Work in progress)

Desenvolvimento de uma ferramenta criptográfica

Objetivo

Desenvolver uma aplicação, que faça uso de alguns dos algoritmos, mecanismos ou protocolos de segurança mais comuns. Assim, através da utilização de um conjunto de APIs de segurança, o aluno deverá explorar uma variedade de serviços criptográficos incluindo assinaturas digitais, message digest, cifras (simétricas, assimétricas, stream e block), message authentication code (MAC), algoritmos padrão (RSA, AES, SHA-2, entre outros) e comunicações seguras.

Proposta de temas

Desenvolver uma aplicação que permita realizar a seguintes operações:

- Juntar vários ficheiros num só ficheiro (semelhante ao tar)
- Garantir a confidencialidade dos dados
- Garantir a autenticação da fonte
- Garantir a integridade da informação

Notas

- Apenas podem ser utilizadas as bibliotecas "base" que fazem parte da linguagem de programação. A utilização de bibliotecas de terceiros requer autorização do docente
- Não são permitidas ferramentas externas, tais como a invocação direta de programas através de algum método de invocação fornecido por uma qualquer linguagem de programação

Ferramentas

Java

A segurança na plataforma Java é fornecida através de um conjunto de bibliotecas: JCE, JAAS, JSSE, JAC, entre outras.

- A tecnologia de segurança Java inclui um conjunto de APIs, ferramentas e implementações de algoritmos, mecanismos e protocolos de segurança mais usados. Estas APIs abrangem uma

ampla variedade de áreas, incluindo criptografia, infraestrutura de chave pública, comunicação segura, autenticação e controle de acesso. A tecnologia de segurança Java fornece aos programadores uma estrutura de segurança abrangente para codificar aplicações, e aos utilizadores e administradores um conjunto de ferramentas para gerir aplicativos com a segurança necessária

- Java Cryptography Extension (JCE) - https://www.oracle.com/pt/java/technologies/javase-jce8-downloads.html
- Java Authentication and Authorization Service (JAAS) - https://docs.oracle.com/javase/8/docs/technotes/guides/security/jaas/JAASRefGuide.html
- Java Secure Sockets Extension (JSSE) - https://docs.oracle.com/javase/9/security/java-secure-socket-extension-jsse-reference-guide.htm

.NET

A segurança na plataforma .NET, é fornecida pelas classes no namespace System.Security.Cryptography:

- O .NET fornece um conjunto de objetos criptográficos, suportando alguns dos algoritmos mais conhecidos, incluindo hash, criptografia e geração de assinaturas digitais. Esses objetos permitem incorporar recursos básicos em operações mais complexas, como assinar e cifrar um documento. Estes objetos criptográficos são usados pelo .NET tanto para serviços internos, como para os programadores que precisam de suporte criptográfico. Alguns das bibliotecas mais conhecidas oferecem funções como cifragem por fluxo, assinaturas digitais, hashing e geração de números aleatórios, entre outros.