Histórico

"O impulso para descobrir segredos está profundamente enraizado na natureza humana. Mesmo a mente menos curiosa é estimulada pela perspectiva de compartilhar o conhecimento oculto aos outros"

(John Chadwick)

Histórico

- 480 a.C. – Grécia x Pérsia
  - Narrado por Heródoto
  - Xerxes, Rei dos Reis, líder dos persas
  - Construção de Persépolis
  - Atenas e Esparta não presentearam o Reino
  - Cinco anos montando seu exército
  - Planejamento de ataque-surpresa a Esparta
  - Demarato, grego que vivia em Susa (Pérsia)
  - Mensagem contando planos de invasão
  - Desafio : Como enviar a mensagem ?
  - Tabuletas de Madeira (revestidas de cera)
  - Mensagem entregue ao destino
  - Gorgo, filha de Cleômenes, desconfiou
  - Armadilha e humilhação do exército persa

Histórico

- 480 a.C. – Outra técnica de ocultação
  - Também narrada por Heródoto
  - Histaeu queria encorajar Aristágora de Mileto a se revoltar contra o rei persa
  - Rapagem da cabeça do mensageiro
  - Mensagem escrita no couro cabeludo
  - Espera pelo crescimento do cabelo
  - Mensageiro revistado sem problemas
  - Chegada ao destino : Nova raspagem da cabeça

Histórico

- Técnica Chinesa Antiga
  - Escrita em seda fina
  - Mensagem amassada e coberta com cera
  - Bola de cera engolida pelo mensageiro
  - Leitura no destino dependia da digestão

Histórico

- Século I d.C. – Tinta Invisível
  - Descrita por Plínio, o velho
  - "leite" da planta titímalo
  - Transparente depois de seca
  - Aquecimento suave queima a tinta, deixando a mensagem escrita marrom

Histórico

- Século XVI – Mensagem no Ovo Cozido
  - Cientista Italiano Giovanni Porta
  - Tinta feita com alume e vinagre
  - Escrita sobre a casca do ovo cozido
  - Solução penetra na casca e estampa o ovo
  - Para ler basta retirar a casca do ovo

Conceitos

"À medida em que a informação se torna uma mercadoria cada vez mais valiosa e a revolução nas comunicações muda a sociedade, o processo de codificação de mensagens vai desempenhar um processo cada vez maior na vida diária"

(Simon Singh)

Conceitos

- Esteganografia (Steganography)
  - Comunicação secreta por ocultação de mensagem
  - Do grego : *steganos* = coberto
    graphein = escrever
  - Utilizada atualmente para esconder textos em imagens ou em outros textos
  - Segurança por obscuridade

Conceitos

- Esteganografia (Steganography)

Exemplo (mensagem escondida em um texto):

O Senhor Evandro quer usar este salão temporariamente. Relembre o fato ocorrido, isto poderia estragar relíquias, florais e imagens talhadas. Obrigado.

O Senhor Evandro quer usar este salão temporariamente. Relembre o fato ocorrido, isto poderia estragar relíquias, florais e imagens talhadas. Obrigado.

O sequestro foi perfeito

Conceitos

- Esteganografia (Steganography)

Exemplo (mensagem escondida em uma imagem):

- Demonstração da ferramenta S-tools
- Imagem .gif ou .bmp
- Necessário software específico
- Necessária senha determinada pelo emissor

Conceitos

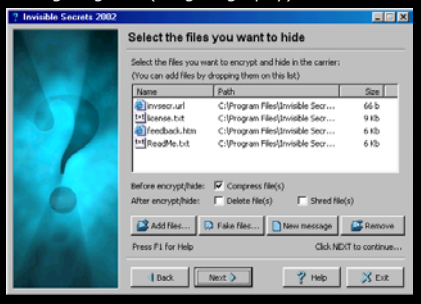
- Esteganografia (Steganography)

Ferramentas Específicas:

- S-tools
- Invisible Secrets
- Gifshuf
- Hideseek
- Gifclean
- HIP (Hide in Picture)

Conceitos

- Esteganografia (Steganography)



Conceitos

Esteganografia (Steganography)

Links Relacionados :

- Invisible Secrets 3.0
http://www.freedownloadscenter.com/Utilities/File_Encryption_Utilities/Invisible_Secrets.html
- Steganographia, by Johannes Trithemius (in Latin)
http://www.esotericarchives.com/tritheim/stegano.htm
- How Steganographia was cracked:
http://cryptome.unicast.org/cryptome022401/tri-crack.htm
- Bin Laden: Steganography Master?
http://www.wired.com/news/politics/0,1283,41658,00.html

Conceitos

Criptografia

- Comunicação secreta por cifragem da mensagem
- Do grego : *kriptos* = oculto
graphein = escrever
- Evolução paralela à Esteganografia
- A mensagem é misturada de acordo com um protocolo específico estabelecido previamente entre o transmissor e o receptor

Conceitos

Criptografia

- Vantagem : leitura ilegível caso interceptada
- **Encriptação :** processo de esconder o significado de uma mensagem
- A criptografia pode ser utilizada em conjunto com a Esteganografia.

Ex: Microponto (utilizado pela Alemanha durante a Segunda Guerra Mundial)

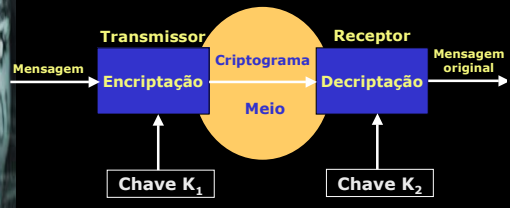
Redução fotográfica de uma página de texto a um ponto com menos de 1mm de diâmetro

Conceitos

Criptografia

- **Simétrica**
  - **Também conhecida como tradicional**
  - **Origem e destino compartilham uma única chave**
  - **Computacionalmente leves / rápidos**
- **Assimétrica**
  - **Cada entidade possui um par de chaves (publica/privada)**
  - **Computacionalmente pesados / lentos**

Conceitos



Em Algoritmos Simétricos $K_1 = K_2 (K)$

Conceitos

Criptografia simétrica

- **Técnicas :**
  - **Substituição**

    Letras da mensagem são substituídas por outras letras e/ou símbolos conforme uma tabela de conversão.

    Ex: A C T R
    ↓ ↓ ↓ ↓
    X Y K Z

    ATACAR = XKXYXZ
  - **Transposição**

    Conteúdo da mensagem rearranjado, gerando um anagrama

    Ex : ema → eam, aem, mea, mae, ame.

Conceitos

- Criptografia simétrica
  - Algoritmo
    - **É o próprio processo de substituição ou transposição**
    - **Passos a serem tomados para realizar a encriptação**
  - Chave
    - **Define o alfabeto cifrado exato que será utilizado em uma codificação em particular**

O algoritmo utilizado em um processo de encriptação pode ser divulgado sem problemas. A chave, porém, deve ser uma informação confidencial do remetente e do destinatário

Conceitos

- Criptografia simétrica
  - Cifra
    - **Nome dado a qualquer forma de substituição criptográfica, no qual cada letra é substituída por outra letra ou símbolo**
  - Alfabeto Original
    - **Conjunto de caracteres usado para escrever a mensagem original (antes de ser encriptada)**
  - Alfabeto Cifrado
    - **Conjunto de caracteres utilizados na substituição de uma mensagem em uma encriptação**

Conceitos

- Criptografia simétrica
  - ***Citale Espartano***
    - **Aparelho criptográfico militar baseado em criptografia por transposição**
    - **Bastão de madeira enrolado com uma tira de couro sobre a qual é escrita a mensagem**
    - **Para desencriptar é necessário um citale com o mesmo diâmetro.**

Conceitos

- Criptografia simétrica
  - **Método da *"cerca de ferrovia"* (transposição)**
    - **Mensagem original escrita alternando as letras em duas linhas (uma abaixo da outra)**
    - **A mensagem cifrada é então escrita concatenando-se as duas linhas**

Ex: para a mensagem REDES CTI 2002

```
R D S C I 2 0
 E E   T   0 2
```

Mensagem Cifrada : RDSCI20EE T 02

Conceitos

- Criptografia simétrica
  - **Algoritmo DES (Data Encription Stardard)**
    - **Criado em 1977, como um padrão para comunicação segura**
    - **Principal Algoritmo derivado da criptografia simétrica**
    - **Algoritmo de criptografia mais usados até os dias atuais (forma original ou alterações)**

Conceitos

- Criptografia simétrica
  - **Algoritmo DES (Data Encription Stardard)**
    - **Utiliza uma chave de 64 bits de comprimento**
    - **Mensagem é codificada em blocos também de 64 bits**
    - **Funcionamento**
      - **Uma transposição inicial**
      - **16 ciclos intermediários de substituições e transposições**
      - **Uma transposição final**
    - **Para cada bloco de entrada é produzido um bloco de saída também de 64 bits**

Conceitos

- Criptografia simétrica

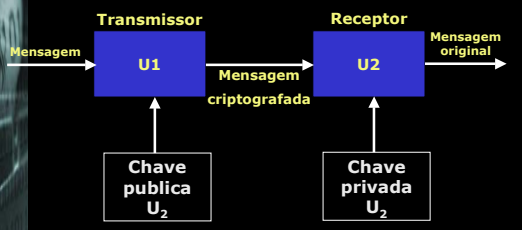
Todos os algoritmos fruto da criptografia simétrica incorrem no problema de distribuição da chave

Conceitos

- Criptografia Assimétrica
  - **Proposta em 1976**
  - **Baseada em princípios de manipulação matemática (matemática modular)**
  - **Cada usuário que deseja utilizar um algoritmo assimétrico possui um par de chaves:**
    - **Uma chave pública, distribuída livremente**
    - **Uma chave privada, secreta**

Conceitos

- Criptografia Assimétrica



Conceitos

- Criptografia Assimétrica
  - **RSA**
    - **Cada usuário calcula de forma independente seu par de chaves**
    - **Para se comunicar com outro usuário devo possuir a sua chave pública**
    - **Uma mensagem criptografada com a chave pública de um usuário só pode ser decriptografada por sua chave privada**

Conceitos

- Criptografia Assimétrica
  - **Os algoritmos de criptografia assimétrica solucionam os problemas de distribuição de chaves, no entanto o seu "peso" computacional ainda representa um fator limitante**
  - **Na prática se utilizam soluções híbridas, onde os algoritmos assimétricos são usados apenas para a troca das chaves**

Conceitos

- Criptografia Assimétrica

O desenvolvimento dos algoritmos de criptografia assimétrica possibilitou o aparecimento de aplicações que trafegam dados na internet de forma segura notadamente do *e-comerce*

Conceitos

- Criptoanálise
  - Estudo de técnicas matemáticas que possibilitam encontrar falhas em sistemas criptográficos
  - Tem como objetivo recuperar mensagens encriptadas sem ter acesso à chave, ou até mesmo recuperar a chave
- Criptologia
  - Estudo da Criptografia e da Criptoanálise

Conceitos

- Princípio de Kerckhoff

"A segurança de um criptossistema não deve depender da manutenção de um algoritmo em segredo.
A segurança depende apenas de se manter em segredo a chave".

Conceitos

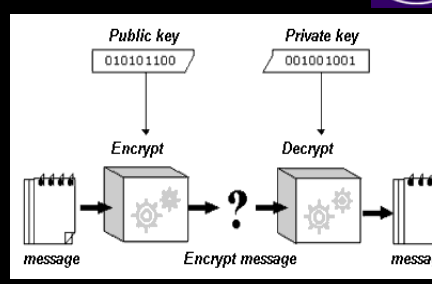
- TELNET
  - Protocolo para acesso a computadores UNIX sem implementação de criptografia (senhas trafegam "limpas" na rede)
- SSH (Secure SHell)
  - Protocolo criptografado para acesso a computadores UNIX como alternativa segura em substituição ao TELNET

Conceitos

- FTP (File Transfer Protocol)
  - Protocolo para acesso a arquivos UNIX (downloads e uploads) sem implementação de criptografia (senhas trafegam "limpas" na rede)
- WinSCP / SCP (Secure CoPy)
  - Protocolo criptografado para acesso a arquivos UNIX como alternativa segura em substituição ao FTP

Conceitos

- PGP (Pretty Good Privacy)



- Destina-se a comunicação segura via e-mail
- Utiliza algoritmos de criptografia de até 1024 bits
- A mensagem enviada pelo remetente é codificada com a chave pública do destinatário.
- O destinatário só consegue ler a mensagem após desencriptá-la com sua chave privada.
- Nenhum intermediário que porventura intercepte a mensagem poderá ver seu conteúdo, já que não dispõe da chave privada para tal

Conceitos

- PGP (Pretty Good Privacy)

Conceitos

- SSL (Secure Socket Layer)

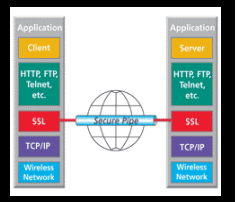
  - Protocolo de comunicação segura para aplicações Internet
  - Desenvolvido pela Netscape Communications (07/1994)
  - Padrão aberto
  - Consensualmente utilizado no e-commerce (por padrão)
  - Incorporado aos Browsers e Servidores
  - Permite :
    - Autenticação de Servidores
    - Encriptação de Dados
    - Integridade de Mensagens
    - Autenticação do Cliente

Conceitos

- SSL (Secure Socket Layer)

  - Todo site que quiser usar SSL precisará de um certificado de autenticação "assinado" por uma entidade certificadora, (como a Verisign, por exemplo)

O SSL provê uma camada de segurança entre a camada de transporte (TCP) e os protocolos de aplicação (HTTP,FTP,Telnet,etc)



Conceitos

- HTTP (HyperText Transfer Protocol)
  - Protocolo utilizado largamente para acesso a páginas web
  - Não provê infraestrutura para operações seguras
  - Tráfego passa "limpo" entre o cliente e o servidor
- HTTPS (HTTP + SSL)
  - Utilização do protocolo HTTP em conjunto com o protocolo SSL (Secure Socket Layer)

Perguntas

"Será que algum dia os criadores de códigos conseguirão elaborar um código realmente indecifrável e triunfar na busca pelo segredo absoluto?

Ou será que os decifradores poderão construir uma máquina capaz de decifrar qualquer mensagem?"

(Simon Singh)