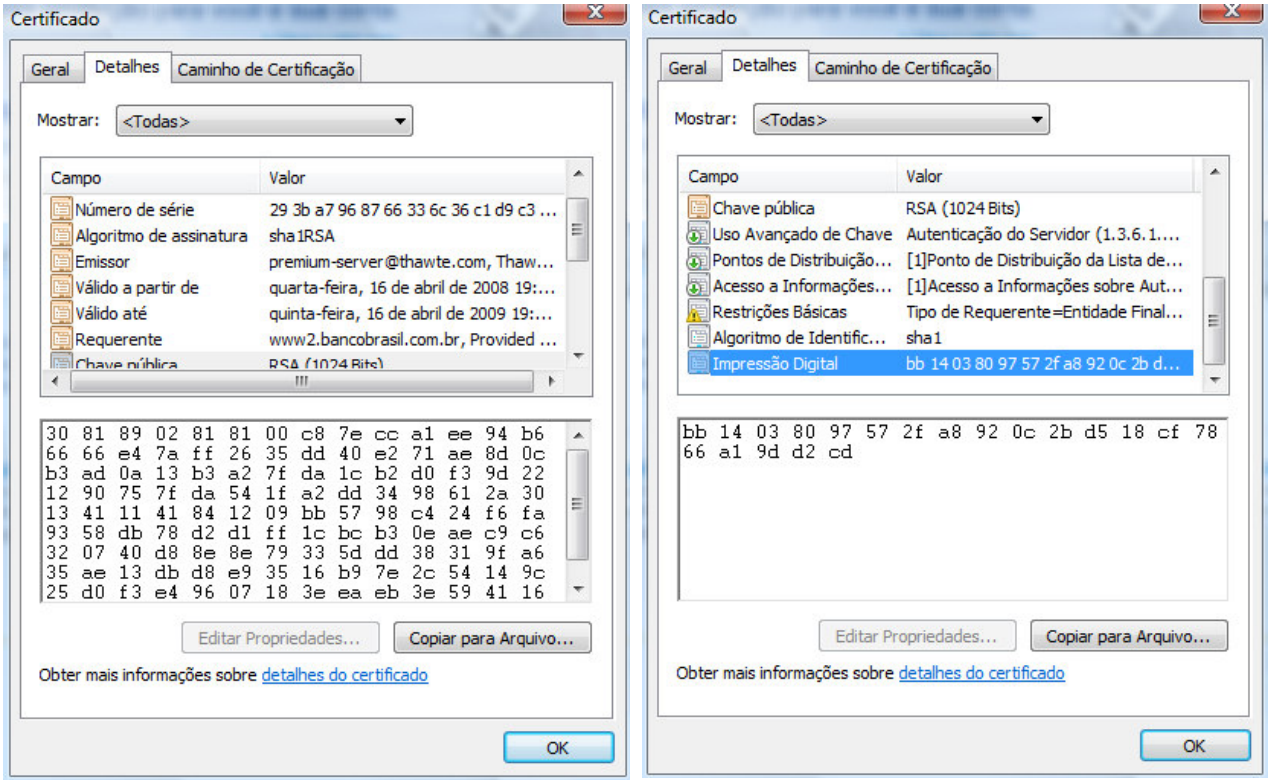
Inatel
Instituto Nacional de Telecomunicações
Criptografia e Certificação Digital – Unid. 2

Um certificado contém:



- Informações do proprietário do certificado
- Informações do emissor do certificado
- Validade

Um certificado contém:



Lista de Exercícios 02: