Criptografia baseada em Identidades Pessoais

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

DCC – IME – USP

Outubro de 2011

CNPq no. 151134/2010-3

Objetivos

- Definir o que é criptografia baseada em identidades pessoais
  - Quais as vantagens?
  - Quais as desvantagens?

Objetivos

- Definir o que é criptografia baseada em identidades pessoais
  - Quais as vantagens?
  - Quais as desvantagens?
- Como é possível implementar protocolos baseados em identidades?

Objetivos

- Definir o que é criptografia baseada em identidades pessoais
  - Quais as vantagens?
  - Quais as desvantagens?
- Como é possível implementar protocolos baseados em identidades?
  - Em que se baseia sua segurança?

Objetivos

- Definir o que é criptografia baseada em identidades pessoais
  - Quais as vantagens?
  - Quais as desvantagens?
- Como é possível implementar protocolos baseados em identidades?
  - Em que se baseia sua segurança?
- Mostrar exemplos de protocolos
  - Acordo de chaves, encriptação, assinatura...

Roteiro

Criptografia Simétrica

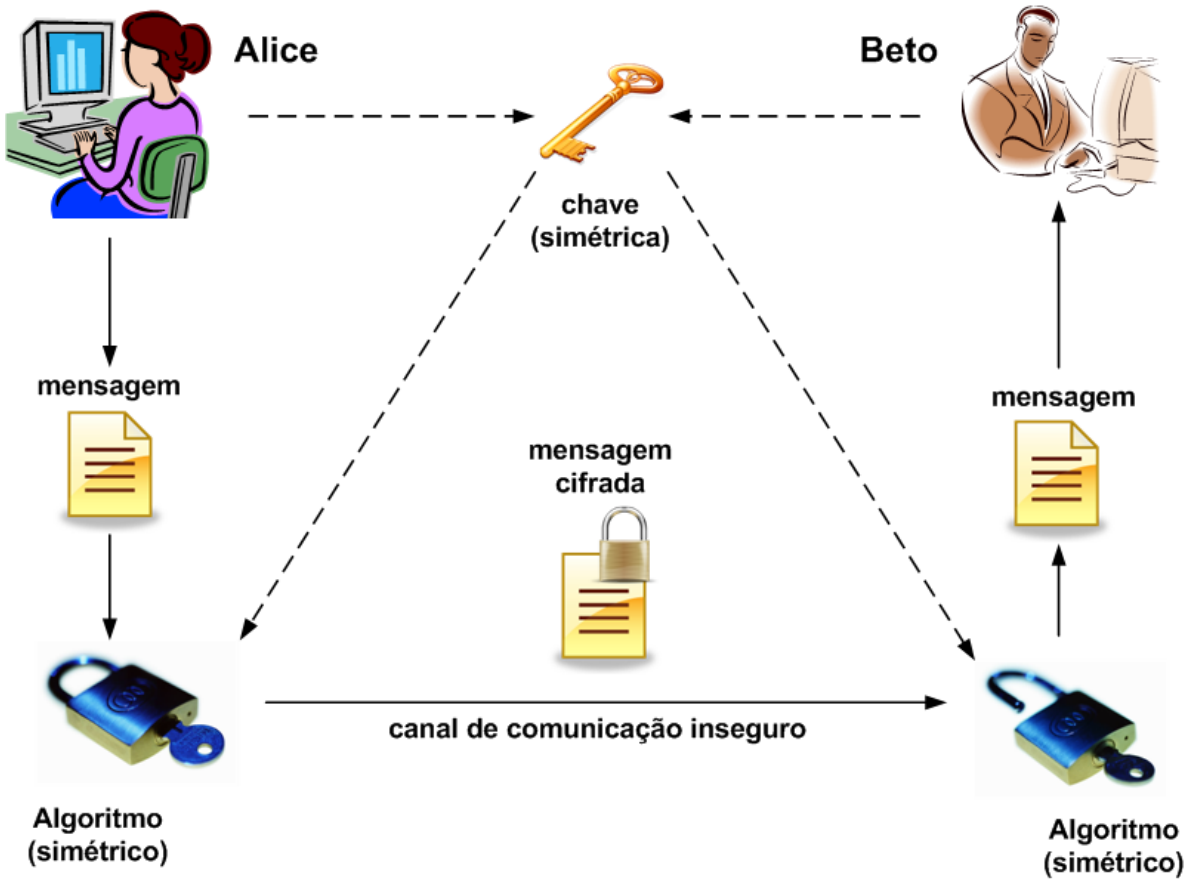


Figura: Modelo de criptografia simétrica

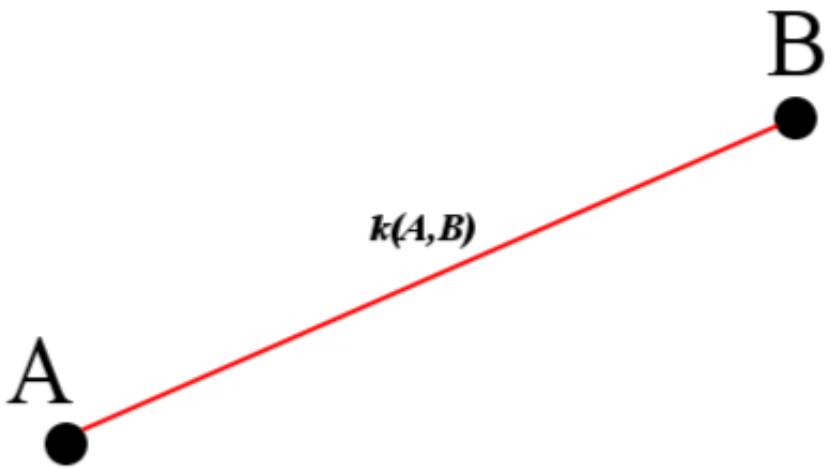
Criptografia simétrica

Alguns problemas da criptografia simétrica

- Problema de distribuição de chaves secretas.
  - Como Alice e Beto podem se comunicar de forma segura sem a necessidade de um encontro para combinar a chave secreta?
- Quantidade de chaves secretas necessárias para n usuários se comunicarem de forma segura cresce de forma quadrática.
  - São necessárias $\frac{n(n-1)}{2}$ chaves secretas.

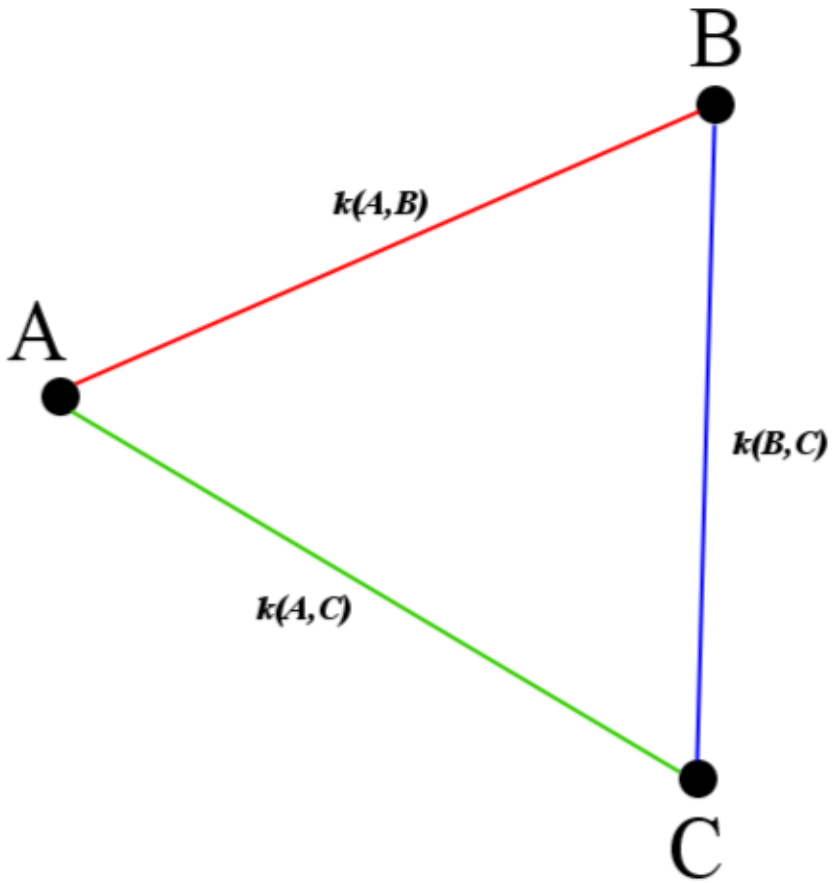
Criptografia simétrica

- Para $n = 2$ participantes, é necessário 1 chave secreta.



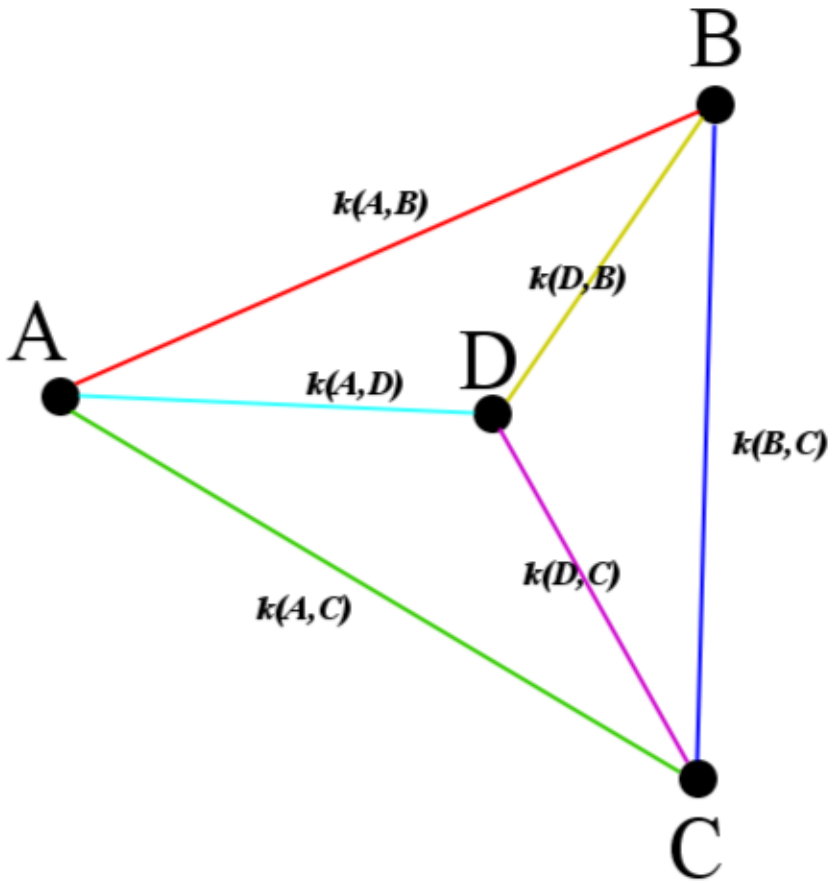
Criptografia simétrica

- Para $n = 3$ participantes, são necessárias 3 chaves secretas.



Criptografia simétrica

- Para $n = 4$ participantes, são necessárias 6 chaves secretas.



Criptografia assimétrica tradicional

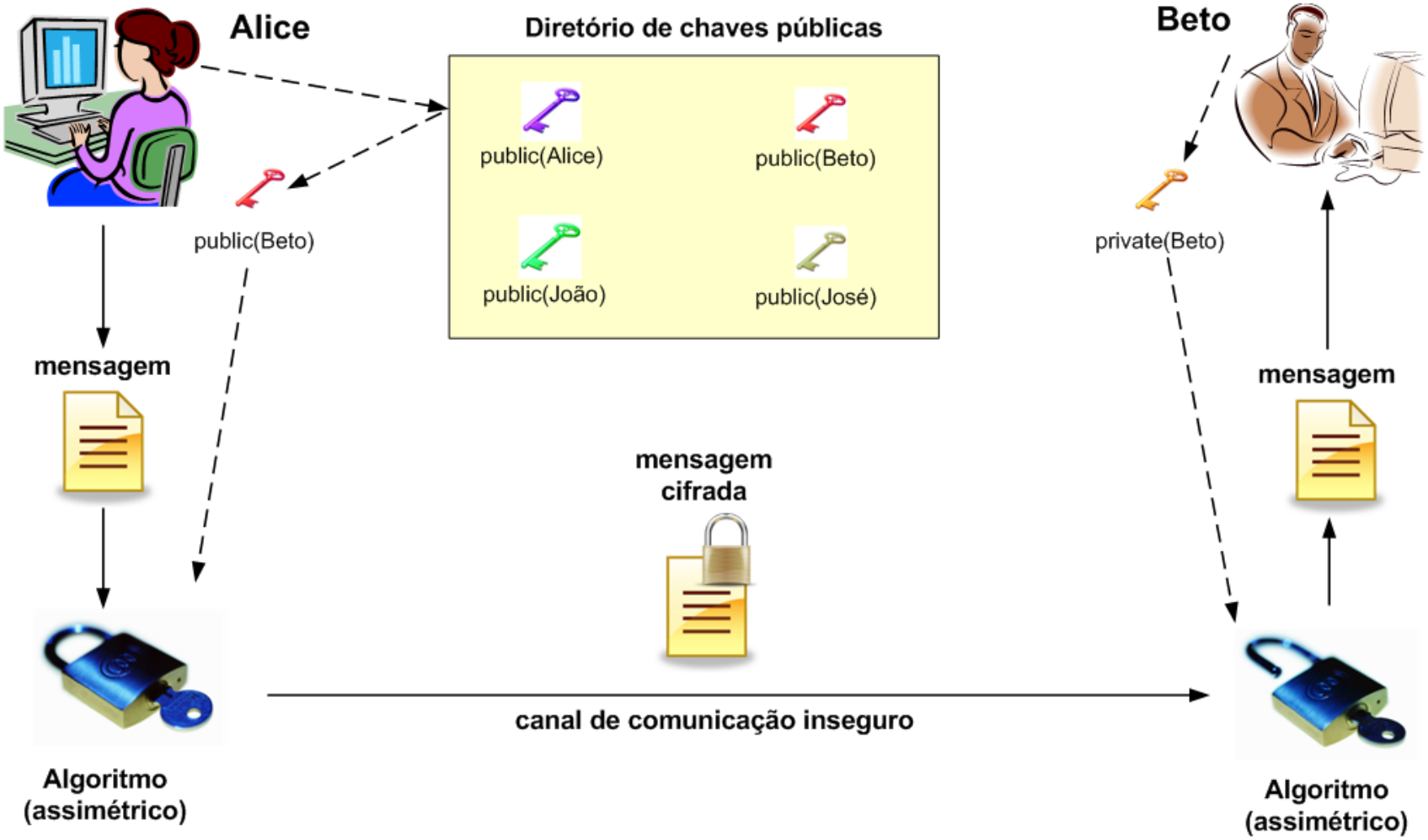


Figura: Modelo de criptografia assimétrica tradicional

Criptografia assimétrica tradicional

Alguns problemas da criptografia assimétrica tradicional

- A chave pública é um número aleatório, e portanto não tem nenhum vínculo com seu dono.
- Tamanho (em bits) das chaves, como no caso do RSA.
- Necessidade de **certificados digitais** para autenticar chaves públicas.

Criptografia baseada em Identidades Pessoais

- O conceito de IBC (*ID-based Cryptography*) foi originalmente proposto por A. Shamir [Shamir 1984].
- Foi concebido para ser um esquema mais simples de obtenção e utilização de chaves públicas.
  - Esquemas tradicionais de infraestrutura de chaves públicas necessitavam de certificados digitais.
- Na época, A. Shamir propôs um esquema de assinatura, cuja segurança se baseava na dificuldade de fatoração de números inteiros (assim como no RSA).
  - O esquema de criptografia baseados em identidades foi considerado um problema em aberto.

Criptografia baseada em Identidades Pessoais

- A idéia é utilizar um **identificador** (único) do usuário A como "chave pública" de A:
  - **Telefone**
  - **E-mail**
  - **CPF**
  - *etc...*
- A chave pública deixa de ser um número aleatório, não sendo mais necessário guardar as chaves públicas das pessoas com quem deseja se comunicar.
- 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.

Curvas Elípticas sobre Corpos Finitos

Sejam:

- $\mathbb{Z}_q$: conjunto de inteiros módulo q.
- $\mathbb{F}_q$: corpo finito de ordem q, onde $q > 3$ é um número primo.
  - Neste caso $\mathbb{Z}_q$ coincide com $\mathbb{F}_q$, pois q é primo.

Curvas Elípticas sobre Corpos Finitos

Sejam:

- $\mathbb{Z}_q$: conjunto de inteiros módulo q.
- $\mathbb{F}_q$: corpo finito de ordem q, onde $q > 3$ é um número primo.
  - Neste caso $\mathbb{Z}_q$ coincide com $\mathbb{F}_q$, pois q é primo.

Definição

- A curva elíptica $y^2 = x^3 + ax + b$ sobre $\mathbb{F}_q$ é o conjunto de soluções $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ para a congruência: $y^2 \equiv x^3 + ax + b \pmod{p}$.

Curvas Elípticas sobre Corpos Finitos

Sejam:

- $\mathbb{Z}_q$: conjunto de inteiros módulo q.
- $\mathbb{F}_q$: corpo finito de ordem q, onde $q > 3$ é um número primo.
  - Neste caso $\mathbb{Z}_q$ coincide com $\mathbb{F}_q$, pois q é primo.

Definição

- A curva elíptica $y^2 = x^3 + ax + b$ sobre $\mathbb{F}_q$ é o conjunto de soluções $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ para a congruência: $y^2 \equiv x^3 + ax + b \pmod{p}$.
- Tem-se que $a, b \in \mathbb{F}_q$ são constantes e que: $4a^3 + 27b^2 \neq 0 \pmod{p}$.
  - Garante que o polinômio $f(x) = x^3 + ax + b$ não tenha raízes múltiplas, sendo possível, assim, traçar uma reta tangente a qualquer ponto da curva.
- Existe um ponto especial $\mathcal{O}$ como elemento identidade, denominado ponto no infinito.

Soma de pontos em Curvas Elípticas

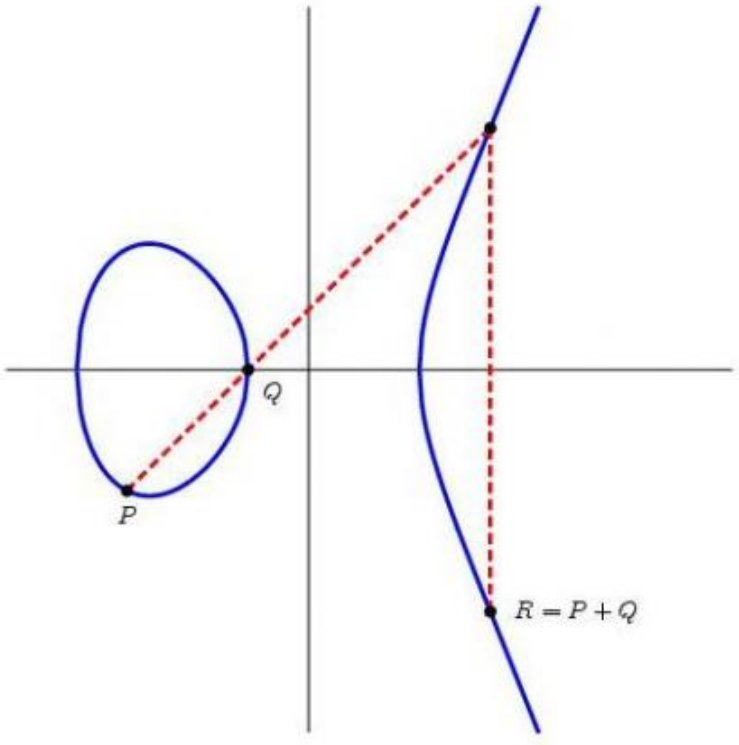


Figura: Soma entre dois pontos P e Q em curvas elípticas

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: $\forall(P, Q)$, tem-se que: $e(P, Q) \neq$ identidade $\mathbb{G}_T$.

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 $e(P, Q)$.

Roteiro

Problema do logaritmo discreto (PLD)

PLD em grupos finitos

- 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)

Um pequeno exemplo

3 é gerador de $\mathbb{Z}_7^*$

s	$3^s \bmod 7$
1	3
2	2
3	6
4	4
5	5
6	1

Parece "fácil" encontrar s para primos pequenos. Mas suponha agora $p \geq 1024$ bits, por exemplo.

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: $\underbrace{P+P+\ldots+P}_{s \text{ vezes}}$.

Segurança em sistemas baseados em identidades

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: $c = ab \bmod n$.

Segurança em sistemas baseados em identidades

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 em sistemas baseados em identidades

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 $\mathbb{G}$.

Segurança em sistemas baseados em identidades

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: $e(P,P)^{abc}$.

Segurança em sistemas baseados em identidades

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.

Funções de espalhamento (*hash*)

Suponha as seguintes funções de *hash*

- H_1: $\{0,1\}^* \rightarrow \mathbb{G}_1$.
- H_2: $\{0,1\}^* \rightarrow \mathbb{F}_q$.
- H_3: $\mathbb{G}_T \rightarrow \{0,1\}^*$.

Geração de Chaves

Par de chaves padrão

- Uma **Autoridade de Confiança** calcula:
  - P, um ponto gerador de $E(\mathbb{F}_{q^k})$, de conhecimento público.
  - $s \in \mathbb{F}_q$, que é o segredo da Autoridade de Confiança.
  - $R_{TA} = sP$.
- Gera o par de chaves: (R_{TA}, s).

Par de chaves baseadas em identidades

- Seja ID um identificador de usuário (exemplo: alice@provedor.com). A autoridade de confiança calcula, para cada usuário:
  - $Q_{ID} = H_1(ID)$.
  - $S_{ID} = sQ_{ID}$.

Roteiro

Acordo de chaves

Acordo de chaves Sakai, Ohgishi, Kasahara

- Proposto em [Sakai *et al* 2000], foi o primeiro esquema de acordo de chaves baseado em identidades.
  - **Alice** calcula:
    $K_{ab} = e(S_{Alice}, Q_{Beto}) = e(sQ_{Alice}, Q_{Beto}) = e(Q_{Alice}, Q_{Beto})^s$.
  - **Beto** calcula:
    $K_{ba} = e(Q_{Alice}, S_{Beto}) = e(Q_{Alice}, sQ_{Beto}) = e(Q_{Alice}, Q_{Beto})^s$.
- Tem-se que $K_{ab} = K_{ba}$.

Encryption Boneh & Franklin (2001)

Criptografia

- **Alice** deseja enviar a mensagem m para Beto. Ela então calcula:
  - Aleatório $r \in \mathbb{F}_q$.
  - $U = rP$.
  - $V = m \oplus H_3(e(rQ_{beto}, R_{TA}))$.
- Alice envia (U, V) para Beto.

Decriptografia

- **Beto** recebe (U, V) de Alice. Ele então calcula:
  - $m = V \oplus H_3(e(S_{beto}, U))$.

Encryption Boneh & Franklin (2001)

Demonstração

- $V \oplus H_3(e(S_{beto}, U)) = V \oplus H_3(e(S_{beto}, rP))$, pois $U = rP$
- $= V \oplus H_3(e(sQ_{beto}, rP))$, pois $S_{beto} = sQ_{beto}$
- $= V \oplus H_3(e(Q_{beto}, P)^{rs})$, por bilinearidade
- $= V \oplus H_3(e(rQ_{beto}, sP))$, por bilinearidade
- $= V \oplus H_3(e(rQ_{beto}, R_{TA}))$, pois $R_{TA} = sP$
- $= \underbrace{(m \oplus H_3(e(rQ_{beto}, R_{TA})))}_{V} \oplus H_3(e(rQ_{beto}, R_{TA}))$
- $= m \oplus (H_3(e(rQ_{beto}, R_{TA})) \oplus H_3(e(rQ_{beto}, R_{TA})))$
- $= m$.

Criptassinatura (Esquema de Nalla & Reddy)

Criptografia e assinatura

- **Alice** escolhe um aleatório $a \in \mathbb{F}_q$ e calcula:
  - $R = aS_{Alice}$.
  - $h = H_2(R||H_3(e(Q_{Beto}, S_{Alice}))||m)$.
  - $S = ahQ_{Alice}$.
  - $k_a = H_3(e(Q_{Beto}, S_{Alice})^{ah})$.
  - $C = k_a \oplus m$.
- Alice envia (R, S, C) para Beto.

Decriptografia e verificação da assinatura

- **Beto** recebe (R, S, C) de Alice. Ele então calcula:
  - $k_b = H_3(e(S_{Beto}, S))$.
  - $m = k_b \oplus C$.
  - $h = H_2(R||H_3(e(S_{Beto}, Q_{Alice}))||m)$.
- E verifica se:
  - $e(S_{Beto}, S) = e(Q_{Beto}, R)^h$.

Criptassinatura (Esquema de Nalla & Reddy)

Demonstração que Alice e Beto calculam a mesma chave

- $k_b = H_3(e(S_{Beto}, S))$
- $= H_3(e(S_{Beto}, ahQ_{Alice}))$
- $= H_3(e(S_{Beto}, Q_{Alice})^{ah})$, por bilinearidade
- $= H_3(e(sQ_{Beto}, Q_{Alice})^{ah})$, pois $S_{Beto} = sQ_{Beto}$
- $= H_3(e(Q_{Beto}, sQ_{Alice})^{ah})$, por bilinearidade
- $= H_3(e(Q_{Beto}, S_{Alice})^{ah})$, pois $S_{Alice} = sQ_{Alice}$
- $= k_a$.

Como $k_a = k_b$, Beto consegue calcular m

- $C \oplus k_b = (m \oplus k_a) \oplus k_b = m$.

Criptassinatura (Esquema de Nalla & Reddy)

Demonstração da verificação da assinatura

- $e(Q_{Beto}, R)^h = e(Q_{Beto}, aS_{Alice})^h$
- $= e(Q_{Beto}, ahS_{Alice})$
- $= e(Q_{Beto}, ahsQ_{Alice})$
- $= e(sQ_{Beto}, ahQ_{Alice})$
- $= e(S_{Beto}, ahQ_{Alice})$
- $= e(S_{Beto}, S)$.

Roteiro

Public Key Generator - PKG

- Qualquer um que possua um par de chaves padrão, pode fazer o papel de PKG.
  - **Exemplo**: Imagine uma empresa que trata de assuntos sensíveis. Se a PKG for uma entidade externa à empresa, ela poderia decriptografar todas as mensagens.
  - O presidente da empresa (no exemplo acima), poderia fazer o papel de PKG, pois neste caso ele seria uma Autoridade de Confiança.

Delegação de serviços

- Suponha que **Alice** é presidente de uma empresa, e deseja se comunicar de maneira segura com vários departamentos, sem que um departamento (digamos A) consiga ler mensagens enviadas por outro departamento (digamos B).
- Isto é possível se Alice fizer o papel da PKG, e concatenar um **assunto** ao seu identificador.
  - **alice@empresa.com||recursos_humanos**
  - **alice@empresa.com||financeiro**
  - **alice@empresa.com||tecnologia**

Validade de chaves públicas

- É possível criar chaves com período de validade pré-estabelecido, concatenando-se o período de validade no identificador.
  - **alice@provedor.com||2011**
  - **alice@provedor.com||outubro2011**
  - **alice@provedor.com||04/10/2011**

Roteiro

Algumas vantagens de sistemas criptográficos baseados em identidades

- Não há necessidade de um diretório de chaves públicas.
- As chaves públicas possuem vínculo com seu dono.
- É possível enviar mensagens criptografadas para um usuário que não tenha ainda recebido seu par de chaves da Autoridade de Confiança.
- Comprimento (em bits) das chaves para um mesmo nível de segurança é menor, comparado com sistemas de criptografia assimétrica tradicionais.

Comprimento de chaves secretas para mesmo nível de segurança

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

Algumas desvantagens de sistemas criptográficos baseados em identidades

- Grande dependência da chave mestra da Autoridade de Confiança.
- A Autoridade de Confiança tem conhecimento de todas as chaves particulares dos usuários.
- Emparelhamentos são operações computacionalmente custosas.

Comparação: ICP *vs* CBI

Característica	**ICP**	**CBI**
Necessidade de diretório de chaves públicas	sim	não
Existência de certificados	sim	não
Geração de chaves em instantes distintos	não	sim
Chave pública escolhida livremente	não	sim
Nível de confiança depositado na autoridade central	médio	alto

Referências Bibliográficas

- BENITS JÚNIOR. Waldyr Dias. **Sistemas criptográficos baseados em identidades pessoais**. Dissertação de mestrado. Instituto de Matemática e Estatística. Universidade de São Paulo. 2003.
- BONEH. D, FRANKLIN. M. **Identity based encryption from the Weil pairing**. Proceedings of CRYPTO 2001.
- NALLA. D, REDDY. K. **Signcryption scheme for Identity-based Cryptosystems**. Disponível em <http://eprint.iacr.org/2003/066>. Acesso em 01/10/2011.

Referências Bibliográficas

- OLIVEIRA. Matheus Fernandes. **Um estudo sobre a implementação de criptossistemas baseados em emparelhamentos bilineares sobre curvas elípticas em cartões inteligentes de oito bits**. Dissertação de Mestrado. Universidade de Campinas. 2010.
- SAKAI. Ryuichi, OHGISHI. Kiyoshi, KASAHARA. Masao. **Cryptosystems Based on Pairing**. The 2000 Symposium on Cryptography and Information Security. Okinawa, Japan. 2000.
- 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!