E-fólio A | Instruções para a realização do E-fólio

SEGURANÇA EM REDES E COMPUTADORES | 21181

Período de Realização

Decorre de 2 de novembro a 25 de novembro de 2022

Data de Limite de Entrega

25 de novembro de 2022, até às 23:59 de Portugal Continental

Temática / Tema / Conteúdos

Métodos criptográficos para a comunicação de informação.

Objetivos

Deve demonstrar:

- Conhecer e compreender as diferentes técnicas criptográficas;
- Compreender a criptografia simétrica e os seus problemas;
- Demonstrar ter um bom entendimento genérico sobre a criptografia assimétrica.

Trabalho a desenvolver

O trabalho a desenvolver consiste na implementação de um algoritmo de cifra simétrica, outro de cifra assimétrica, à vossa escolha. Tal pode ser feito em 2 programas independentes ou optarem por fazer tudo no mesmo programa.

Tem de permitir a introdução de um texto em claro por digitação do mesmo (podem limitar a respetiva dimensão) e mostrar o mesmo após cifra. Tem de ser possível guardar as chaves de cifra, de modo a podermos reverter o processo, ou seja, obter o texto em claro a partir do texto cifrado.

A linguagem de programação a utilizar é à vossa escolha, de entre o seguinte leque: Java, C, C++ ou Python. Em último caso, podem até recorrer ao Excel para o efeito.

O trabalho é entregue num zip, onde colocarão: o(s) ficheiro(s) com o código-fonte (txt), o executável correspondente e um relatório (word ou pdf) onde explicam os algoritmos de cifra escolhidos, detalhando os mesmos, e onde justificam as vossas opções.

Notem que, se se limitarem a fazer reutilização das bibliotecas criptográficas disponíveis para as linguagens acima referidas, então devem aproveitar para explicar com grande nível de detalhe como funciona(m) o(s) algoritmo(s) de cifra implementado(s).

Algumas notas: - Atenção à estrutura do documento e respetivo conteúdo; - Atenção ao nível do português utilizado; - Atenção às referências bibliográficas; - Atenção aos erros ortográficos; - Atenção à reutilização de código obtido diretamente na web (nota: eu também conheço essas fontes!); - Atenção às "reutilizações" de textos de livros, artigos ou outros trabalhos. Plágios serão penalizados!

Recursos

Utilize os recursos à sua disposição, nomeadamente:

1. Editor de código que utilize habitualmente
2. Fórum de discussão do tópico 2 e fórum específico do eFolio A
3. Manual recomendado

Critérios de avaliação e cotação

Na avaliação do trabalho serão tidos em consideração os seguintes critérios e cotações:

1. Se código funcionar corretamente = 0,5 valores.
2. Se algoritmo selecionado estiver corretamente implementado (nota: o código pode funcionar, mas o algoritmo de cifra estar mal implementado!) = 1,0 valor.
3. Qualidade do conteúdo do relatório, quer em termos técnicos, quer em termos de justificação das opções tomadas = 1,0 valor.

   Notem que os pontos 1. e 2. repetem-se para cada um dos algoritmos pedidos.

Total: 4 pontos = 4 valores

Normas a respeitar

Deve redigir o seu relatório na Folha de Resolução disponibilizada na turma e preencher todos os dados do cabeçalho.

Todas as páginas do documento devem ser numeradas.

O seu relatório não deve ultrapassar 4 páginas A4 (excluindo a folha de rosto) redigidas em Arial, tamanho de letra 11. O espaçamento entre linhas deve corresponder a 1,5 linhas.

Nomeie o ficheiro com o seu número de estudante, seguido da identificação do E-fólio, segundo o exemplo apresentado: 000000efolioA.

Deve carregar os ficheiros para a plataforma no dispositivo E-fólio A até à data e hora limite de entrega. Evite a entrega próximo da hora limite para se

precaver contra eventuais problemas. O ficheiro a enviar não deve exceder 8 MB.

Votos de bom trabalho!

Henrique S. Mamede