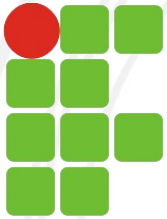


INSTITUTO FEDERAL
PIAUÍ
Campus Parnaíba

Criptografia

Prof. Msc Denival A. dos Santos

Noticia

"Dois meses e meio depois de apreender cinco discos rígidos no apartamento do banqueiro Daniel Dantas, durante a Operação Satiagraha, a Polícia Federal ainda não conseguiu decifrar a criptografia que protege os dados. Numa análise inicial, peritos da Polícia Federal disseram que precisariam de um ano para quebrar os códigos. Um dos peritos disse que nunca havia visto um sistema de proteção tão sofisticado no Brasil.
O impasse levou os investigadores da PF a estudar uma alternativa jurídica para o rompimento do sigilo. Em conjunto com o juiz federal Fausto De Sanctis, informado há mais de um mês sobre os problemas nos HDs, os policiais discutem a possibilidade de obrigar, por ordem judicial, a empresa norte-americana que criou o software a fornecer as chaves eletrônicas que abrem os arquivos."

Fonte: http://stoa.usp.br/gnusp/weblog/32631.html

Introdução

- Criptografia diz respeito ao conjunto de princípios e técnicas utilizadas na proteção digital ou mecânica de informações.
- Utilizada desde a antiguidade greco-romana, as práticas criptográficas eram inicialmente aplicadas por ferramentas mecânicas muito simples e perspicazes, que ocultavam mensagens legíveis, cifrando-as em formato incompreensíveis.
- Historicamente, alguns grupos de pessoas contribuíram para a sua evolução, entre eles os militares e amantes.
- A criptografia possui duas abordagens. Uma baseada em leis matemáticas – criptografia clássica e outra nas leis da física – criptografia quântica.
- A abordagem quântica utiliza fótons para gerar chaves “inquebráveis”, as ditas “chaves quânticas”.

Tipos de algoritmos da criptografia clássica

- Algoritmo de transposição – rearranja a ordem dos caracteres de uma mensagem.
  - Exemplo:

    Muito obrigado >>> omtui oobdraig
- Algoritmo de substituição – substitui caracteres ou grupos de caracteres por outros caracteres ou grupos de caracteres.
  - Exemplo:

    Muito obrigado >>> nvjup pcsjhbep

Simetria

- Diz respeito à igualdade de propriedades existente entre dois lados opostos de uma mesma situação.
- A proteção de informações para uso próprio é um caso si métrico, já que a pessoa a utilizar um dado arquivo é ger almente a mesma que o guardou.
  - Um situação comum que se enquadra nesse caso é o backup.
- Um segundo caso – proteção de informações trocadas co m outros – é assimétrico, pois envolve dois usuários distin tos.
  - O exemplo básico é a troca de emails confidenciais.

Chaves

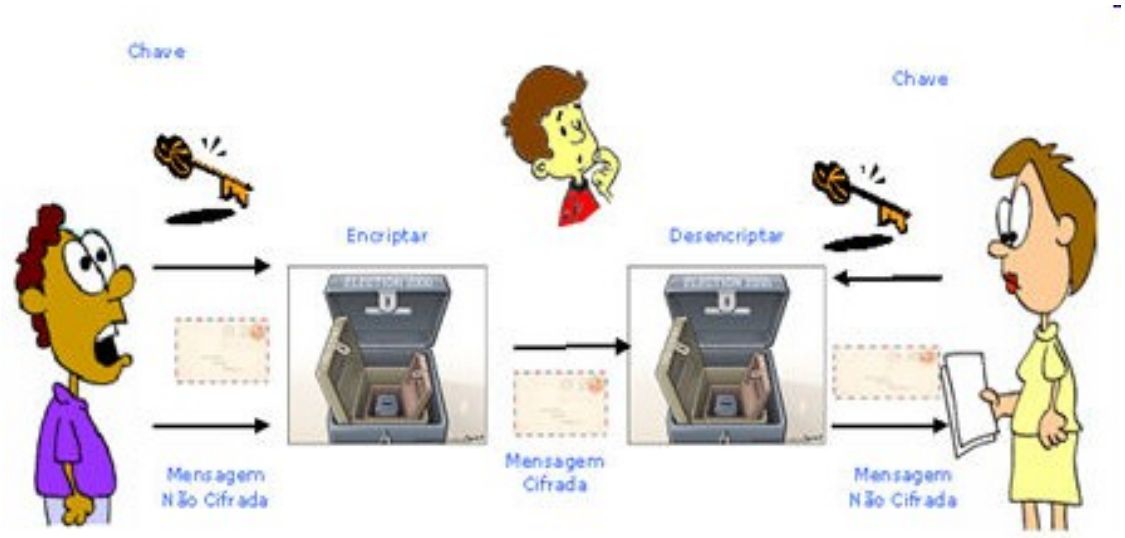
- Uma chave trata-se de uma parâmetro utilizado para se encriptar e decriptar informações.
- Chaves pequenas oferecem melhor desempenho nas operações criptográficas, mas são facilmente quebradas. Em contrapartida, o uso de chaves grandes causa lentidão, mais oferece extrema segurança.
- Geralmente, chaves de 1024 bits costumam oferecer um compromisso interessante entre desempenho e segurança das operações.
- **Privada** – deve ser de conhecimento exclusivo de seu usuário. Geralmente de com no mínimo 1024 bits.
- **Pública** – como o próprio nome diz, deve ser de domínio público. Utilizada nas seguintes situações:
  - Quando for encriptar informações que devem ser reveladas apenas ao destinatário da chave pública.
  - Quando desejar verificar a autenticidade da assinatura digital de alguém que lhe enviou algum email ou arquivo.

Algoritmos

- Os algoritmos criptográficos são utilizados em criptografia simétrica e assimétricos para fins diversos, e nem sempre estão diretamente ligados a encriptação ou decriptação.
- Podem servir a outros propósitos, como a geração de pares de chaves, ou ainda para assinaturas digitais.

Criptografia simétrica

- Este tipo de criptografia é caracterizado por ter apenas uma chave secreta que é partilhada pelo emissor e pelo receptor da mensagem, isto é, a chave que encripta é a mesma que desencripta.
- Um exemplo de utilização de criptografia simétrica é o Wi-Fi, cuja proteção mais eficiente atualmente, o WPA2, utiliza cifras simétricas entre dois ponto. Isto se deve ao desempenho proporcionado por algoritmos simétricos.
- Como exemplo de algoritmos simétricos temos: AES, DES, IDEA, Bowfish, etc.



Criptografia assimétrica

- Este tipo de algoritmo é caracterizado por utilizar um par de chaves distintas em que, embora não se consiga obter uma chave a partir de outra, estas encontram-se matematicamente relacionadas, conseguindo uma desencriptar aquilo que a outra encriptou.
- A chave pública de um usuário de email deve ser do conhecimento das pessoas que lhe desejam enviar mensagens, e pode até ser disponibilizada publicamente. Já sua chave privada deve ser conhecida exclusivamente pelo próprio dono.
- O emprego das duas chaves leva em conta que os interlocutores já possuem, cada um, a chave pública do outro.
- Basicamente, caso uma chave pública seja utilizada por um lado, uma chave privada correspondente deverá ser utilizada pelo outro, e vice-versa.

Referências Bibliográficas

- Barbado, Marcio Jr. Linux Magazine, São Paulo. N. 62, p 64-69, jan. 2010.
- DIAS, Cláudia. Segurança e Auditoria da Tecnologia da Informação. Axcel Books. Rio de Janeiro, 2000.