Mark: 9.5/20 (total score: 14.1/30)

+267/1/24+

Fundamentos de Segurança Informática **LEIC**
14/11/2023 **Duração: 1H** **Final**

Este é um teste de escolha múltipla que será corrigido automáticamente. Siga por favor as regras:

- Não utilize lápis ou cores leves. Marque a sua resposta utilizando apenas caneta **azul** e **preta**.
- Rasuras não são detectadas automaticamente. Marque apenas caixas, sendo generoso na tinta.
- Pode sublinhar texto ou tirar notas nas margens. Apenas as caixas importam para a correção.

O teste está cotado para 20 pontos. Cada pergunta vale 20/30 pontos.

Há 30 perguntas no total, cada uma com 4 opções. **Apenas uma destas opções é aceite como correta, podendo esta opção indicar que todas as opções estão corretas.**

Pode marcar uma ou duas escolhas por questão. A cotação é atribuida da seguinte forma:

- Uma resposta correta marcada (100%).
- Uma resposta incorreta marcada (-20%).
- Nenhuma resposta marcada (0%).
- Duas resp. marcadas, uma correta (50%).
- Duas resp. marcadas, zero corretas (-20%).
- Mais do que duas resp. marcadas (-20%).

☐0	■0	☐0	■0	■0	☐0	☐0	☐0	☐0
☐1	☐1	☐1	☐1	☐1	☐1	☐1	☐1	☐1
■2	☐2	■2	☐2	☐2	☐2	☐2	☐2	☐2
☐3	☐3	☐3	☐3	☐3	☐3	☐3	☐3	☐3
☐4	☐4	☐4	☐4	☐4	■4	☐4	■4	☐4
☐5	☐5	☐5	☐5	☐5	☐5	☐5	☐5	☐5
☐6	☐6	☐6	☐6	☐6	☐6	☐6	☐6	■6
☐7	☐7	☐7	☐7	☐7	☐7	☐7	☐7	☐7
☐8	☐8	☐8	☐8	☐8	☐8	☐8	☐8	☐8
☐9	☐9	☐9	☐9	☐9	☐9	■9	☐9	☐9

← Codifique o seu número de estudante de 9 dígitos upYYYYXXXXX horizontalmente na grelha à esquerda. Escreva também o seu número de estudante e o primeiro e último nomes em baixo.

Número de estudante:

up | 2 | 0 | 2 | 0 | 0 | 4 | 9 | 4 | 6 |

Primeiro e ùltimo Nome:

Daniela Tomás

Grupo 1 Criptografia *(10 questões)*

Questão 1.1 ♣ Suponha um cenário em que A envia para B (pk, m, σ) em que m é uma mensagem e $\sigma = Sig(sk, m)$ é uma assinatura digital (segura) de m. Um atacante Man-In-The-Middle (MitM) poderia convencer um destinatário B de que A enviou $m' \neq m$.

-0.2/1

- [x] Convencendo B de que que A é dono de outra chave pública diferente de pk.
- [ ] Mantendo pk, substituindo a mensagem m por m' e gerando uma outra assinatura σ'.
- [■] Não é possível realizar ataques MitM quando se usam assinaturas.
- [ ] Mantendo pk, e substituindo o par (m, σ) por (m', σ).

Assinatura → autenticidade / integridade
→ não repúdio

Questão 1.2 ♣ Qual atribuição para (A) assinaturaRSA, (B) AES-CTR, (C) RSA-OAEP e (D) HMAC está correta?

	Confidencialidade	Autenticidade
Simétrica	(1)	(2)
Assimétrica	(3)	(4)

1/1

☐ 1-A;2-C;3-B;4-D. ☐ 1-A;2-B;3-C;4-D. ☐ 1-C;2-A;3-D;4-B. ☒ 1-B;2-D;3-C;4-A.

Questão 1.3 ♣ Num KDS, um Key Distribution Center interage com N agentes e:

-0.2/1

☐ Armazena de forma permanente um número variável de chaves de sessão, que vão sendo fornecidas pelos participantes.

☒ Armazena 1 chave de longa duração que utiliza para estabelecer um número arbitrário de chaves de sessão.

☒ Armazena N chaves de longa duração que utiliza para estabelecer um número arbitrário de chaves de sessão.

☐ Armazena $N*(N-1)/2$ chaves de longa duração que disponibiliza quando são necessárias para comunicação.

Questão 1.4 ♣ A diferença entre uma cifra simétrica autenticada (AE) e uma cifra simétrica autenticada com dados associados (AEAD) é que:

1/1

☐ O AEAD permite gerar chaves com dados associados.

☐ AEAD garante confidencialidade de dados associados e AE não.

☐ AEAD é probabilística e AE é deterministica.

☒ AEAD permite vincular metadados públicos a um criptograma e AE não.

Questão 1.5 ♣ O modo de operação Electronic Code Book é:

1/1

☒ Uma construção insegura de uma cifra simétrica a partir de uma cifra de blocos.

☐ Uma construção insegura de um MAC a partir de uma cifra por blocos.

☐ Uma construção segura de uma cifra simétrica a partir de uma cifra de blocos.

☐ Uma construção segura de um MAC a partir de uma cifra por blocos.

Questão 1.6 ♣ A afirmação "*Criptografia de chave pública tornou criptografia simétrica obsoleta*" é:

-0.2/1

☒ Verdadeira, mas apenas em aplicações onde não se pode ter uma chave pré-partilhada.

☐ Falsa: se não houver PKI, é obrigatório utilizar criptografia simétrica.

☒ Falsa: as duas técnicas são sempre usadas em conjunto por questões de performance.

☒ Verdadeira, excepto aplicações onde se pretende segurança contra computadores quânticos.

Questão 1.7 ♣ A propriedade de não repúdio é importante no contexto da autenticação de mensagens. Qual destas frases é verdadeira? Note que MAC denota Message Authentication Code.

1/1

☐ As cifras assimétricas garantem esta propriedade desde que a chave pública seja autêntica.

☒ Um MAC não garante esta propriedade.

☐ Um MAC garante esta propriedade, desde que se confie no emissor.

☐ As assinaturas digitais garantem esta propriedade, mesmo depois de ser comprometida a chave secreta de longa duração.

Questão 1.8 ♣ A propriedade de Perfect Forward Secrecy garante que:

1/1

☐ Corromper uma chave de longa duração não deve corromper sessões futuras.

☐ Corromper uma chave de sessão não deve corromper sessões futuras.

☒ Corromper uma chave de longa duração não deve corromper sessões passadas.

☐ Corromper uma chave de sessão não deve corromper sessões passadas.

Questão 1.9 ♣ Recorde que um Message Authentication Code (MAC) tem a seguinte sintaxe $\mathsf{MAC}(k, m) = t$. Um MAC garante:

1/1

- ☐ Confidencialidade, integridade e autenticidade de uma sequência de mensagens.
- ☐ Confidencialidade, integridade e autenticidade de uma mensagem.
- ☒ Integridade e autenticidade de uma mensagem.
- ☐ Integridade e autenticidade de uma sequência de mensagens.

Questão 1.10 ♣ Uma construção comum de cifra simétrica segura é da forma $\mathsf{Enc}(k, n, m) = \mathsf{PRG}(k, n) \oplus m$. A seguinte propriedade demonstra que esta cifra **não** garante integridade:

1/1

- ☐ A operação XOR cancela: $\mathsf{PRG}(k, n) \oplus \mathsf{PRG}(k, n) \oplus m = m$.
- ☐ O gerador PRG produz uma distribuição uniforme.
- ☐ O gerador PRG não produz uma distribuição uniforme.
- ☒ Alterar um bit no criptograma altera um bit na mensagem recuperada.

Grupo 2 Infraestrutura de Chave Pública *(5 questões)*

Questão 2.1 ♣ Quando se utilizam certificados de chave pública para transferir informação cifrada com uma cifra assimétrica de A para B:

0/1

- ☒ A tem de conhecer e validar a priori o certificado de B.
- ☐ B tem de conhecer e validar a priori o certificado de A.
- ☐ A e B têm de trocar e validar certificados a priori.
- ☐ A e B têm de ter certificados emitidos pela mesma Autoridade de Certificação.

Questão 2.2 ♣ Para uma autoridade de certificação, uma Certificate Revocation List (CRL)

1/1

- ☐ Contém todos os certificados emitidos que podem ser utilizados.
- ☐ Contém todos os certificados emitidos que não devem ser utilizados.
- ☒ Contém todos os certificados emitidos, ainda dentro do período de validade, que não devem ser utilizados.
- ☐ Contém apenas certificados emitidos que estão dentro do período de validade e podem ser utilizados.

Questão 2.3 ♣ Qual é o canal mais comum para que um utilizador obtenha informação sobre as Autoridades de Certificação que funcionam como âncoras/raízes nas relações de confiança de uma PKI?

1/1

- ☐ Os seus certificados são fornecidos pelos websites que visitam.
- ☐ Apenas obtêm essa informação quando compram um certificado pessoal.
- ☒ Os seus certificados vêm instalados nos sistemas operativos ou browsers.
- ☐ Apenas obtêm essa informação quando compram um certificado para um servidor.

Questão 2.4 ♣ A infra-estrutura de chave pública vem resolver o seguinte problema fundamental:

1/1

- ☐ A partilha de chaves secretas simétricas usando chaves públicas.
- ☐ A autenticação e confidencialidade de chaves públicas.
- ☒ A autenticação de chaves públicas.
- ☐ A partilha de chaves secretas assimétricas

Questão 2.5 ♣ Recorde o que estudou sobre cadeias de certificação. Suponha que a autoridade de certificação A assina o certificado da autoridade de certificação B, e que a única informação que tem sobre as autoridades de certificação A e B é o que está escrito neste certificado.

0/1

- [x] A confiança em B não pode ser maior que a confiança em A.
- [ ] A confiança em A não pode ser maior que a confiança em B.
- [ ] B não pode funcionar enquanto não assinar o certificado de A.
- [ ] A confia em B para assinar o certificado de A.

Grupo 3 Autenticação *(4 questões)*

Questão 3.1 ♣ Qual a principal diferença entre *autenticação de origem de mensagens* (MA) e *autenticação de entidades* (EA)?

0.5/1

- [x] Na EA o destinatário tem a garantia que a mensagem foi enviada por uma entidade específica, ao passo que na autenticação de origem de mensagens o destinatário apenas sabe que a mensagem enviada é válida.
- [ ] Um mecanismo de EA requer a utilização de um mecanismo de MA, mas não vice-versa.
- [x] Na EA, pretende-se verificar que a entidade participa em tempo real num protocolo.
- [ ] Na MA existe tipicamente um requisito que a mensagem foi enviada recentemente, pela entidade correta.

Questão 3.2 ♣ Qual destes **não** é um ataque a um mecanismo de autenticação baseado em passwords?

1/1

- [ ] Data breach num servidor releva passwords de utilizadores.
- [ ] Malware regista keystrokes do utilizador.
- [x] Utilizador escolhe uma password fraca.
- [ ] Site de phishing rouba credenciais de utilizadores.

Questão 3.3 ♣ Qual **não** representa um risco de segurança para sistemas de autenticação biométrica?

0.5/1

- [ ] Forjar características de indivíduos.
- [ ] Roubar características de indivíduos.
- [x] Alta taxa de falsos negativos.
- [x] Alta taxa de falsos positivos.

Questão 3.4 ♣ Qual a melhor forma de uma aplicação web guardar tokens de sessão do lado do cliente?

1/1

- [ ] Em campos escondidos em formulários.
- [ ] Em cookies.
- [x] Uma combinação de todas as outras opções.
- [ ] No conteúdo de links.

Grupo 4 Segurança de Redes *(6 questões)*

Questão 4.1 ♣ Considere ataques ao sistema DNS. Qual das seguintes afirmações *não* é verdadeira?

-0.2/1

- [x] DNS cache poisoning é um ataque direcionado a um servidor DNS legítimo.
- [ ] Ambos DNS spoofing e DNS cache poisoning permitem direcionar utilizadores para máquinas maliciosas.
- [ ] DNS spoofing pode ser feito por malware diretamente na máquina do utilizador.
- [x] DNS spoofing consiste em inundar um servidor DNS com pedidos de registos de IPs.

Questão 4.2 ♣ Qual dos seguintes ataques aos protocolos UDP/TCP é mais difícil de realizar?

0/1

- ☐ Enviar mensagem de RST.
- ☐ UDP session hijacking.
- ☐ TCP session spoofing.
- ☒ TCP session hijacking.

Questão 4.3 ♣ No contexto de filtragem de pacotes de uma *firewall*, qual das seguintes afirmações é verdadeira?

0/1

- ☐ A filtragem de pacotes não distingue tráfico recebido de tráfico enviado.
- ☐ Uma política *Default allow* oferece tipicamente mais proteção que uma política *Default deny*.
- ☐ Filtragem sem estado tem a desvantagem de ser mais difícil de configurar excepções para utilizadores legítimos.
- ☒ Filtragem com estado tem a desvantagem de poder ser difícil de implementar.

Questão 4.4 ♣ Qual dos seguintes é um ataque ao nível da camada de transporte?

1/1

- ☐ DNS cache poisoning.
- ☒ TCP session hijacking.
- ☐ MAC flooding.
- ☐ Rogue DHCP.

Questão 4.5 ♣ Um MAC address identifica fisicamente uma máquina numa dada rede. Qual das seguintes afirmações **não** é verdadeira?

0/1

- ☐ Um ataque de MAC spoofing permite usurpar o MAC address de outra máquina.
- ☒ Um ataque de MAC flooding tenciona fazer Denial of Service de um switch.
- ☐ Um ataque de MAC flooding pode forçar um switch a fazer broadcast de todos os pacotes.
- ☐ Um ataque de MAC spoofing permite personificar um hub/router/switch.

Questão 4.6 ♣ Ao nível das comunicações de rede, qual das seguintes afirmações é verdadeira?

1/1

- ☐ Um atacante *eavesdropper* só não pode modificar pacotes.
- ☐ Um atacante *on-path* apenas pode enviar pacotes.
- ☒ Um atacante *man-in-the-middle* pode controlar todas as comunicações.
- ☐ Um atacante *off-path* apenas pode receber pacotes.

Grupo 5 Malware e Deteção *(3 questões)*

Questão 5.1 ♣ Qual das seguintes afirmações **não** é verdadeira?

0.5/1

- ☐ Um *worm* é um malware que se auto-propaga.
- ☐ Um *worm* pode ser utilizado para criar uma *botnet*.
- ☒ Um *worm* é um malware utilizado como "isco" para enganar utilizadores.
- ☒ Uma *botnet* é uma rede de computadores de malware com um controlo comum.

Questão 5.2 ♣ Qual **não** é uma estratégia que um *vírus* actual utiliza para evitar ser detectado?

-0.2/1

- ☒ Comportar-se de forma diferente quando é executado numa *sandbox*.
- ☒ Terminar os processos lançados pelo antivírus.
- ☐ Cifrar o seu código de maneira probabilística em cada infeção.
- ☐ Dissimular-se de ficheiros normais e mutar-se ao executar.

Questão 5.3 ♣ Em que consiste o conceito de deteção de malware baseado em assinaturas?

0/1

- [ ] Detectar assinaturas pessoais que hackers deixam no código do malware que criam.
- [ ] Identificar assinaturas digitais de servidores aos quais o malware tenta aceder.
- [x] Detectar padrões de ataques conhecidos.
- [ ] Assinar digitalmente o software para impedir que malware modifique a sua execução.

Grupo 6 Transport Layer Security (TLS) *(2 questões)*

Questão 6.1 ♣ Qual dos seguintes ataques é possível de evitar utilizando ligações TLS?

-0.2/1

- [x] Páginas web que incluem mixed content HTTP/HTTPS.
- [ ] Análise de tráfego de rede para obter metadados.
- [ ] DNS spoofing.
- [x] Ataques man-in-the-middle, desde que o cliente valide o certificado do servidor.

Questão 6.2 ♣ Qual a diferença do handshake do TLS 1.3 para versões anteriores?

-0.2/1

- [x] Corromper chave do servidor não afeta sessões passadas.
- [ ] Por questões de performance, as ligações não garantem sempre perfect forward secrecy.
- [ ] Não utiliza chaves de longa duração.
- [x] Utiliza transporte RSA em vez de Diffie-Hellman autenticado.