Criptografia de chave pública sem certificado

Rafael Will Macedo de Araujo
(rwill@ime.usp.br)

DCC – IME – USP

Abril de 2012

CNPq no. 151134/2010-3

Objetivos

- Estudar dois modelos de criptografia de chave pública que não fazem uso de certificados digitais.
- Listar as principais vantagens e desvantagens dos modelos apresentados
- Mostrar algumas aplicações

Roteiro

Criptografia de Chave Pública Convencional

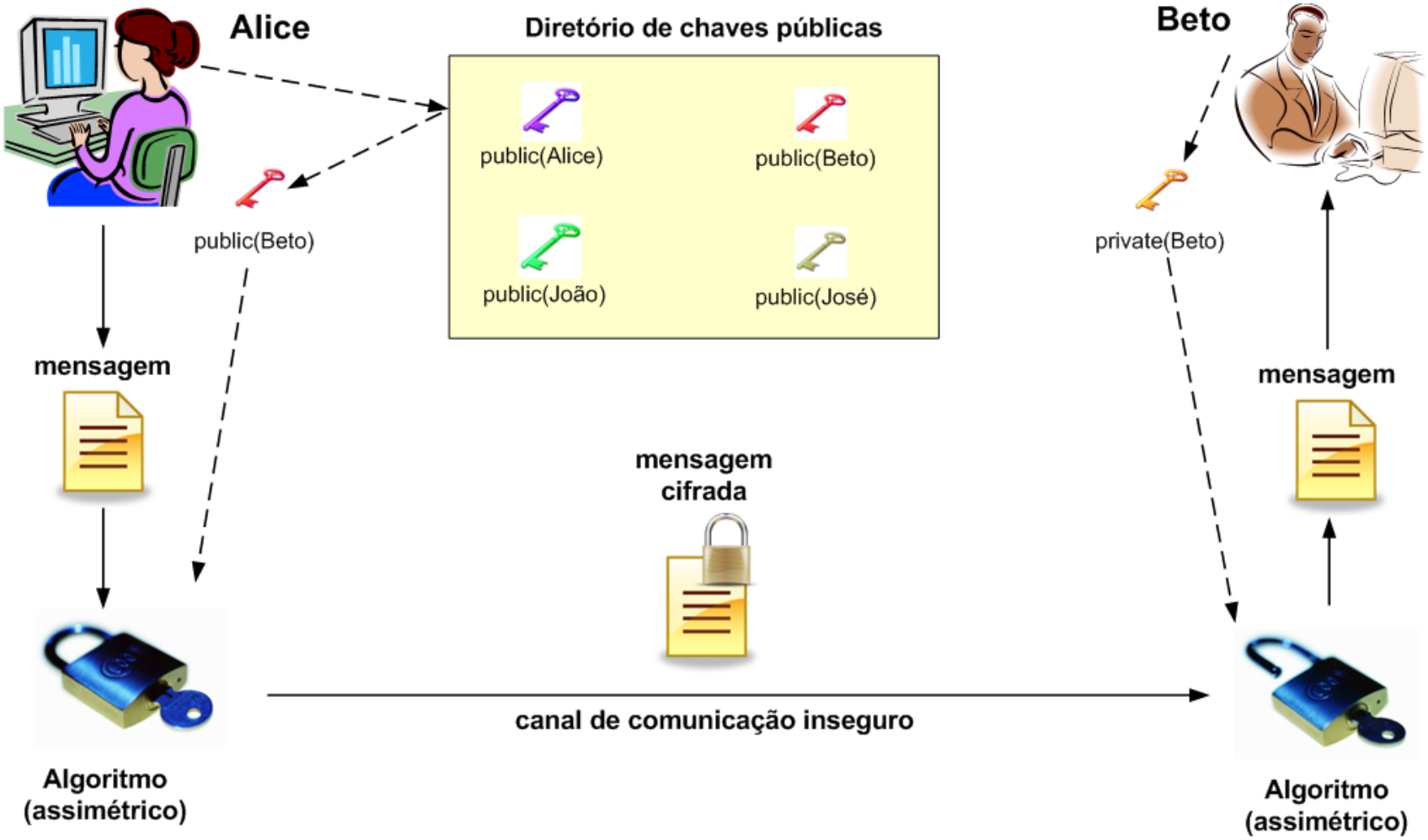

Figura: Criptografia de chave pública

Criptografia de Chave Pública Convencional

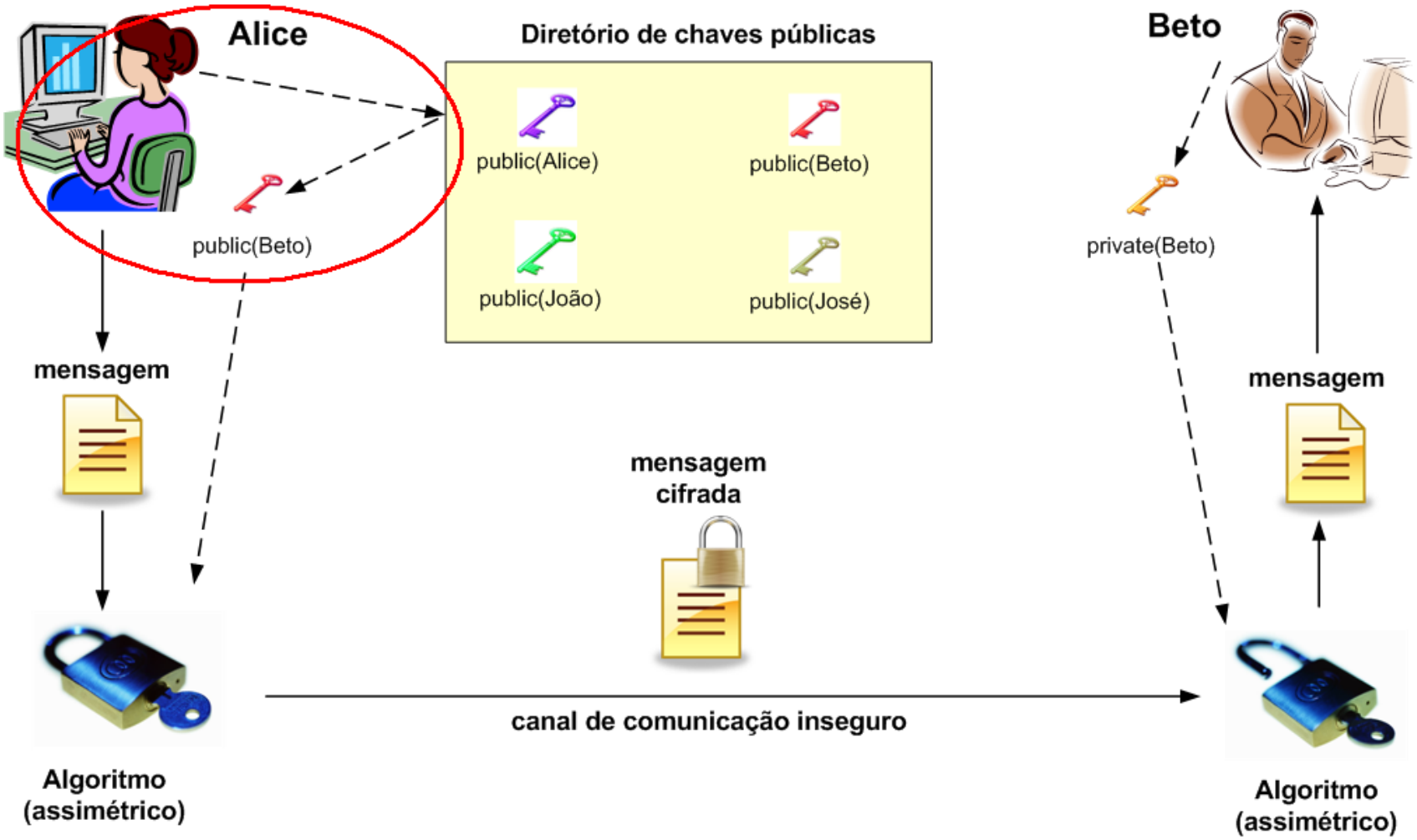

Figura: Criptografia de chave pública

Personificação

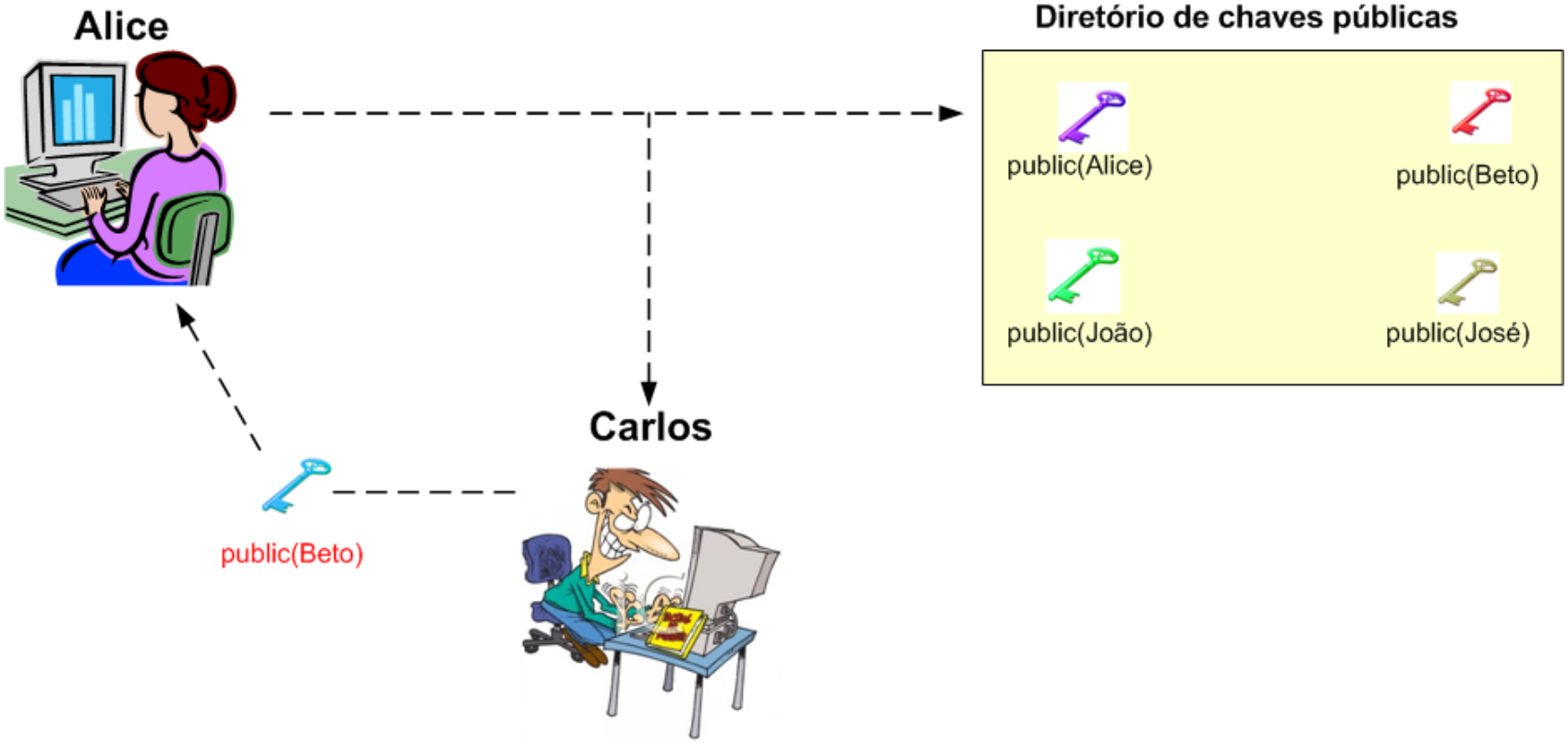

Figura: Carlos tenta se passar por Beto perante Alice

Ataque *Man-in-the-Middle*

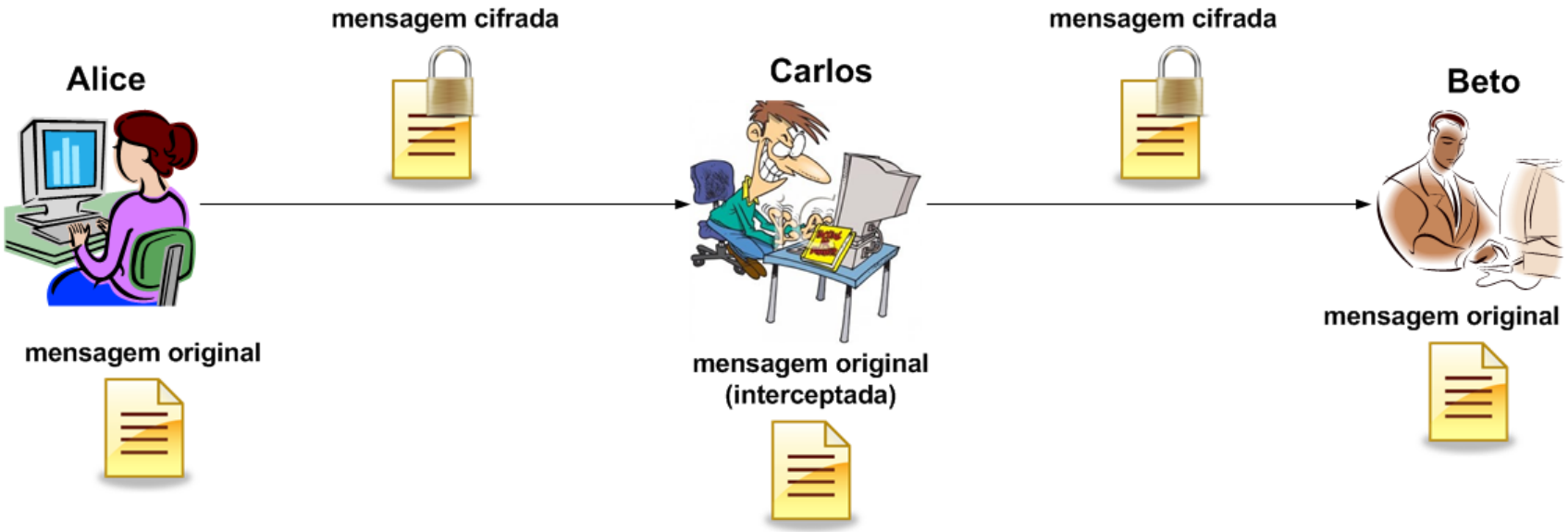

Figura: Ataque *man-in-the-middle*

Certificado Digital

- Necessidade de um documento que legitimasse as chaves públicas.
- Tais documentos deveriam ser emitidos por uma autoridade idônea, após verificação de propriedade das chaves públicas.
- De tempos em tempos seria necessário comprovar a propriedade das chaves públicas.
- Surgimento dos certificados digitais e das autoridades certificadoras.

Certificado Digital

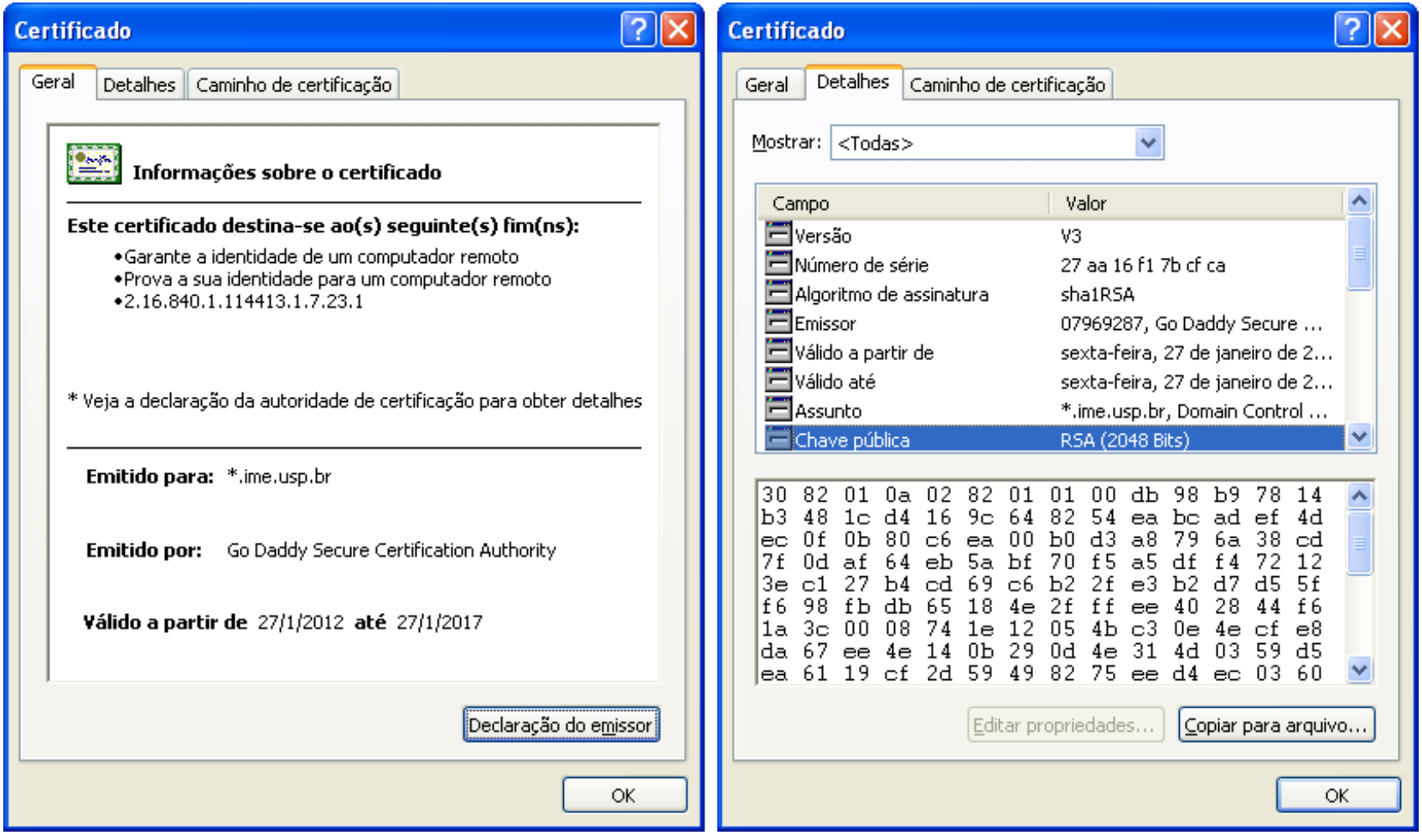

Figura: Certificado digital (padrão X.509)

Como funciona...

Suponha que *Beto* deseja enviar uma mensagem para *Alice*:

1. *Beto* obtém o certificado digital de *Alice*.
2. *Beto* verifica a validade do certificado e sua assinatura.
   - Pode envolver consulta a uma lista de certificados revogados.
3. Se o certificado não esta revogado, *Beto* extrai a chave pública de *Alice*.
4. *Beto* cifra a mensagem utilizando a chave pública de *Alice* e a envia.

Modelo de Certificação

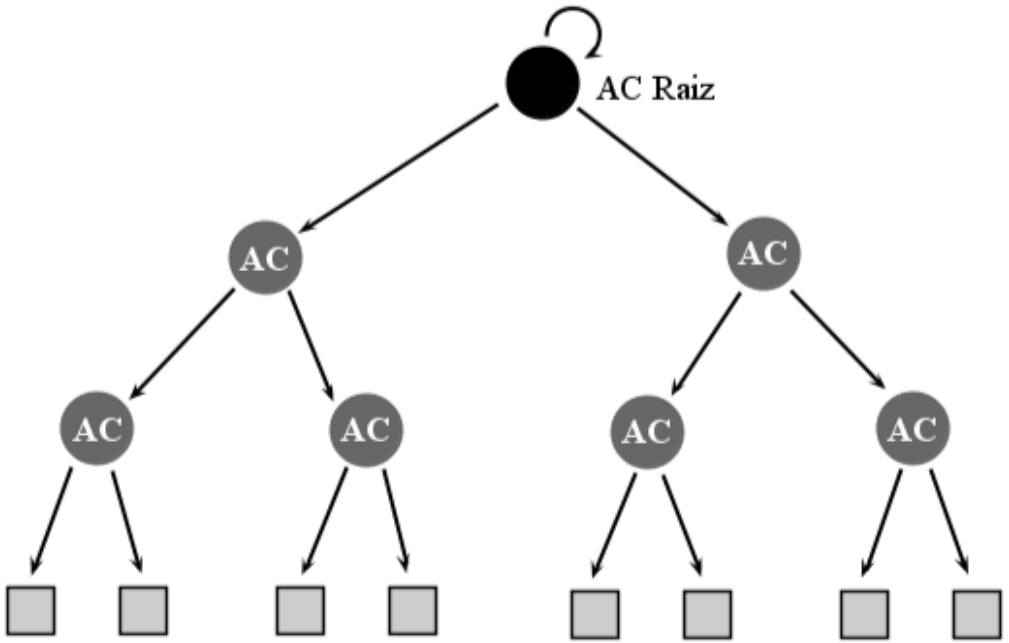

Figura: Modelo de certificação em árvore

Desafios da Criptografia de Chave Pública Convencional

- Obrigatoriedade de legitimar chaves públicas através de certificados digitais.
- Dificuldade de revogar certificados digitais.
- Complexidade de implantação e manutenção da ICP.
- Custo do processo de recuperação e validação de certificados.

Curvas Elípticas sobre Corpos Finitos

- Seja $\mathbb{F}_q$ um corpo finito de ordem q, onde $q > 3$ é um número primo.
  - Como q é primo, então $\mathbb{F}_q$ coincide com $\mathbb{Z}_q$.
- Uma curva elíptica E sobre um corpo $\mathbb{F}_q$, representada por $E(\mathbb{F}_q)$ ou $E/\mathbb{F}_q$, é o conjunto dos pares $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ que satisfazem a equação:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

onde $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_q$, com $\Delta \neq 0$.

Curvas Elípticas sobre Corpos Finitos

- Δ é o discriminante de $E/(\mathbb{F}_q)$, e é definido como:

$$\begin{cases} \Delta = -d_2^2 d_8 - 8d_4^3 - 27d_6^2 + 9d_2 d_4 d_6 \\ d_2 = a_1^2 + 4a_2 \\ d_4 = 2a_4 + a_1 a_3 \\ d_6 = a_3^2 + 4a_6 \\ d_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \end{cases}$$

- O discriminante $\Delta \neq 0$ garante que não existirão duas ou mais retas tangentes distintas para um ponto na curva.
- Existe um ponto $\mathcal{O}$, dito ponto no infinito.

Soma de pontos em Curvas Elípticas

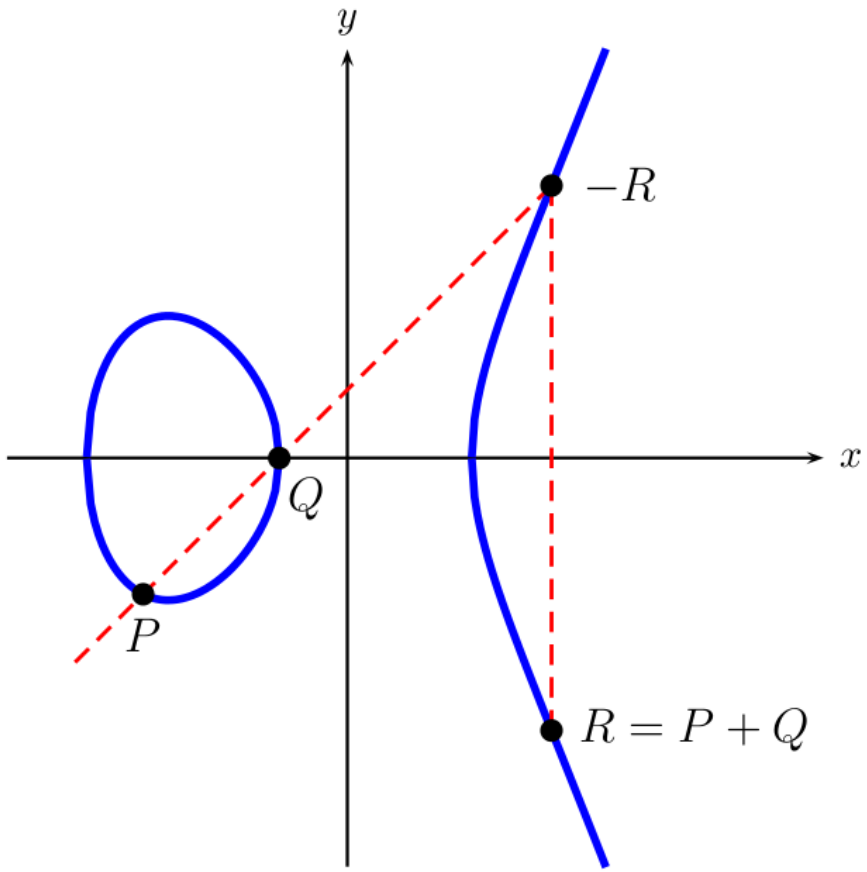

Figura: Soma de dois pontos P e Q em uma curva elíptica

Dobro de um ponto em Curvas Elípticas

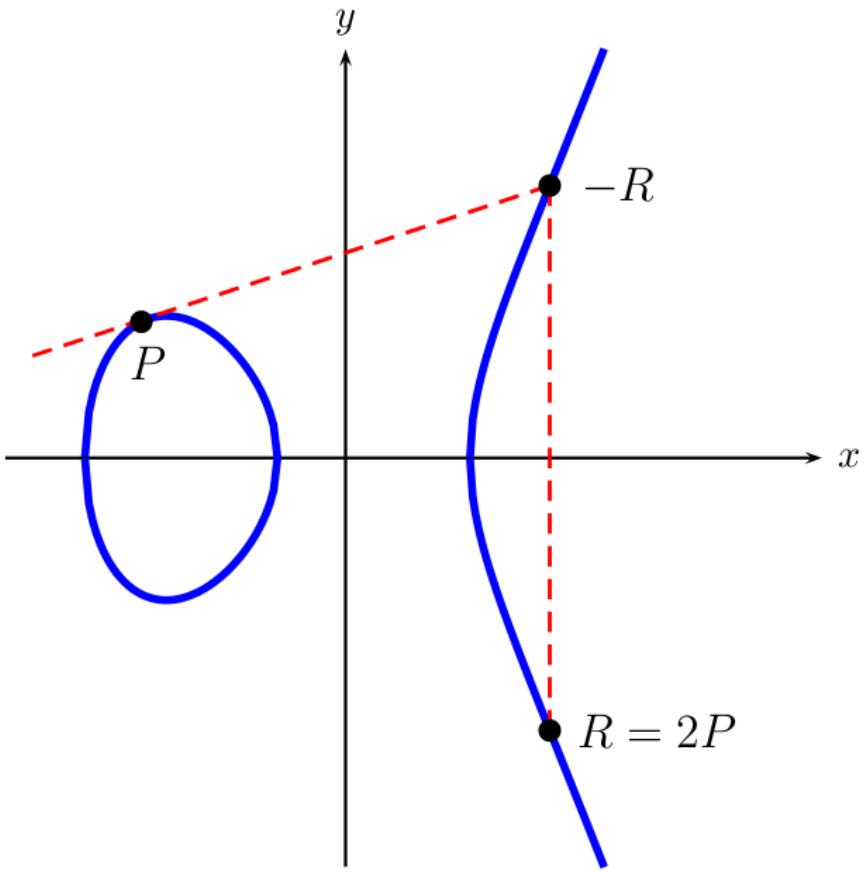

Figura: Dobrando um ponto P em uma curva elíptica

Problema do logaritmo discreto (PLD)

PLD nos Inteiros

- Sejam:
  - G: grupo cíclico finito (por exemplo $\mathbb{Z}_p^*$)
  - g: gerador de G
  - p: número primo (grande)
- Dados p, g e (g^s mod p), encontrar s.

Problema do logaritmo discreto (PLD)

PLD em curvas elípticas

- Dados dois pontos P e R de uma curva elíptica definida sobre um corpo finito, onde P é um ponto gerador, achar um inteiro s tal que:
  - $R = sP$

Note que podemos interpretar sP como: $\underbrace{P + P + \cdots + P}_{s \text{ vezes}}$.

Emparelhamento Bilinear

Definição

- Mapeamento entre dois grupos: $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$.

Propriedades

- **Bilinear**: Para quaisquer $P, Q, R \in \mathbb{G}_1$ ou $\mathbb{G}_2$, e $a, b \in \mathbb{Z}_q$ tem-se:
  - $e(P + Q, R) = e(P, R).e(Q, R)$.
  - $e(P, Q + R) = e(P, Q).e(P, R)$.
  - $e(aQ, bQ) = e(Q, Q)^{ab} = e(abQ, Q) = e(Q, abQ)$.
- **Não-degenerado**: um emparelhamento é dito não-degenerado se não mapeia todos os pares $\mathbb{G}_1 \times \mathbb{G}_2$ para o elemento identidade de $\mathbb{G}_T$.
- **Ser computável**: $\forall(P, Q), \exists R \rightarrow R \equiv e(P, Q)$.
  - Isto é, existe algoritmo **eficiente** (i.e., de tempo polinomial) para calcular $e(P, Q)$.

Tipos de Emparelhamentos Bilineares

- No trabalho de [Galbraith *et al*, 2006], são apresentados três tipos de emparelhamentos:
  - **Tipo 1**: $\mathbb{G}_1 = \mathbb{G}_2$, (emparelhamento simétrico).
  - **Tipo 2**: $\mathbb{G}_1 \neq \mathbb{G}_2$, e existe um isomorfismo eficientemente computável: $\phi : \mathbb{G}_2 \rightarrow \mathbb{G}_1$.
  - **Tipo 3**: $\mathbb{G}_1 \neq \mathbb{G}_2$, contudo não existe isomorfismo que seja eficientemente computável entre $\mathbb{G}_1$ e $\mathbb{G}_2$.

Segurança

Decision Diffie-Hellman Problem (DDHP)

- Sejam:
  - $a, b, c, n \in \mathbb{Z}_q$.
  - $P \in \mathbb{G}$.
- Dados: $P, aP, bP, cP \subset \mathbb{G}$, decidir se: $c = ab \bmod n$.

Computacional Diffie-Hellman Problem (CDHP)

- Sejam:
  - $a, b \in \mathbb{Z}_q$.
  - $P \in \mathbb{G}$.
- Dados: $P, aP, bP \subset \mathbb{G}$, calcular: abP.

Segurança

Gap Diffie-Hellman Problem (GDHP)

- Seja $\mathbb{G}$ um grupo onde o DDHP é tratável.
- O **Problema Diffie-Hellman Lacunar** consiste em resolver o **CDHP** em $\mathbb{G}$, dado que o **DDHP** é tratável em $\mathbb{G}$.

Bilinear Diffie-Hellman Problem (BDHP)

- Variação do CDHP.
- Dados: $P, aP, bP, cP \subset \mathbb{G}$, calcular: $e(P,P)^{abc}$.

Observação

- Se o **GDHP** é fácil, então o **BDHP** também é fácil.
  - Se é possível calcular abP (pois o CDHP é fácil), então podemos calcular $e(abP, cP) = e(P,P)^{abc}$ também.

Roteiro

Criptografia de Chave Pública Baseada em Identidade

- Modelo proposto em 1984 por A. Shamir.
  - Shamir propõe um esquema de assinatura, cuja segurança se baseava na dificuldade de fatoração de números primos.
- A chave pública deixa de ser um valor gerado aleatoriamente, e passa ser a própria **identidade do usuário**.
  - Exemplos: *nome, e-mail, CPF, n° de telefone, endereço IP.*
- Características semelhantes com as de um correio físico:
  - Sabendo-se o endereço de uma pessoa, é possível enviar uma mensagem de modo que somente ela poderá ler.
- Na época, um esquema de criptografia baseado em identidades continuou sendo um problema em aberto.

Criptografia de Chave Pública Baseada em Identidade

- Somente no ano 2001 foram publicados esquemas de criptografia (*encryption*) no modelo baseado em identidades.
  - D. Boneh e M. Franklin propuseram uma solução baseada em emparelhamentos bilineares sobre curvas elípticas.
  - C. Cocks propôs uma solução baseada em resíduos quadráticos.
- Atualmente, a grande maioria dos esquemas de criptografia baseados em identidade fazem uso de emparelhamentos bilineares sobre curvas elípticas.

Gerador de Chaves Privadas

- O modelo baseado em identidade pressupõe a existência de um **Gerador de Chaves Privadas** (PKG - *Private Key Generator*).
- Trata-se de uma **Autoridade de Confiança**, responsável por:
  - Gerar e guardar a chave-mestra secreta do sistema.
  - Calcular as chaves secretas de todos os usuários.
  - Entregar as chaves secretas dos usuários de forma segura (com sigilo e autenticidade).

Atributos do modelo

Geração de chaves do PKG

- P, um ponto gerador de $E(\mathbb{F}_{q^k})$, de conhecimento público.
- $s \in \mathbb{F}_q^*$, que é chave-mestra secreta do PKG.
- $R_{TA} = sP$, chave pública do PKG.
- Par de chaves: (R_{TA}, s).

Geração de chaves do usuário

- Seja ID_A um identificador da usuária *Alice*.
  - $Q_A = f(ID_A)$, chave pública de *Alice*.
  - $S_A = sQ_A$, chave secreta de *Alice*, calculada pelo PKG e enviada para *Alice* através de um canal seguro.
- Par de chaves de Alice: (ID_A, S_A).

Diagrama do Modelo Baseado em Identidade

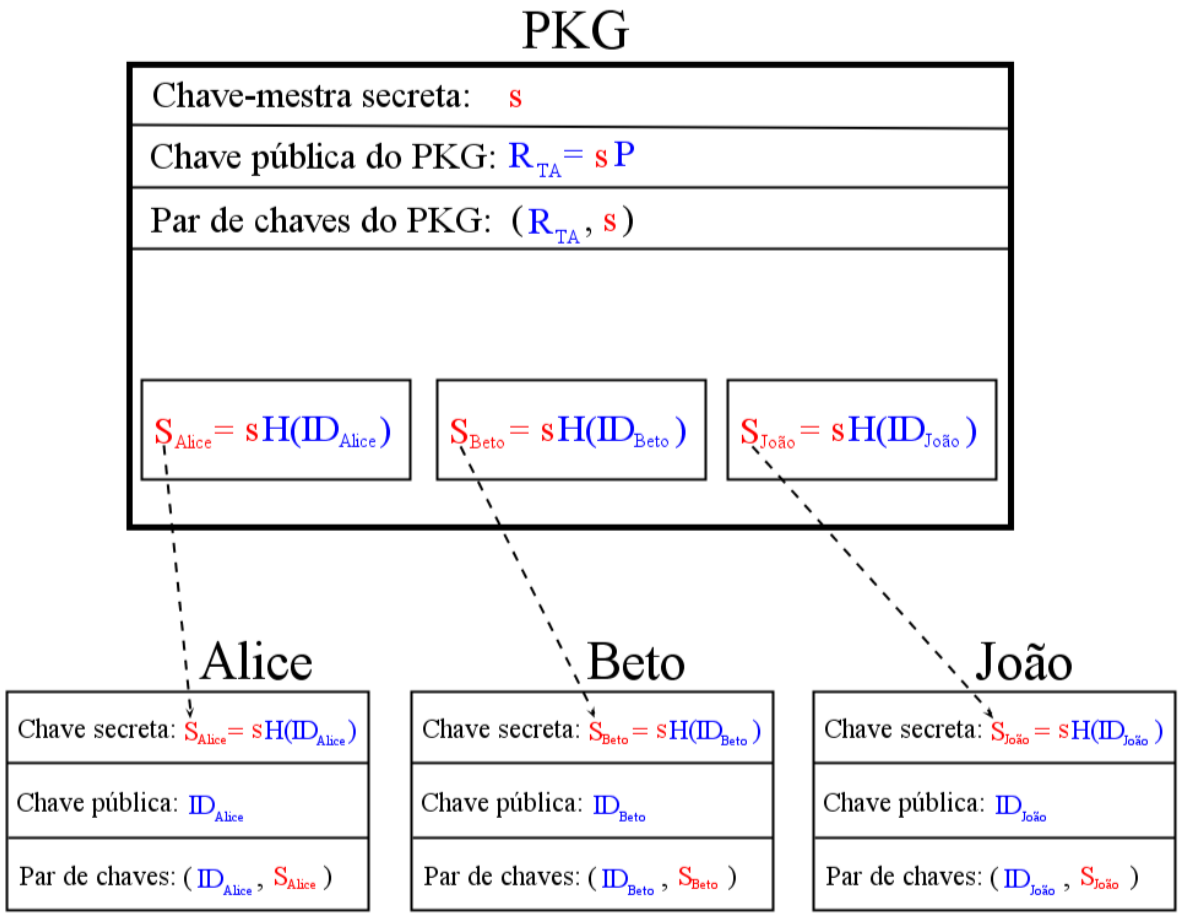

Figura: Distribuição das chaves privadas no modelo baseado em identidade

Vantagens do Modelo Baseado em Identidade

- Chave pública memorizável por humanos.
- Possibilidade de utilizar a chave pública de um usuário que ainda não possua chave secreta.
- Não há necessidade de diretórios de chaves públicas.
- Não há necessidade de certificados digitais (certificação implícita).
- Não há necessidade de Infraestrutura de chave pública.

Desvantagens do Modelo Baseado em Identidade

- Custódia de chaves.
  - Em alguns ambientes pode ser desejável.
- Necessidade de um canal seguro e autenticado para distribuição das chaves secretas.
- Alto grau de criticidade da chave-mestra secreta.
- Não há irretratabilidade, pois o PKG pode personificar qualquer usuário, se quiser.

Modelo Baseado em Identidade - Conclusões

- Modelo ideal para grupos fechados.
- Nível 1 de segurança, na classificação de [Girault, 1991].
  - Departamento de uma empresa, rede de lojas, etc.
- Podem ser criadas chaves públicas com período de validade (revogação de chave pública).
  - Exemplos:
    alice@provedor.com-2012
    alice@provedor.com-abril2012
    alice@provedor.com-11/04/2012

Roteiro

Criptografia de Chave Pública sem Certificado

- Modelo proposto em 2003 por S. Al-Riyami e K. Paterson.
  - Combina as ideias do modelo baseado em identidades com o modelo de chave auto-certificada (proposto por Girault em 1991).
- Um dos principais objetivos era eliminar a propriedade de custódia de chaves, inerente ao modelo baseado em identidade.
- Trata-se de um modelo intermediário entre o baseado em identidade e a ICP.

Centro de Geração de Chaves

- Como no modelo baseado em identidade, o modelo sem certificado pressupõe a existência de uma Autoridade de Confiança, chamada de KGC (*Key Generation Center*).
- O KGC é responsável por:
  - Gerar e guardar a chave-mestra secreta do sistema.
  - Calcular as chaves secretas parciais de todos os usuários.
  - Entregar as chaves secretas parciais dos usuários de forma segura (com autenticidade).

Geração e Manipulação de Chaves

- O KGC calcula parte da chave privada do usuário. Cabe ao usuário calcular a outra parte de sua chave secreta.
  - Estando em posse das duas "partes" da chave secreta, o usuário pode então calcular sua chave secreta completa.
  - Apenas o usuário terá acesso a sua chave secreta completa.
- A identidade do usuário passa ser parte da chave pública. A outra parte da chave pública é calculada como uma função de sua chave secreta.

Cifragem e Verificação de Assinatura

- Para que *Beto* possa cifrar uma mensagem ou verificar a assinatura de *Alice*, é necessário:
  - A chave pública de *Alice*.
  - A identidade de *Alice*.

Decifração e Assinatura

- Para que *Alice* possa decifrar uma mensagem ou assinar uma mensagem para *Beto*, é necessário:
  - A chave secreta completa de *Alice*.
  - A identidade de *Alice*.

Atributos do modelo

Geração de chaves do KGC

- P, um ponto gerador de $E(\mathbb{F}_{q^k})$, de conhecimento público.
- $s \in \mathbb{F}_q^*$, que é chave-mestra secreta do KGC.
- $R_{TA} = sP$, chave pública do KGC.
- Par de chaves: (R_{TA}, s).

Geração de chaves do usuário

- Seja ID_A um identificador da usuária *Alice*.
  - $Q_A = f(ID_A)$, parte da chave pública de *Alice*.
  - $D_A = sQ_A$, chave secreta parcial de *Alice*, calculada pelo KGC.
  - $x_A \in \mathbb{F}_q^*$, valor secreto de *Alice*, calculado por ela.
  - $S_A = x_A D_A = x_A s Q_A$, chave secreta completa de *Alice*, calculada por ela.
  - $P_A = x_A P$, parte da chave pública de *Alice*, em função de sua chave secreta parcial.
- Par de chaves de Alice: $([ID_A, P_A], S_A)$.

Diagrama do Modelo sem Certificado

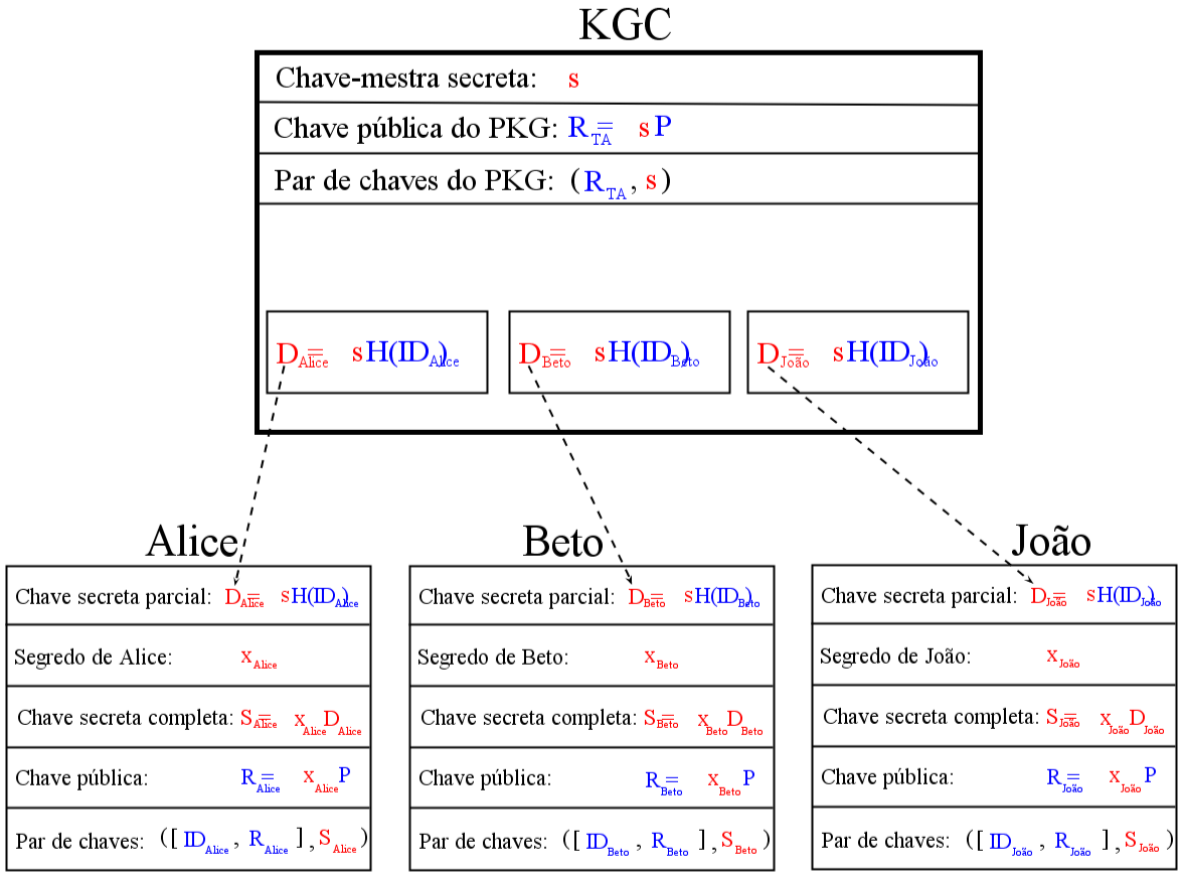

Figura: Distribuição das chaves privadas parciais no modelo sem certificado

Vantagens do Modelo sem Certificado

- Eliminação da custódia de chaves.
- Menor criticidade da chave-mestra secreta.
  - Seu comprometimento afeta apenas as chaves secretas parciais.
- Controle do usuário sobre renovação de chaves (independe de comunicação com o KGC).
- A chave pública pode ser criada e utilizada antes do KGC entregar a chave secreta parcial para o usuário.
- Não há necessidade de certificados digitais (certificação implícita).

Desvantagens do Modelo sem Certificado

- Requer um repositório ou alguma outra forma de distribuição de chaves públicas.
- Possibilidade de substituição da chave pública por algum mal intencionado.
  - Quem utiliza a chave pública não tem como verificar sua legitimidade.
- Vulnerável ao ataque DoD (*Denial of Decryption*).
  - A substituição de uma chave pública impede que a mensagem seja decifrada.

Modelo sem Certificado - Conclusões

- Modelo ideal para grupos fechados.
- Nível 2 de segurança, na classificação de [Girault, 1991].

Roteiro

Comprimento de chaves secretas

ECC (bits)	RSA (bits)	Razão de crescimento	AES (bits)
160	1024	$\approx 1 : 6$	80
256	3072	$1 : 12$	128
384	7680	$1 : 20$	192
512	15360	$1 : 30$	256

- Interesse de aplicação dos modelos estudados à ambientes com dispositivos de poder computacional restrito.
  - Menor complexidade de implantação dos dois modelos.
  - Chaves de menor tamanho para um mesmo nível de segurança.

Protocolos de Acordo de Chave

- Protocolos em que dois participantes podem combinar uma chave secreta utilizando um canal público.
- Acordo de chaves com autenticação dos participantes.
- Modelos de segurança.
  - Contra adversário forte, moderado e fraco.
- Artigos que comparam vários protocolos dentro da classe dos protocolos de acordo de chave: [Chen *et al*, 2007] e [Swanson & Jao, 2009].

Ponto de Partida

- Projeto Borboleta (Fapesp).
  - Um dispositivo móvel (PDA) deseja se comunicar com um servidor de banco de dados de forma segura.
  - Implementação dos protocolos GOT (Goya-Okida-Terada) e LBG (Lippold-Boyd-González Nieto) por [Okida, 2011].
- Comparar o cenário existente no projeto Borboleta caso fossem utilizados outros protocolos de acordo de chave.
- Utilização da biblioteca **Relic Toolkit**, em linguagem C.
  - Suporte para cuvas elípticas.
  - Suporte para emparelhamentos bilineares.
  - Crescente uso pela comunidade acadêmica.
  - Documentação via *doxygen*, e frequente correção de *bugs*.

Atividades e cronograma

1. Estudo de modelos de criptografia sem certificado.
2. Escrita do texto de qualificação.
3. Estudo de protocolos de acordo de chave baseados em identidade e sem certificado.
4. Implementação dos protocolos estudados.
5. Elaboração da dissertação final.
6. Defesa da dissertação final.

2012												
Ativ.	1	2	3	4	5	6	7	8	9	10	11	12
1	x	x	x									
2	x	x	x	x								
3				x	x	x	x	x				
4						x	x	x	x			
5							x	x	x	x	x	
6												x

Referências Bibliográficas

- AL-RIYAMI. S, PATERSON. K. **Public Key Cryptography**. ASIACRYPT 2003.
- BONEH. D, FRANKLIN. M. **Identity based encryption from the Weil pairing**. Proceedings of CRYPTO 2001.
- CHEN. L. , CHENG, Z., SMART. N. P. **Identity-based key agreement protocols from pairings**. 2007.
- COCKS. C. **An Identity Based Encryption Scheme Based on Quadratic Residues**. 2001.
- GIRAULT, Marc. **Self-certified public keys**. EuroCrypt 1991.
- GALBRAITH. S., PATERSON. K., SMART. N. **Pairings for Cryptographers**. 2006

Referências Bibliográficas

- OKIDA, C. **Protocolos de acordo de chaves baseados em emparelhamentos para dispositivos móveis**. Dissertação de mestrado. Universidade de São Paulo, 2011.
- SWANSON, C., JAO, D. **A study of two-party certificateless authenticated key-agreement protocols**. INDOCRYPT 2009.
- SHAMIR. A. **Identity based cryptosystems and signature schemes**. Proceedings of CRYPTO 84.
- TERADA. Routo. **Segurança de Dados**. Editora Blucher. São Paulo, Brasil. 2008.

Perguntas?

Obrigado!