Segurança no processo *ETL*

Pretende-se incorporar no processo ETL de um sistema de Data WareHouse garantias de segurança oferecidas pelas técnicas criptográficas estudadas.

- O processo *ETL* envolve a comunicação entre diferentes componentes;
- Aspectos de autenticidade e confidencialidade devem assim ser avaliados nesse contexto.
- Pretende-se então:
  - Analisar os problemas de segurança que se poderão colocar no processo *ETL*;
  - Propor uma solução que responda aos problemas de segurança identificados;
  - (?) Implementar a solução proposta.

Aspectos de Segurança em Sistemas DW

According to a recent survey conducted by CSO Magazine, two-thirds of respondents said their company did not have a well-defined company-wide security policy in place. Moreover, this survey found that employees have access to critical data when they don't necessarily need access. (Source: www.csoonline.com/csoresearch/report14.html)

- Sistemas de *Data WareHouse* agregam (por definição) volumes consideráveis de dados sobre os quais é legítimo considerar requisitos de segurança específicos (e.g. privacidade, anonimato, etc.)
- Pretende-se então analisar um determinado cenário de *Data WareHouse* onde se coloquem aspectos de segurança
  - Identificar cenário (e.g. domínio médico/hospitalar; salvaguarda de privacidade em sistemas de retalho; ...).
  - Analisar os requisitos e eventuais problemas de segurança que se colocam no cenário escolhido.
  - Identificar técnicas criptográficas aplicáveis e as dificuldades encontradas.

RSA OAEP

*O RSA, como qualquer cifra determinística, não satisfaz os requisitos de segurança mais exigentes. Com este trabalho pretende-se realizar um **tutorial** que apresente o esquema RSA-OAEP — uma variante do RSA que pode ser demonstrada segura para noções de segurança mais exigentes.*

- Quais os problemas associados ao esque ma original (modelos de segurança “semântica”).
- Apresentar o esquema RSA-OAEP;
- ...e as propriedades de segurança associadas.
- Referências:
  - Wikipedia/Google...
  - Especificação - `ftp://ftp.rsasecurity.com/pub/rsalabs/rsa_algorithm/rsa-oaep_spec.pdf`
  - Sobre a segurança - `http://www.rsa.com/rsalabs/node.asp?id=2147`

Modelo de Segurança para Cifras

A segurança de técnicas criptográficas é estabelecida por intermédio de uma redução: mostra-se que, se for possível quebrar a cifra, seria igualmente possível resolver um problema que se acredita intratável. Neste trabalho pretende-se realizar um ***tutorial*** *que mostre como pode ser demonstrada a segurança da técnica El-Gamal.*

- Apresentar as noções de segurança semânticas (jogos, probabilidades, etc.)
- Assunpções de segurança.
- Transformações de jogos e reduções;
- Prova da segurança do *El-Gamal*.
- Referências:
  - Acetatos do Prof. Manuel Barbosa - `http://wiki.di.uminho.pt/cripto/mygames.pdf`

Cifra *One-Time Pad*

A cifra One-Time Pad é uma cifra incondicionalmente segura. Este trabalho consiste num ***tutorial*** *que explique o significado da frase apresentado.*

- Noção de *entropia* e conceitos associados;
- Noção de segurança incondicional;
- Demonstração de segurança da cifra;
- Discussão do resultado.
- Referências:
  - Acetatos disponibilizados;
  - Wikipedia, Google, ...

Cifras Clássicas I

As cifras utilizadas na antiguidade constituem excelentes exemplos da necessidade de formalização e rigor matemático no estudo da criptografia.

- Apresentar e classificar algumas das cifras utilizadas;
- Ilustrar ataque a uma cifra escolhida;
- Mostrar conceitos relevantes (e.g. idempotência, produto de cifras, substituição/permutação).
- Referências:
  - Acetatos disponibilizados;
  - Web...

Cifras Clássicas II

As máquinas de cifra, utilizadas durante a segunda grande guerra, exibiam já um elevado grau de sofisticação. A sua cripto-análise constitui um importante desafio para a comunidade cientifica da época.

- Apresentação da máquina de cifra *Enigma*.
- Aspectos da sua utilização e principais desafios colocados à sua cripto-análise.
- Quais as vulnerabilidades exploradas para a quebrar.
- Referências:
  - Web (Wikipedia, Google)
  - `http://www.codesandciphers.org.uk/enigma/index.htm`

JCA/JCE

*O framework Java Cryptography Architecture/Java Cryptography Extension disponibilizam, para a linguagem Java, suporte ao desenvolvimento de Software Criptográfico. Neste **tutorial** ilustra-se a utilização desse framework no desenvolvimento de uma pequena aplicação.*

- Apresentação da JCA/JCE (objectivos, arquitectura, *providers*, ...)
- Serviços disponibilizados (*engine classes*)
- Exemplos de utilização
- Discussão (pontos fortes, pontos fracos, ...)
- Referências:
  - *Sun*...
  - `http://wiki.di.uminho.pt/twiki/bin/view/Education/Criptografia/CriptografiaAplicadaTP`

Segurança em Web-Services

Os Web Services dão suporte à computação distribuída. Estão, por isso, expostos aos problemas de segurança inerentes aos ambientes de execução não controlados. Neste projecto pretende-se estudar os problemas de segurança associados a esses serviços e as propostas actuais para ultrapassar esses problemas.

- Os problemas de segurança em *Web-Services*; Soluções *ad-hoc* para o problema (quais são, o que resolvem, limitações).
- *WSS* - Objectivos, mecanismos disponibilizados, *Security Tokens*.
- Standards relacionados.
- Discussão (?é mesmo necessário?, suporte das plataformas de desenvolvimento, vantagens/desvantagens, ...)
- Referências:
  - `http://www-128.ibm.com/developerworks/library/specification/ws-secure/`
  - `http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss`
  - `http://www.xml.com/pub/a/ws/2003/03/04/security.html?page=1`

Criptografia em Curvas Elípticas

- Bases matemáticas...
- Ilustração do conceito.
- Curvas elípticas em corpos finitos.
- Exemplo de técnica criptográfica.
- Discussão (vantagens/desvantagens; domínios de aplicação; etc.)
- Referências:
  - Wikipedia, google
  - `http://www.peterindia.net/ECCLinks.html` (muitos *links* desactualizados...)
  - `http://www.certicom.com/index.php?action=ecc_tutorial,home`

Assinaturas para um Arquivo Digital

Num arquivo digital, como em qualquer repositório de informação, são pertinentes questões de segurança como: garantias de integridade, autenticidade, controlo de acesso à informação, etc. Pretende-se realizar uma análise de requisitos para uma solução baseada nas técnicas criptográficas que permitam dar resposta às questões levantadas.

- Quais as propriedades de segurança relevantes (integridade, autenticidade, confidencialidade, ...)?
- Quais os pressupostos de confiança do sistema? É para certificar documentos armazenados no arquivo ou as cópias desses documentos? (ou ambos...?)
- Que tecnologias são relevantes no projecto?
- Propostas para a realização do projecto (escolha de pacotes de Software, etc.)

Algoritmos *Data Minning* para cripto-análise

A identificação de padrões é um recurso típico em técnicas de cripto-análise. ??? Podem algoritmos e/ou técnicas oriundas da área de Data Minning ser exploradas com sucesso na cripto-análise de uma cifra???

- Trabalho assumidamente "especulativo" (pelo menos da minha parte...).
- Como tal, é necessário estar preparado para resultados "pela negativa" :-(.
- Deverá ser prudente focar num problema de cripto-análise pequeno, onde o problema da identificação de padrões seja evidente (e.g. Vigenère).

Dinheiro Digital

A conceptualização de um análogo digital do dinheiro coloca desafios consideráveis pela grande diversidade de requisitos impostos (muitos deles contraditórios). A par dos protocolos de eleições electrónicas, constituem domínios privilegiados para aplicação de técnicas e protocolos criptográficos elaborados.

- Identificação do problema: quais as propriedades desejaveis.
- Exemplificação de um protocolo de *Digital Cash*.
- Discussão: riscos de utilização; o dinheiro electrónico “na prática”; etc.
- Referências:
  - Web...
  - *Applied Cryptography*, Bruce Schneier, John Wiley & Sons, Inc. (pag. 139–147)