Segurança de Redes e Sistemas de Computadores
2016/2017, 2º Semestre

Aula Prática (LAB 3)

Exercícios de programação usando:

- **Geração de chaves criptográficas para algoritmos criptográficos simétricos**
- **Password-Based Encryption**
- **Keystores para armazenamento e gestão de chaves criptográficas simétricas**

Para os próximos pontos, comece por obter o arquivo lab3.tgz. Abra o arquivo de modo a obter o material que lhe é fornecido.

---

1. Geração de chaves criptográficas para algoritmos criptográficos simétricos

No arquivo preparado para a aula prática ver o código da diretoria
Keygeneration

A partir do código base (ver **KeyGeneratorExample.java**) verificar o funcionamento e treinar o uso de geradores de chaves para algoritmos criptográfico simétricos.

---

2. Password Based Encryption

No arquivo preparado para a aula prática ver o código da diretoria

pbencryption

Ser-lhe-á feita uma apresentação sobre os esquemas de cifra com passwords, a sua utilização e os seus princípios de funcionamento. Deverá seguir essa apresentação (que pode aceder em documento PDF que também encontra no arquivo lab3. De seguida deverá praticar os exemplos e exercícios sugeridos na aula, a partir do código inicialmente disponibilizado, verificando bem as diferenças de utilização prática.

PBEWithParamsExample.java
PBEWithoutParamsExample.java
BEOtherExample.java

Com base nas implementações de esquemas do tipo PBE que possui, deve verificar que é possível usar qualquer implementação normalizada deste tipo de algoritmos e esquemas criptográficos que encontra nos diversos provedores criptográficos para a JCE.

---

3. Keystores para armazenamento de chaves criptográficas para algoritmos simétricos

Ser-lhe-á feita uma demonstração do uso de Keystores (normalizadas para Java) e que têm em vista sistematizar e normalizar o processo de gestão de chaves secretas para criptografia simétrica. Para este efeito:

a) Ser-lhe-á mostrado como utilizar a ferramenta keytool (ou outras ferramentas congéneres), bem como os aspeto relativos às diversas opções para geração de chaves criptográficas bem como seu armazenamento em keystores.

b) A seguir irá compreender a estrutura interna dos objectos "keystore", nomeadamente keystores do tipo JCEKS, bem como pode manipular esses objetos no contexto de programas JAVA que usam o suporte JCA/JCE.

Desafios (trabalho de casa)

Exercício (para programar)
A partir dos exercícios dos desafios lançados no LAB-1 (*challenges*) tente agora iterar esses desafios que visavam proteger mensagens no canal com propriedades de CONFIDENCIALIDADE E INTEGRIDADE, usando MACs, mas fazendo agora a gestão das chaves (chaves de confidencialidade e chaves MAC) em keystores. Para tal, dependendo do exercício que considerou:

- Para a aplicação C/S CAPITALIZATION, a informação da keystore deverá estar partilhada entre cliente e o servidor.

- Para a aplicação MCHAT (Multicast Chat), a keystore deverá estar partilhada entre todos os utilizadores (endpoints) da sessão de multicasting-chat.

Note que a proteção de cada keystore pode ser feita com diferentes passwords, de modo a "personalizar" a distribuição do conteúdo das keystores, no primeiro caso pelo cliente e servidor, no segundo caso pelos vários utilizadores das sessões de multicasting/chat. Note que neste último caso, diferentes CHAT-SESSIONS (definidas combase em diferentes endereçso Multicast), podem ter diferentes keystores.