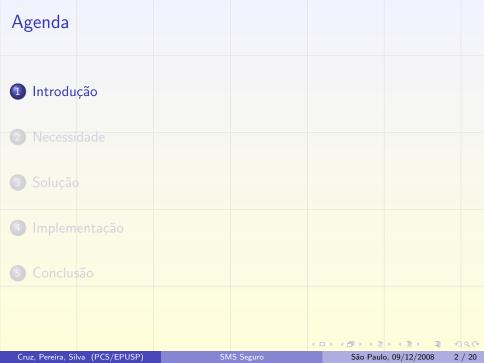
### Sistema de SMS Seguro PCS2050 - Projeto de Formatura II Apresentação Final

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 / 20

• 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:

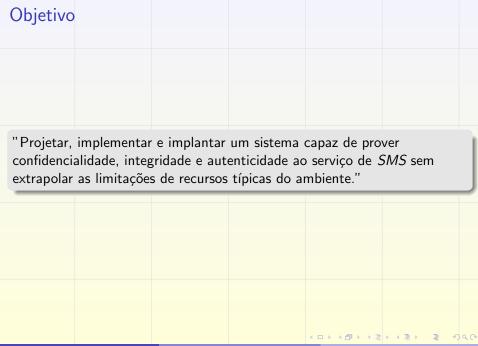
- Crescimento do uso do SMS no mundo:
  - 2,3 trilhões de mensagens em 2010 (previsão)
- Plataforma leve e barata, com grande base de usuários:
  - 2,4 bilhões de pessoas

- 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
- Ausência de uma solução universalmente adotada.

- 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
- Ausência de uma solução universalmente adotada.
- Possibilidade de produzir pesquisa: inovação



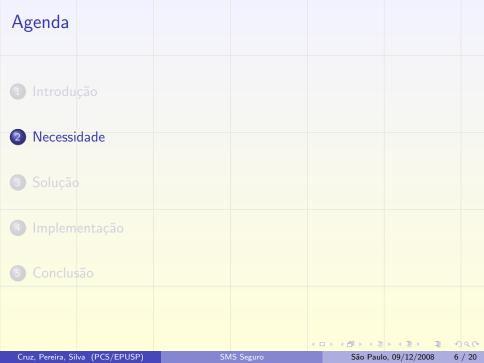
# Metodologia • Estudo do cenário, detalhamento do problema e levantamento de requisitos

### 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 / 20

### Aplicações Potenciais

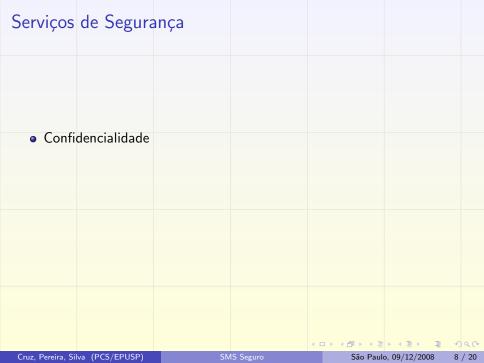
- Comunicação interpessoal
- Transações bancárias e pagamentos

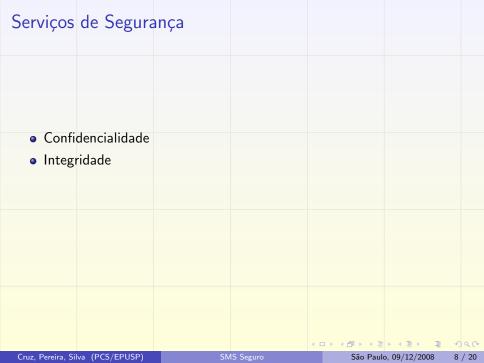
### Aplicações Potenciais

- 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 / 20

### Serviços de Segurança Confidencialidade Integridade Autenticidade Irretratabilidade Cruz, Pereira, Silva (PCS/EPUSP) São Paulo, 09/12/2008 8 / 20

# 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 20 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 20 mensagens para trocar um certificado
- Algoritmos simétricos: Dificuldade em gerenciar as chaves

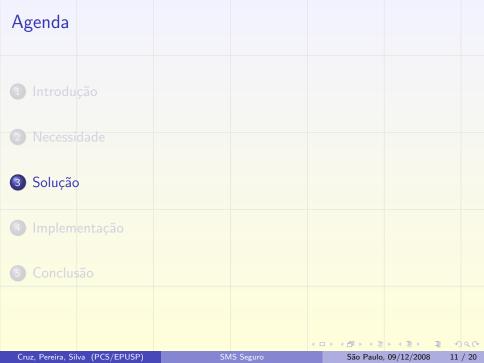
# Métricas e Requisitos • Tempo de espera Cruz, Pereira, Silva (PCS/EPUSP) São Paulo, 09/12/2008 10 / 20

### Métricas e Requisitos • Tempo de espera • Espaço útil da mensagem Cruz, Pereira, Silva (PCS/EPUSP) São Paulo, 09/12/2008 10 / 20

# 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



### Esquema de segurança desenvolvido

Ao longo do trabalho, foi bolado um esquema de segurança inovador

Curvas elípticas

40.49.45.45.5

### Esquema de segurança desenvolvido

Ao longo do trabalho, foi bolado um esquema de segurança inovador

- Curvas elípticas
- Chaves menores

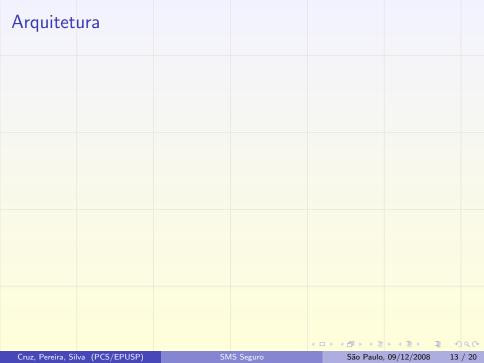
- Curvas elípticas
- Chaves menores
- Criptografia auto-certificada

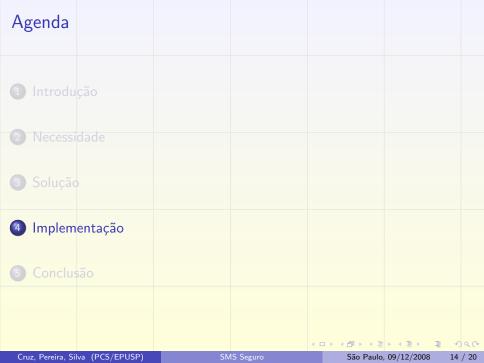
- Curvas elípticas
- Chaves menores
- Criptografia auto-certificada
- Criptografia baseada em identidades

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

- Curvas elípticas
- Chaves menores
- Criptografia auto-certificada
- Criptografia baseada em identidades
- Gerenciamento de chaves simplificado
- Publicação de artigo no SBSEG'08 definindo o novo esquema

- Curvas elípticas
- Chaves menores
- Criptografia auto-certificada
- Criptografia baseada em identidades
- Gerenciamento de chaves simplificado
- Publicação de artigo no SBSEG'08 definindo o novo esquema
- Publicação de artigo no WTICG'08 sobre o nosso projeto de formatura (menção honrosa)





Classes					
• Esque	ema impleme	ntado em J2	ME		
Cruz, Pereira, Sil	va (PCS/EPUSP)	SM	1S Seguro	São Paulo,	.5 / 20





