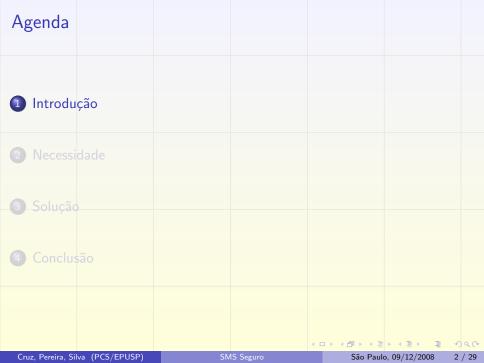
Sistema de SMS Seguro PCS2050 - Projeto de Formatura II Apresentação Final

Eduardo de Souza Cruz Geovandro Carlos Crepaldi Firmino Pereira Rodrigo Rodrigues da Silva Orientador: Prof. Dr. Paulo S. L. M. Barreto

Departamento de Engenharia de Computação e Sistemas Digitais Escola Politécnica da Universidade de São Paulo

São Paulo, 09/12/2008



Motivação e Cenário Crescimento do uso do SMS no mundo: Cruz, Pereira, Silva (PCS/EPUSP) São Paulo, 09/12/2008 3 / 29

Crescimento do uso do SMS no mundo:

2,3 trilhões de mensagens em 2010 (previsão)

- Crescimento do uso do SMS no mundo:
 - 2,3 trilhões de mensagens em 2010 (previsão)
- Plataforma leve e barata, com grande base de usuários:

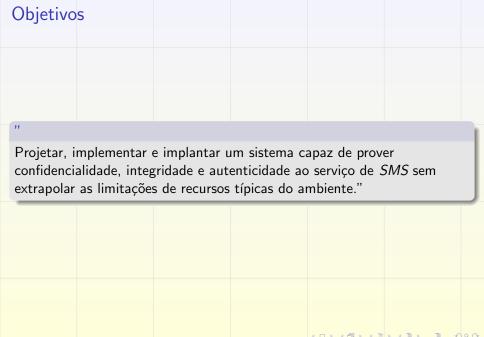
- Crescimento do uso do SMS no mundo:
 - 2,3 trilhões de mensagens em 2010 (previsão)
- Plataforma leve e barata, com grande base de usuários:
 - 2,4 bilhões de pessoas

- Crescimento do uso do SMS no mundo:
 - 2,3 trilhões de mensagens em 2010 (previsão)
- Plataforma leve e barata, com grande base de usuários:
 - 2,4 bilhões de pessoas
- Diversas oportunidades econômicas:

- Crescimento do uso do SMS no mundo:
 - 2,3 trilhões de mensagens em 2010 (previsão)
- Plataforma leve e barata, com grande base de usuários:
 - 2,4 bilhões de pessoas
- Diversas oportunidades econômicas:

72,5 bilhões de dólares para operadoras em 2006

- Crescimento do uso do SMS no mundo:
 - 2,3 trilhões de mensagens em 2010 (previsão)
- Plataforma leve e barata, com grande base de usuários:
 - 2,4 bilhões de pessoas
- Diversas oportunidades econômicas:
 - 72,5 bilhões de dólares para operadoras em 2006
- Possibilidade de produzir pesquisa: inovação



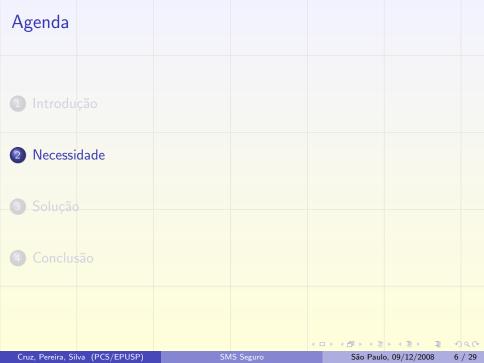
Metodologia • Estudo do cenário, detalhamento do problema e levantamento de requisitos

Metodologia

- Estudo do cenário, detalhamento do problema e levantamento de requisitos
- Estudo de esquemas de segurança em busca de uma solução adequada ao problema

Metodologia

- Estudo do cenário, detalhamento do problema e levantamento de requisitos
- Estudo de esquemas de segurança em busca de uma solução adequada ao problema
- Projeto, implementação e testes



Aplicações Potenciais Comunicação interpessoal Cruz, Pereira, Silva (PCS/EPUSP) 7 / 29

Aplicações Potenciais

- Comunicação interpessoal
- Transações bancárias e pagamentos

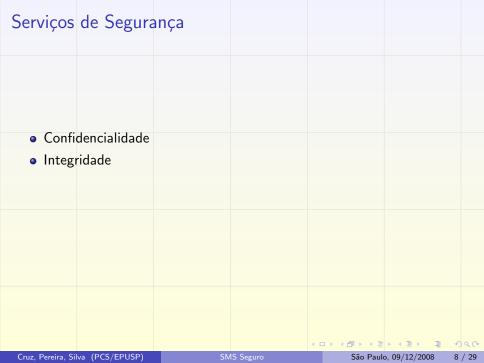
Aplicações Potenciais

- Comunicação interpessoal
- Transações bancárias e pagamentos
- Comunicação corporativa e governamental sigilosa

Aplicações Potenciais

- Comunicação interpessoal
- Transações bancárias e pagamentos
- Comunicação corporativa e governamental sigilosa
- Monitoração remota





Serviços de Segurança Confidencialidade Integridade Autenticidade Cruz, Pereira, Silva (PCS/EPUSP) São Paulo, 09/12/2008 8 / 29

Serviços de Segurança Confidencialidade Integridade Autenticidade Irretratabilidade Cruz, Pereira, Silva (PCS/EPUSP) São Paulo, 09/12/2008 8 / 29

Definição do Problema • SMS armazenado em aberto nas integradoras e operadoras

- SMS armazenado em aberto nas integradoras e operadoras
- Recursos limitados: processamento, memória, largura de banda

- SMS armazenado em aberto nas integradoras e operadoras
- Recursos limitados: processamento, memória, largura de banda
- Algoritmo A5 da rede GSM quebrado

- SMS armazenado em aberto nas integradoras e operadoras
- Recursos limitados: processamento, memória, largura de banda
- Algoritmo A5 da rede GSM quebrado
- Poucas soluções de segurança no mercado

- SMS armazenado em aberto nas integradoras e operadoras
- Recursos limitados: processamento, memória, largura de banda
- Algoritmo A5 da rede GSM quebrado
- Poucas soluções de segurança no mercado
- RSA: cerca de 15 mensagens para trocar um certificado

- SMS armazenado em aberto nas integradoras e operadoras
- Recursos limitados: processamento, memória, largura de banda
- Algoritmo A5 da rede GSM quebrado
- Poucas soluções de segurança no mercado
- RSA: cerca de 15 mensagens para trocar um certificado
- Algoritmos simétricos: grande quantidade de senhas

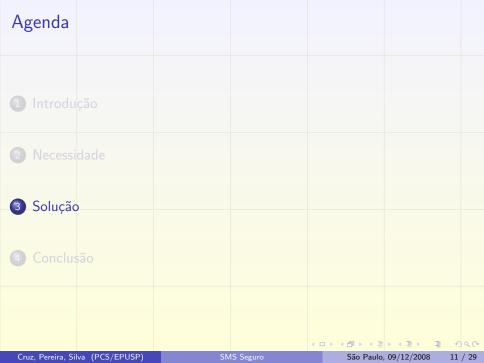
Métricas e Requisitos • Tempo de espera Cruz, Pereira, Silva (PCS/EPUSP) São Paulo, 09/12/2008 10 / 29

Métricas e Requisitos • Tempo de espera • Espaço útil da mensagem Cruz, Pereira, Silva (PCS/EPUSP) São Paulo, 09/12/2008 10 / 29

Métricas e Requisitos • Tempo de espera • Espaço útil da mensagem Tamanho da chave

Métricas e Requisitos

- Tempo de espera
- Espaço útil da mensagem
- Tamanho da chave
- Overhead do protocolo



Especificação Especificacao Cruz, Pereira, Silva (PCS/EPUSP) São Paulo, 09/12/2008 12 / 29

Arquitetura Arquitetura Cruz, Pereira, Silva (PCS/EPUSP) São Paulo, 09/12/2008 13 / 29



Implementação Curvas elípticas Chaves menores Cruz, Pereira, Silva (PCS/EPUSP) São Paulo, 09/12/2008 14 / 29

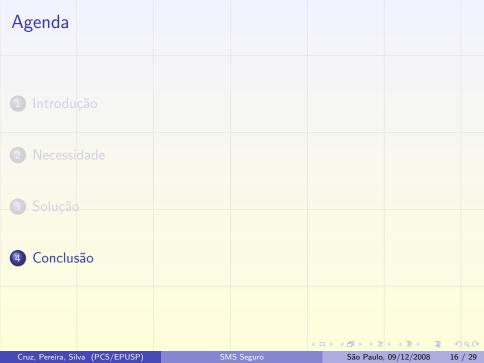
Implementação Curvas elípticas Chaves menores Criptografia auto-certificada

Implementação Curvas elípticas Chaves menores Criptografia auto-certificada • Criptografia baseada em identidades

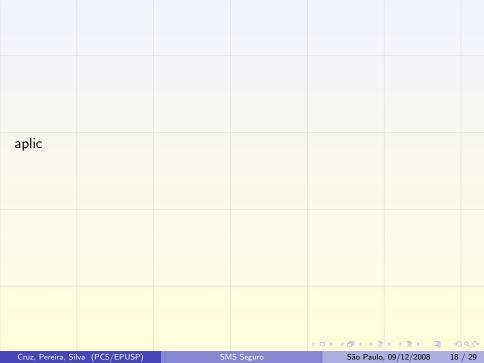
Implementação

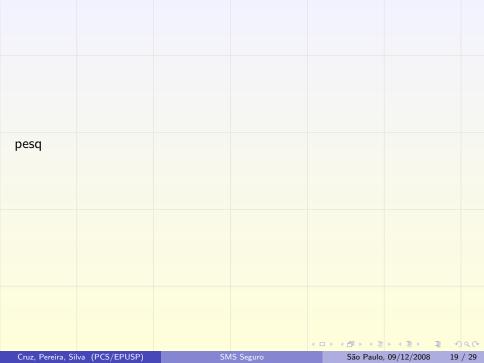
- Curvas elípticas
- Chaves menores
- Criptografia auto-certificada
- Criptografia baseada em identidades
- Gerenciamento de chaves simplificado

Resultados res Cruz, Pereira, Silva (PCS/EPUSP) São Paulo, 09/12/2008 15 / 29



Conclusão concl Cruz, Pereira, Silva (PCS/EPUSP) São Paulo, 09/12/2008 17 / 29



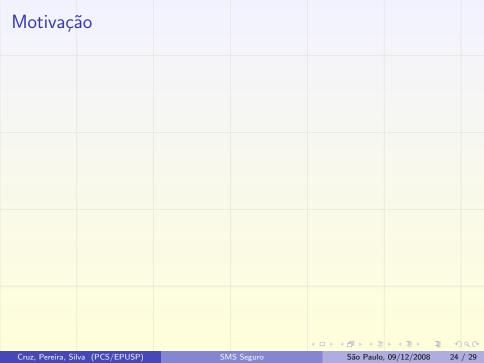


Desenvolvimentos	futuros			
fut				
Cruz, Pereira, Silva (PCS/EPUSP)	SM	1S Seguro	◆ □ ▶ ◆ 吾 ▶ ◆ 臺 São Paulo	0 4 (~





This is a short introduction to	o Beamer class.	
Cruz, Pereira, Silva (PCS/EPUSP)	SMS Seguro	 ✓ □ → ✓ □ → ✓ □ → ✓ □ → ○ □ São Paulo, 09/12/2008 23 / 2



Motivação Beamer is a wonderful class Cruz, Pereira, Silva (PCS/EPUSP) São Paulo, 09/12/2008 24 / 29

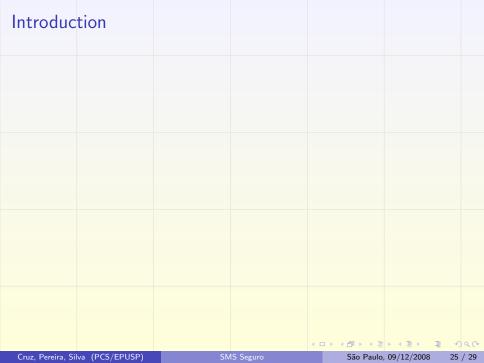
Motivação Beamer is a wonderful class One can make animations 24 / 29

Motivação Beamer is a wonderful class One can make animations • One uses the **pause** command, for example

Motivação

- Beamer is a wonderful class
- One can make animations
- One uses the **pause** command, for example
- in order to bring in important ideas

This is a short introduction to Beamer class.

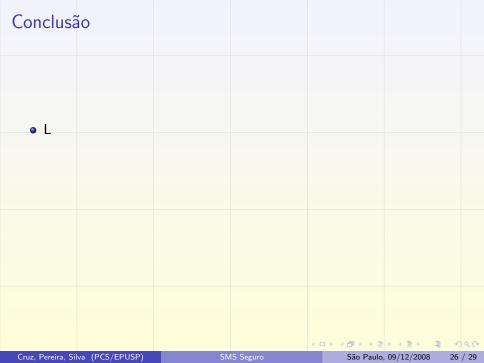


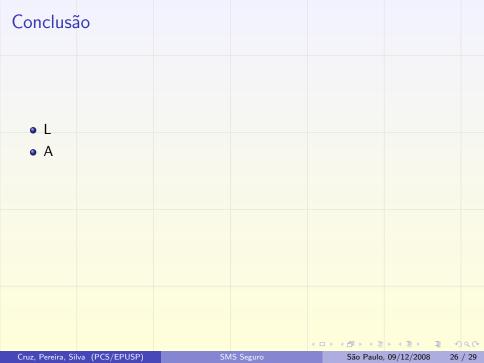
Introduction appears from slide 2 on • appears from slide 2 to slide 4 Cruz, Pereira, Silva (PCS/EPUSP) São Paulo, 09/12/2008 25 / 29

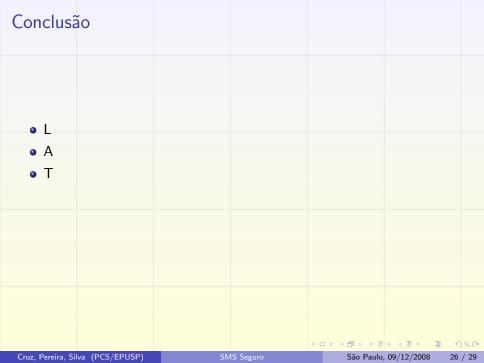
Introduction • appears from slide 2 on • appears from slide 2 to slide 4 appears from slide 3 on

Introduction appears from slide 2 on • appears from slide 2 to slide 4 • appears on slide 4 appears from slide 3 on

Introduction • appears from slide 2 on • appears from slide 3 on • 5 Cruz, Pereira, Silva (PCS/EPUSP) São Paulo, 09/12/2008 25 / 29

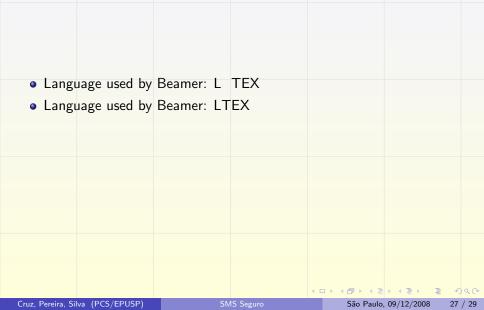




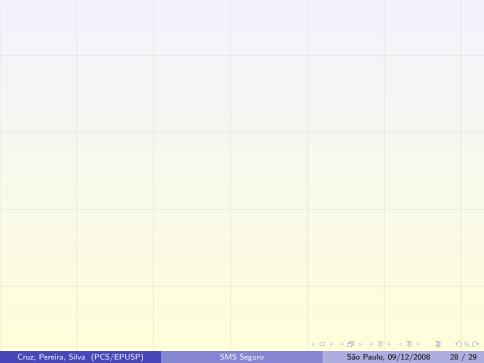


Conclusão L A T E Cruz, Pereira, Silva (PCS/EPUSP) São Paulo, 09/12/2008 26 / 29

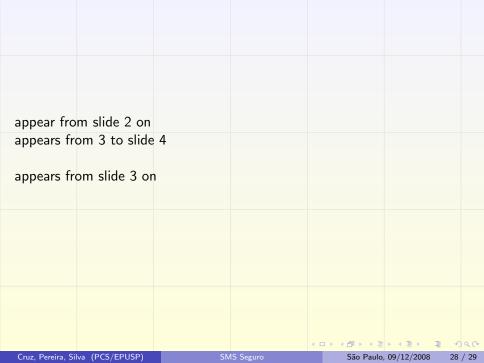
Conclusão L A T E X Cruz, Pereira, Silva (PCS/EPUSP) São Paulo, 09/12/2008 26 / 29













Block title This is a block in blue Alert-block title This is a block in red

Example-block title
This is a block in green