DI/FCT/UNL- Segurança de Redes e Sistemas de Computadores - 1º Sem, 2019/2020
Época de Exame, 17/Janeiro/2020

Exame de Recurso ou de Melhoria de Nota
Parte Sem Consulta

Questão 1

a) Vai usar-se um algoritmo criptográfico simétrico de cifra por blocos, que processa blocos fixos de 128 bits e usa uma chave de 168 bits. Utilizando-se o modo CBC para cifrar um ficheiro (*plaintext*) de 4096 bits e usando-se *padding* PKCS#5, qual vai ser o tamanho do ficheiro depois de cifrado (*ciphertext*)? Justifique.

b) As operações de cifra de um bloco em claro (*plaintext*) P para obter o correspondente bloco cifrado (*ciphertext*) C, quando se usa um algoritmo criptográfico simétrico em modo CTR, representa-se da seguinte forma.

C1 = P1 xor E(Counter$_0$), Ci = Pi xor E(Counter$_i$), sendo *Counter$_0$* o valor do contador inicial ou valor convertido do vetor de inicialização. *E( )* representa a função para cifrar.

Escreva a representação para a operação de decifra que permite obter P1 e Pi.

c) Explique a diferença entre as propriedades de resistência fraca a colisões (*Weak-Collision Resistance*) e resistência forte a colisões (ou *strong collision resistance*) numa função de síntese de segurança.

d) Qual das propriedades em c) é garantida pelo algoritmo SHA-256 ?

Questão 2

a) Um mecanismo para autenticidade e integridade de mensagens do tipo MAC (HMAC ou CMAC) pode ser usado como prova de autenticação de um principal (*Peer-Authenticity*) que emitiu uma mensagem, tendo em conta a definição dessa propriedades na *framework* X.800? Justifique.

b) Se usarmos o algoritmo RSA e um par de chaves de N bits, podemos cifrar ficheiros (ou mensagens) com tamanho superior a N bits? Justifique.

c) Se usarmos algoritmo RSA com a construção normalizada RSA-PKCS#1 e tendo um par de chaves de N bits, podemos assinar um ficheiro (ou mensagem) com tamanho superior a N bits? Justifique.

d) Se fizer duas assinaturas RSA-PSS seguidas de um mesmo conteúdo M (ex. o mesmo ficheiro) e usando a mesma chave privada (no mesmo par), o resultado das assinaturas (output) é igual ou é diferente? Porquê ?

e) Se fizer duas assinaturas DSA seguidas de um mesmo conteúdo M (ex. o mesmo ficheiro) e usando a mesma chave privada (no mesmo par), o resultado das assinaturas (output) é igual ou é diferente? Porquê ?

f) Se fizer duas assinaturas ECDSA seguidas de um mesmo conteúdo M (ex. o mesmo ficheiro) e usando a mesma chave privada (no mesmo par), o resultado das assinaturas (output) é igual ou é diferente? Porquê ?

Questão 3

a) Dois principais *A* e *B* vão usar o método de acordo de *Diffie-Hellman* (DH) para negociarem um segredo partilhado, com resistência a um ataque do tipo "homem-no-meio". Então A e B devem trocar necessariamente os respetivos números públicos DH gerados, assinados com um uma assinatura digital e além disso, enviados cifrados num envelope criptográfico com a chave pública do destinatário, usando um algoritmo criptográfico assimétrico (por exemplo, RSA). VERDADEIRO OU FALSO ? Justifique.

a) Tendo em conta a), podemos implementar o acordo seguro DH usando apenas o algoritmo ECDSA? Justifique.

b) Um cliente e um servidor que comunicam com TLS com autenticação mútua acordaram no uso da seguinte *ciphersuite*:

ECDHE TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256.

Quantas exponenciais modulares são calculadas pelo cliente e pelo servidor para executarem e concluírem o *handshake* TLS com sucesso e obterem a chave de sessão estabelecida? Justifique.

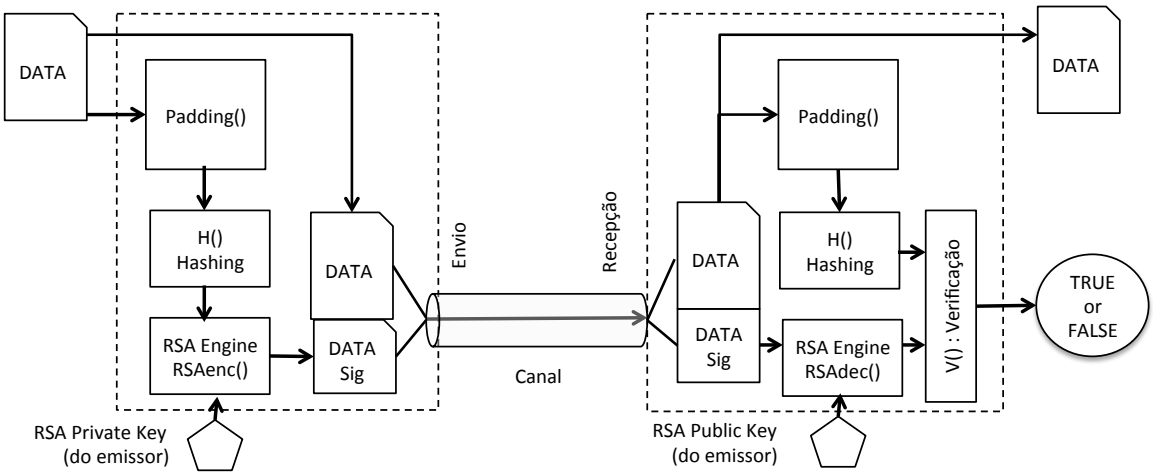
Questão 4

Explique em que consiste a autenticação interdomínio (ou *interrealm*) no sistema Kerberos e indique como se processa a autenticação de um utilizador num domínio *D1* que pretende usar um recurso (num servidor final) de um domínio D2.

Sugestão: pode apresentar a resposta com ajuda de um esquema caracterizando os passos da comunicação envolvida (sem precisar de indicar o detalhe do conteúdo das mensagens trocadas).

Questão 5

Considere o seguinte esquema que representa o processamento normalizado de uma assinatura digital RSA dos dados (DATA), tendo sido usada a construção normalizada RSA-PKCS#1. É suposto interpretar corretamente o esquema e conhecer o processamento das funções no emissor (assinatura) e destinatário (verificação da assinatura).



a) Em que bloco tem lugar o processamento subjacente à utilização de PKCS#1 na assinatura? Justifique.

b) Considere que a implementação da assinatura no emissor está programada em Java (suporte JCE), do seguinte modo:

```
Signature signature = Signature.getInstance("SHA256withRSA”);
…
signature.initSign(PrivateKey);   // A chave tem 2048 bits
…
signature.update(DATA);
…
```

diga a que corresponde, do lado do emissor, o bloco H() e o cálculo matemático no bloco RSAenc() e do lado do receptor, o bloco H(), o cálculo matemático RSAdec() e a computação na função V().

c) O que seria diferente no esquema apresentado se a assinatura fosse RSA-PSS em vez de RSA-PKCS1?

d) Considerando a sua resposta em *c)* e o esquema apresentado, assumindo que o emissor pretende assinar os dados (DATA) tendo estes o tamanho 8 Kbits. isso vai ser possível? Justifique.

Questão 6

Considere as propriedades de segurança definidas na *framework* de segurança X.800 na resposta às seguintes alíneas.

a) Se usarmos TLS em transporte TCP, garante-se confidencialidade de tráfego (*traffic-flow confidentiality*) e confidencialidade orientada à conexão (*connection-oriented-confidentiality*). Verdadeiro ou Falso? Justifique.

b) Se usarmos TLS em transporte UDP não se garante confidencialidade de tráfego (*traffic-flow confidentiality*) e garante-se confidencialidade de todos os *datagramas* UDP na sessão TLS. Verdadeiro ou Falso? Argumente.

c) O estabelecimento de associações de segurança em IPSec para que dois *hosts* troquem depois mensagens com base no protocolo ESP com autenticação, integridade, confidencialidade e não retransmissão ilícita de pacotes IP, garante a propriedade de *peer-authentication* dos endpoints envolvidos. Porquê ?

d) De acordo com o seu entendimento, pode o protocolo IPSec suportar o envio de pacotes IP *Multicast* para receptores que pertencem ao respetivo grupo *Multicast*? Argumente.

Exame de Recurso ou de Melhoria de Nota
Parte Com Consulta

Questão 7

O protocolo TLS pode ser usado com diferentes configurações. Uma das configurações corresponde ao modo de autenticação (anónima, unilateral ou mútua) e outra ao tipo de autenticação subjacente à CIPHERSUITE acordada entre cliente e servidor. Estas configurações repercutem-se na operação do subprotocolo *HANDSHAKE*, nomeadamente no fluxo de mensagens no processamento criptográfico por parte dos *endpoint*s. No caso de uso de *ciphersuites* que envolvem o algoritmo *Diffie-Hellman* (em diversas versões do protocolo) é possível estabelecer chaves de sessão no modo "*EDH - Ephemeral Diffie-Hellman*", "*FDH - Fixed Diffie-Hellman*" ou "*ADH - Anonymus DIffie-Hellmen*".

a) Qual a diferença entre os modos FDH e EDH e que segurança acrescida pode ter um sobre o outro?

b) A variante EDH permite proteger um ataque de um adversário do tipo "homem-no-meio" entre um cliente e um servidor se estes decidiram usar autenticação unilateral do cliente ? Justifique.

Questão 8

a) Um servidor HTTPS está a usar o protocolo TLS (versão TLSv1.2, numa configuração considerada com base na *ciphersuite*: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 .

   Os clientes e o servidor usam certificados de chaves públicas de tamanho 2048 bits, trocados no *handshake* TLS em cadeias de certificados, pertencendo o certificado raiz a uma CAs de confiança comum reconhecida por ambos. Os certificados na cadeia estão todos assinados com chaves de tamanho igual ou superior a 2048 bits. Neste caso, seria possível um cliente (que tem que estar necessariamente autenticado) explorar uma vulnerabilidade do tipo *Heartbleed* – caso esta vulnerabilidade exista do lado do referido servidor HTTPS. Justifique a sua resposta.

b) No *handshake* que estabeleceu a *ciphersuite* indicada em a) podem os certificados do clientes e do servidor conter chaves públicas RSA mas estando contidos em cadeias de certificação enviadas por ambos, em que outros certificados dessa cadeia são certificados de chaves DSA? Argumente.

Questão 9

Considere que se tem uma ***VPN*** para suportar acessos de uma rede sem fios doméstica (suportada em ***WLAN IEEE 802.11g***) onde se suporta ***IPv4*** com endereçamento privado (ex., 192,168.1.0/24 ou *mask* 255.255.255.0). A ***VPN*** será usada para aceder a uma rede IP institucional que usa internamente endereços privados ***IPv4***.

Para suportar a ***VPN*** utilizar-se-á ***IPSec*** em modo túnel. A ideia é que o túnel possa ser utilizado entre qualquer dispositivo wireless da rede doméstica (ex., computadores, *tablets* ou *smartphones*), através do *router* wireless doméstico com acesso à *Internet* e do *router* de acesso I*nternet* da instituição.

Nas ligações *Internet* os *routers* usarão endereçamento público ***IPv6*** e encaminhamento de pacotes ***IPv6***.

a) Se a ideia for garantir autenticação, confidencialidade, integridade e privacidade de todos os pacotes IPV4 enviados pelo túnel, qual deverá ser o subprotocolo da pilha *IPSec* que deve ser estabelecido para suportar o túnel? Justifique.

b) Quantas associações de segurança são precisas para suportar o túnel e o tráfego *inbound*/*outbnoud* em cada *router*? Justifique.

c) Numa solução como a que se preconiza em a) indique, justificando, como considera estar protegido o tráfego internet na interligação dos dois *routers*:

   C1) confidencialidade, autenticação e integridade de pacotes mas não confidencialidade do tráfego

   C2) confidencialidade, autenticação e integridade de pacotes e confidencialidade parcial de tráfego

   C3) confidencialidade, autenticação e integridade de pacotes e confidencialidade completa de tráfego

d) No suporte da referida ***VPN***, poderia ainda usar-se uma solução de túnel iterado. Para o túnel iterado (na sua proteção externa) faria sentido usar o subprotocolo ***IPSec AH*** ? Justifique a resposta com base no que se acrescentaria em termos de propriedades de segurança, a partir do que indicou em a).

Questão 10: *QUESTÃO VALORATIVA* (opcional, só para respostas em exames de melhorias de nota)

Dadas as possíveis parametrizações para *handshake* TLS (TLS 1.2 ou 1..3) que opções negociadas podem induzir vulnerabilidades em sistemas ou aplicações WEB suportadas ? A resposta será considerada válida se para três das sete vulnerabilidades indicadas as opções de parametrizações que devem ser descartadas forem bem indicadas

HEARTBLEED; BREACH; POODLE; LUCKY 13; FREAK; SWEET 32; BEAST