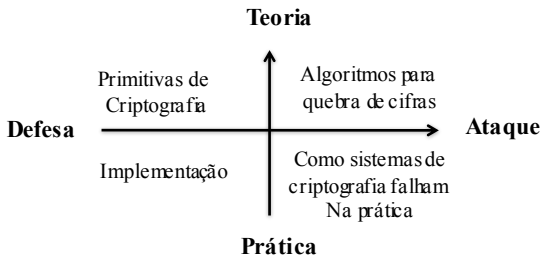
Segurança de Sistemas Criptografia

Prof. Avelino Francisco Zorzo
Escola Politécnica- PUCRS

PS: Este curso está baseado no curso CSC-3661 Cryptography preparado Prof. Feng Hao – Newcastle University e no curso *online* Cryptography preparado pelo Prof. Dan Bonneh – Stanford University.

Objetivos



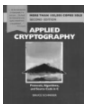
Livros de referência

Firewalls e Segurança na Internet (William Cheswick, 2003)

Criptografia e segurança de redes (William Stallings, 2008)

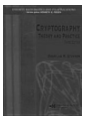
O Livro de códigos (Simon Singh, 2004)

Applied Cryptography (Bruce Schneier, 1996)



Handbook of Applied Cryptography (Alfred Menezes, 1997)

Cryptography: Theory and Practice (Doug Stinson, 2006)



O que é criptografia?

- "A arte e ciência de manter informações seguras".

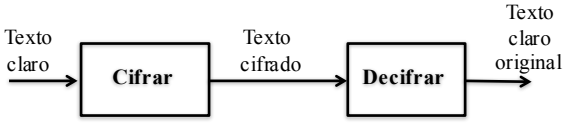
  - Bruce Scheneier

- "Criptografia envolve a projeção de confiança: levar confiança de onde existe para onde é necessária."

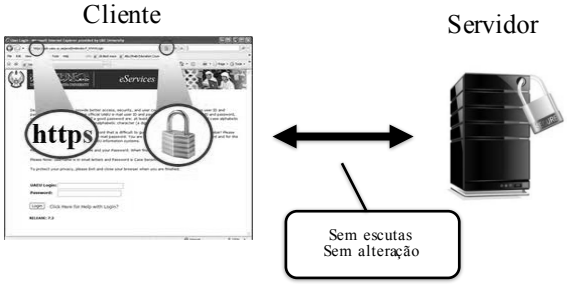
  - Ross Anderson

Terminologia

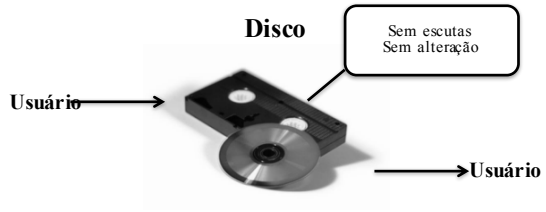
- Enviador e receptor
- Mensagens e cifrar (criptografar)



Comunicação segura (bancos)



Comunicação pessoal (cifrar um disco)



Similar à comunicação segura:
Usuário hoje envia uma mensagem para ele mesmo amanhã.

Objetivos/metas básicas

1. **Privacidade**: sem vazar dados confidenciais
2. **Autenticação**: sem se passar por outro
3. **Integridade**: sem alteração
4. **Não-repúdio**: não ser capaz de negar

Algoritmos e chaves

- **Cifra**: um algoritmo criptográfico para cifrar (criptografar) e decifrar (decriptografar).
- **Chave**: usada para cifrar e decifrar
- **Espaço da chave**: quantia de chaves possíveis

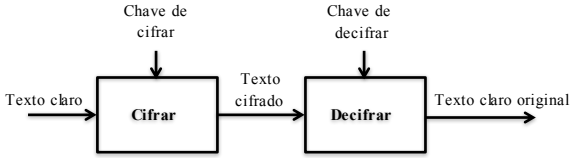
- "O segredo deve estar totalmente na chave e não na cifra".

Princípio de Kerckhoff

Seis princípios de Kerckhoff (1883)

1. O sistema deveria ser inquebrável na prática, se não teoricamente inquebrável.
2. O projeto de um sistema não de necessitar segredo do sistema.
3. A chave deve ser memorizável e fácil de alterar.
4. Os criptogramas devem ser transmissíveis por telégrafo.
5. O equipamento deve ser portável e operável por uma única pessoa.
6. O sistema deve ser fácil de usar.

Cifras simétricas e assimétricas



- Chaves de cifrar e decifrar podem ser
  - A mesma nas cifras **simétricas**
  - Ou diferentes em cifras **assimétricas**

Criptoanálise

- A arte e ciência de analisar fraquezas em algoritmos criptográficos (cifras)
- Também conhecido como **ataque**.

- **Criptologia** = **Criptografia** + **Criptoanálise**

Quatro tipos de ataques genéricos

1. Ataque **só com texto cifrado** (*Ciphertext-only*)
2. Ataque **com texto claro conhecido** (*Known-plaintext*)
   - Na II Guerra Mundial: mensagens alemãs começavam com uma data
3. Ataque **com texto claro escolhido** (*Chosen-plaintext*)
   - Quebra de código na batalha de Midway (II GM)
4. Ataque **com texto cifrado escolhido** (*Chosen-ciphertext*)
   - O objetivo é deduzir a chave (ataque na hora do almoço)

Nomes utilizados

- **Alice** - Primeira pessoa que participa
- **Bob** - Segundo participante
- **Carol** - Terceiro participante
- **Eve** - Alguém na escuta (*eavesdropper*)
- **Mallory** - Atacante ativo

Grandes números (armazenar)

- Número de átomos no planeta 2^{170}
- Número de átomos no sol 2^{190}
- Número de átomos na galáxia 2^{223}
- Número de átomos no universo 2^{265}

- Para armazenar uma chave de 256-bit 2^{264} bits

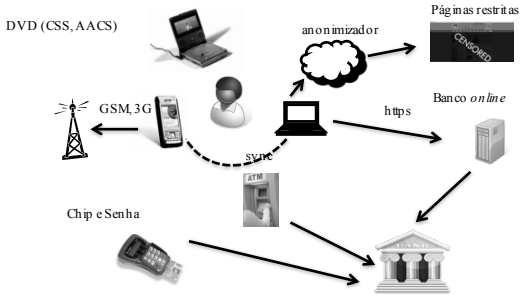
Grandes números (tempo)

- Tempo até a próxima era do gelo 2^{14} anos
- Tempo até o sol virar nova 2^{30} anos
- Idade do planeta Terra 2^{30} anos
- Idade do Universo 2^{34} anos

- Tempo para quebrar por força bruta uma chave de 256 bits 2^{192} anos

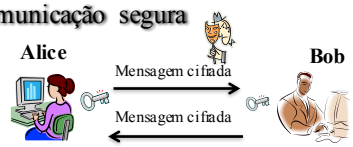
(Assumindo testar 1 bilhão de chaves em 1 ms)

Criptografia em todos lugares



Núcleo de criptografia

- Comunicação segura



- Estabelecer a chave

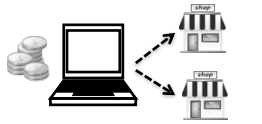
Mas criptografia pode muito mais

- Assinatura digital

É uma falsificação?

- Dinheiro digital

Gastou duas vezes?



Cara ou coroa no telefone

- Alice e Bob decidem jogar honestamente cara ou coroa via telefone

Alice → Bob: Eu jogo. Venço se der cara.
Bob → Alice: OK. Jogue.
Alice → Bob: Feito! Deu cara.
Bob → Alice: Humm… como eu sei que você não trapaceou?

Para lembrar

- Leis de segurança de Shamir (Prêmio Turing 2002)
  1. Sistemas completamente seguros não existem.
  2. Para diminuir suas vulnerabilidades pela metade, deve-se dobrar os gastos.
  3. Criptografia é normalmente contornada, não quebrada.