P.PORTO ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO	Tipo de Prova Mini-teste	Ano letivo 1º	Data 09-06-2022
	Curso Licenciatura em Segurança Informática em Redes de Computadores		Hora 13h00
	Unidade Curricular Segurança Informática		Duração 01h10

Observações
- Com consulta de documentação própria.
- A cotação atribuída a cada pergunta é apresentada entre parêntesis retos.
- O tempo previsto para responder a cada questão é apresentado entre parêntesis retos.

1) [5 min] **(2,5 valores)**

Classifique cada um dos seguintes mecanismos, em termos de medidas para garantir Confidencialidade (C), Integridade (I), Disponibilidade (D), ou combinação de várias.

Nota: à seleção de uma resposta incorreta é descontado 50% do valor atribuído à questão

a) Mecanismo de permissões/controlo de acesso a diretorias e ficheiros (0,5 valores)
b) Mecanismos de cifra irreversível SHA-512 (0,5 valores)
c) Mecanismo de cifra reversível AES-CBC (0,5 valores)
d) Mecanismo de backup (0,5 valores)
e) Mecanismo Apparmor (0,5 valores)

2) [10 min] **(3,5 valores)**

A Alice pretende comunicar com o Bob. Para isso, admitamos que **(E_A , D_A) e (E_B, D_B) são os pares de chaves pública-privada** de Alice e Bob, respetivamente. **Enc e Dec são os processos de cifra e decifra, respetivamente**. Se necessário, Alice e Bob têm acesso a uma **função de hash H** (e.g., SHA-512).

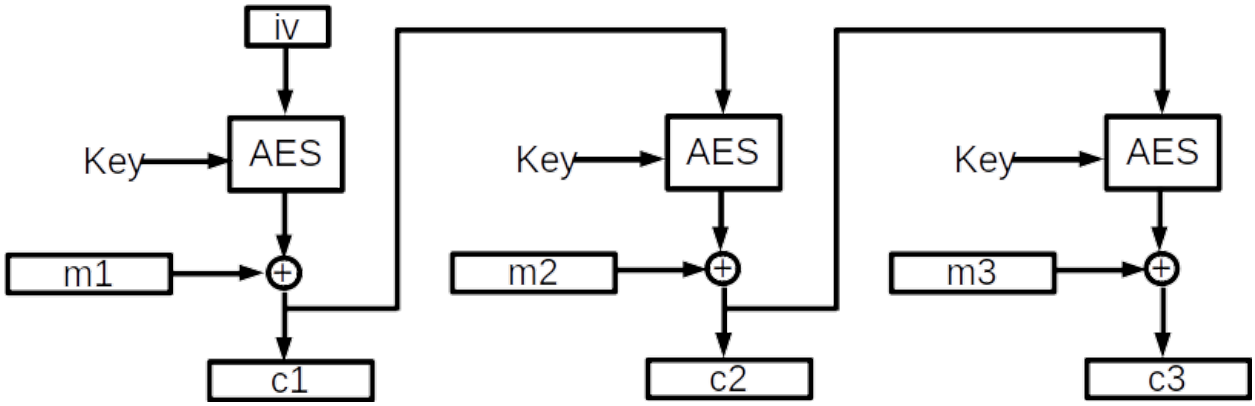
A título de exemplo, ficam algumas expressões:
- cifrar uma mensagem M com a chave E_A: Enc(E_A, M)
- criar um resumo da mensagem M: H(M)

A Alice pretende enviar uma **mensagem M** ao Bob. Indique a expressão de cifra que permita:

a) O envio da mensagem M, garantindo apenas confidencialidade (1,0 valores)
b) O envio da mensagem M, garantindo apenas integridade (1,0 valores)
c) Admita que o Bob pretende responder à Alice, apenas assinando digitalmente a sua mensagem de resposta. Indique a expressão correta. (1,5 valores)

3) [15 min] **(4,0 valores)**

Considere uma mensagem m, divisível em blocos de mensagens m1, m2, m3. A cifra AES, usando o modo CFB, é aplicada de forma a obter o par cifrado c (i.e. c1, c2 e c3). O processo de cifra é apresentado na imagem seguinte.



Na imagem, ivector representa o vetor inicial e ⊕ é a operação XOR.

a) Escreva as **expressões** para os processos de cifração AES, que permitem obter cada um dos blocos de mensagens c1, c2, e c3 (1,0 valores)
b) Considere que o bloco de texto c2 chega corrompido ao recetor. Será possível obter os blocos de mensagens m1, m2, e m3? Justifique de forma clara e sucinta (2,0 valores)
c) Escreva a **expressão** de decifra para o bloco c1, usado a simbologia presente na imagem (c1, m1, key, ⊕, etc.). (1,0 valores)

4) [10 min] **(3,0 valores)**

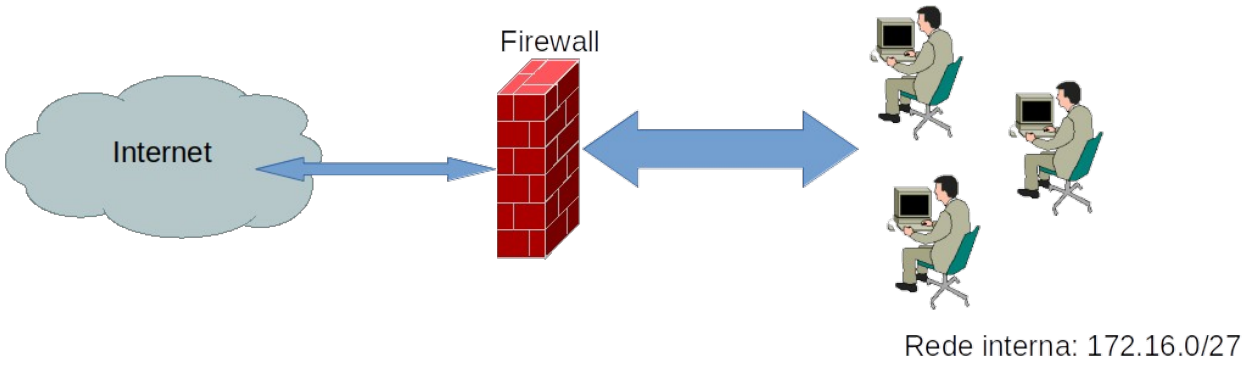
Explique por que o algoritmo Diffie Hellman (DH) é suscetível a ataque man-in-the-middle(mitm).. Que soluções existirão para tornar o DH seguro contra tal ataque e em que se baseiam?.

5) [15 min] **(4,0 valores)**

Considere que no seu novo local de trabalho se depara com uma equipa de profissionais que usa o SSH para aceder remotamente a um conjunto de servidores que correm as aplicações de vendas da empresa. A autenticação SSH dos utilizadores é feita recorrendo a senhas. Explique por que esta não é a solução mais adequada. Sugira alternativa(s) de autenticação (mútua?), indicando o que seria necessário para a(s) implementar.

6) [5 min] **(3,0 valores)**

Considere o cenário de uma rede de uma empresa de pequena dimensão, com acesso à Internet protegido por uma firewall (computador Linux + netfilter + iptables):



Defina regras iptables que permitam responder às seguintes políticas:

a) Um datagrama é descartado quando não se enquadra nas regras já definidas nas chains INPUT, OUTPUT e FORWARD (1,0 valores)
b) O endereço IP de origem para qualquer datagrama, com proveniência de um qualquer dispositivo da rede interna, com destino o endereço IP 8.8.8.8 exterior à rede, deve ser alterado para 193.139.93.1 (2,0 valores)