# 1. Codifique em Python, C# ou Java uma aplicação cliente/servidor onde o cliente deve enviar um arquivo de tamanho razoável ao servidor. O arquivo deve estar protegido de bisbilhoteiros. (3,0)

# Descrição da aplicação: O cliente envia uma mensagem ao servidor requisitando uma troca de chaves para proteger o envio do documento. O servidor gera um par de chaves usando criptografia de chave pública e envia a chave pública ao cliente. O cliente então gera uma versão protegida do arquivo usando uma chave privada e protege a chave privada usando a chave pública fornecida pelo servidor. O cliente em seguida envia um pacote ao servidor contendo a chave e o arquivo em questão. O servidor ao receber o pacote deve conseguir ler o arquivo sem dificuldades.

**2. Codifique em Python, C# ou Java uma aplicação que, dado um arquivo qualquer, realize buscas por esse arquivo em um diretório cheio de arquivos, objetivando encontrar arquivos repetidos. Porém, esse processo deve se dar de forma mais eficiente, contrariando a comparação por conteúdo dos arquivos. Mostre através da aplicação em execução que a técnica utilizada foi, ou não foi, mais eficiente que a comparação dos arquivos por conteúdo. (2,0)**

# Descrição da aplicação: Construa uma aplicação que realize uma comparação de todos arquivos em um diretório com o arquivo previamente selecionado. A escolha da técnica de comparação por conteúdo é livre. Calcule o HASH do arquivo pesquisado. Calcule o HASH de todos os arquivos em um diretório e armazene esses dados em uma estrutura. Realiza uma busca utilizando as duas técnicas e demonstre na aplicação funcional os resultados obtidos.

# Decifre o seguinte texto: (1,0)

SEESETTXPODOSEREEDICRFDAPOROMUTACEINACAMSIISPMELVSMASOEVSREETSOASEEPTRSO

Que técnica de criptografia foi usada?

**4. Descreva autenticação e autorização. Justifique por que utilizar autenticação multifator? Dê 2 exemplos. (0,5)**

**5. Em um cenário de simulação de uma conexão (spoofing de autenticação) de cookie, utiliza-se a ferramenta BurpSuite para interceptar o trafego através de umaconfiguração de proxy. São analisados os conteúdos das seguintes interceptações: (1,5)**

**Login rafael, senharafael:**

GET /WebGoat/attack? HTTP/1.1

Host: 10.10.10.17

User-Agent: Mozilla/5.0 (X11; Linux i686; rv:31.0)

Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,

\*/\*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer:

http://10.10.10.17/WebGoat/attack?Screen=73&menu=1800

Cookie: AuthCookie=04764jcydyp;

JSESSIONID=78CD3A990F37AC910FADAC44FCB8DD13;

acopendivids=swingset,jotto,phpbb2,redmine;

acgroupswithpersist=nada

Authorization: Basic Z3Vlc3Q6Z3Vlc3Q=

Connection: keep-alive

**Login raquel, senharaquel:**

GET /WebGoat/attack?WACLogout=true HTTP/1.1

Host: 10.10.10.17

User-Agent: Mozilla/5.0 (X11; Linux i686; rv:31.0)

Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,

\*/\*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer:

http://10.10.10.17/WebGoat/attack?Screen=73&menu=1800

Cookie: AuthCookie=04764jcseyp;

JSESSIONID=78CD3A990F37AC910FADAC44FCB8DD13;

acopendivids=swingset,jotto,phpbb2,redmine;

acgroupswithpersist=nada

Authorization: Basic Z3Vlc3Q6Z3Vlc3Q=

Connection: keep-alive

**6. Explique a diferença entre o ataque de XSS persistente e o não persistente. Para que são usados CAPTCHA's e quais as premissas para sua criação? (0,5)**

**7. Descreva a vulnerabilidade Cross-Site RequestForgery (CSRF), seus vetores de ataque, como se prevenir e demonstre esse tipo de ataque através de um cenário de exemplo. (1,0)**

**8. Descreva o problema da exposição de dados sensíveis, quais vetores de ataque, como se prevenir e exemplifique utilizando um cenário de ataque. (1,0)**

**9. Descreva dois problemas fundamentais dos algoritmos de HASH MD5. Um desses problemas exige uma explicação mais elaborada, identifique o problema e forneça essa descrição mais aprofundada. (1,0)**

**10. O perfeito conceito de acesso em segurança leva em consideração três elementos. Cite, descreva e exemplifique cada um deles. (0,5)**