DI/FCT/UNL- Segurança de Redes e Sistemas de Computadores - 1º Sem, 2019/2020
Prova em Época de Exame, 17/Janeiro/2020 - RESPOSTAS DA PARTE COM CONSULTA

Recurso de Repescagem do Teste 2
Parte Sem Consulta

Questão 1

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

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

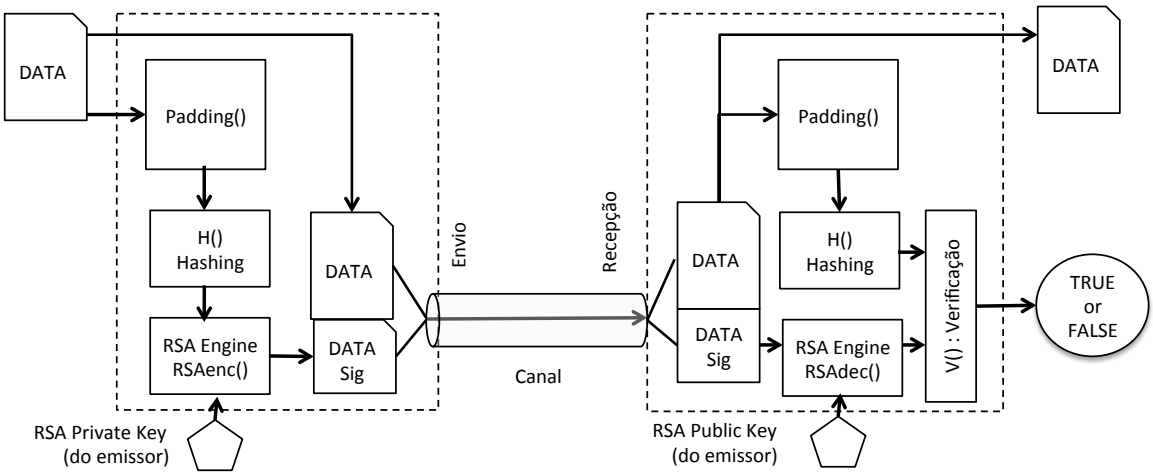
c) Um cliente e um servidor que vão comunicar usando TLS, acordaram usar a seguinte *ciphersuite*:

ECDHE TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256.

Que tipo de computações ou operações criptográficas tiveram lugar no cliente e no servidor durante o *handshake*, até que ambos tenham determinado a chave de sessão estabelecida?

Questão 2

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 3

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.

Questão 4

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. Por outro lado, as configurações repercutem-se na operação do subprotocolo *handshake*, nomeadamente no fluxo de mensagens e 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 ? Que segurança acrescida tem um modo face ao outro?

b) No caso de EDH e usando-se autenticação unilateral do cliente, garante-se resistência a ataques do tipo "homem-no-meio"? Argumente.

c) Repita a resposta à questão b) mas no caso de usar EDH e autenticação unilateral do servidor.

Questão 5

a) Em que consiste a utilização de IPSec em modo túnel e que vantagens encontra para suportar redes virtuais seguras (VPNs) para utilizadores domésticos (ligados em computadores de redes domésticas wireless, 802.11) ligadas a fornecedores de serviços Internet e acedendo remotamente a servidores com endereçamento provado, em redes institucionais ou corporativas.

b) Em que consiste a noção de adjacência de modos IPSec?

c) Dois computadores que utilizam endereçamento IPV6 privado, podem comunicar por IPSec em modo transporte ? Justifique se sim ou não e em que condições.

d) Quatro computadores numa rede local vão usar ESP com autenticação e confidencialidade para suporte das comunicações IPSec usando modo transporte. Se esses computadores vão comunicar todos entre si enviando e recebendo pacotes IPV4, quantas associações de segurança IPSec (SAs) precisam de ter estabelecidas em cada um com base no protocolo IKE? Justifique.

Recurso de Repescagem do Teste 2
Parte Com Consulta

Questão 6

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 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 7

No protocolo IKE que os dois extremos do túnel da questão 6 d) vão ter de executar para estabelecerem as respetivas associações de segurança, quantas assinaturas digitais terão que ser realizadas? Justifique.

Questão 8

Considere uma aplicação WEB que está protegida por HTTPS (para suportar interações HTTP/1.0), sendo o suporte parametrizado para *handshake* TLS v1. 2, autenticação unilateral do cliente, com o *handshake* estabelecendo uma *ciphersuite* que pode ser :

C1: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
C2: TLS_RSA_WITH_AES_256_CBC_SHA256

a) Quantas exponenciais modulares poupará o cliente para processar para completar o *handshake* TLS e estabelecer uma conexão HTTP1.0/TLS no caso de usar C2 em vez de C1, cada vez que o cliente pretender descarregar uma página HTML estática que é disponibilizada pelo servidor? Justifique.

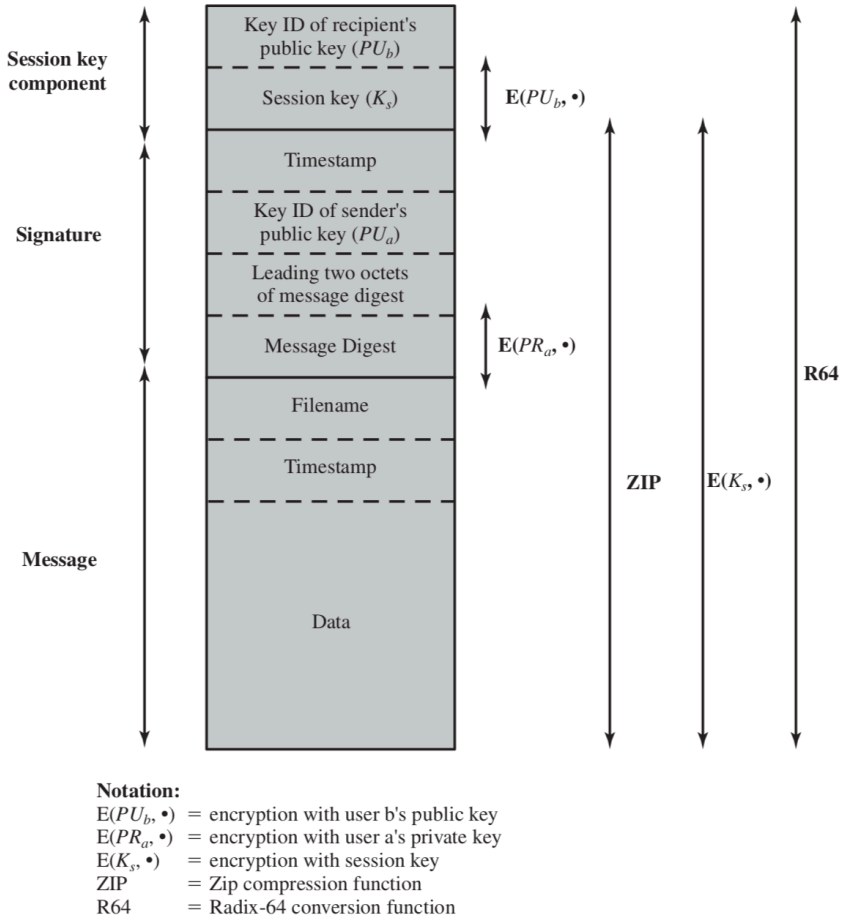
b) Quantas exponenciais modulares poupa o servidor se usar C2 em vez de C1, em cada conexão para pedido de um página pelo cliente? Justifique.

c) Nas *ciphersuites* indicadas, pode o cliente enviar no *handshake* um certificado ao servidor contendo a sua chave RSA, enviado este certificado numa cadeia em que os outros certificados da cadeia possuem chaves DSA? Justifique.

Questão 9

Para se enviarem mensagens seguras de um principal ***A*** para um principal ***B***, com garantias de segurança extremo-a-extremo pode utilizar-se o seguinte formato normalizado.

Com as proteções indicadas, as mensagens ficam protegidas mesmo que tenham que ser reencaminhadas por sistemas intermédios (como por exemplo, servidores *relay*, como é o caso de servidores SMTP para reencaminhamento e entrega de mensagens E-Mail, com base em processamento *store* and *forward*) ou trocas de mensagens através de servidores em serviços de *Messaging Store and Forward*),



Interprete o formato mostrado. No processamento do emissor (*A*), a chave de sessão *Ks* é gerada de forma segura pelo emissor, para cada mensagem enviada, sendo assim a chave usada apenas para a mensagem para a qual foi criada. Assuma que o campo *Filename* pode ser preenchido com um identificador obtido a partir de uma síntese segura (*hash value*) do *Subject (plaintext)* da mensagem (considerando por exemplo a estrutura genérica de uma mensagem *Email* ou do Título ou Identificador (plaintext) de cada mensagem, (campos que voltam a ser incluídos com o corpo da mensagem nos dados (*Data*), enviada cifrado.

Indique qual a sequência de operações que o emissor deve realizar dada a mensagem inicial (*plaintext)* para enviar a mensagem de forma correta, genérica e robusta, independentemente de todos os mecanismos ou soluções no processamento do cliente. Indique qual a opção que considera correta e justifique eporquê.

Opção A: (1) Cifrar a mensagem inicial, (2) Comprimir e (3) Assinar a Mensagem cifrada e comprimida
Opção B: (1) Assinar a mensagem inicial, (2) Cifrar a mensagem inicial e (3) comprimir a mensagem cifrada
Opção C: (1) Assinar a mensagem inicial, (2) Comprimir a mensagem inicia e (3) Cifrar a mensagem comprimida

Questão 10

Dadas as possíveis parametrizações para *handshake* TLS (TLS 1.2 ou 1..3) que opções podem induzir vulnerabilidades em sistemas ou aplicações WEB suportadas em TLS dos seguintes tipos. A resposta será considerada válida se para três dos sete casos apresentados de vulnerabilidades as opções de parametrizações forem bem indicadas

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