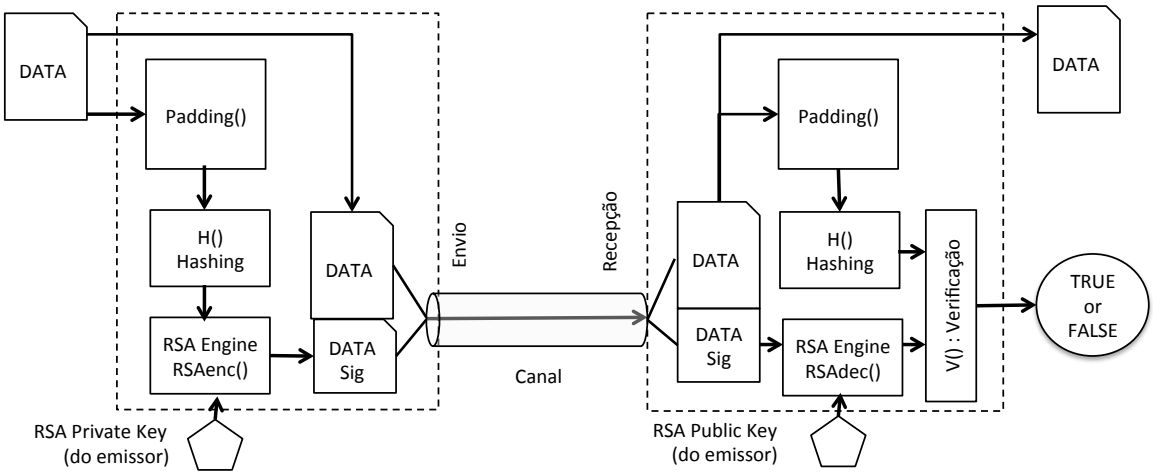
DI/FCT/UNL
Mestrado Integrado em Engenharia Informática
Segurança de Redes e Sistemas de Computadores
2º Semestre, 2015/2016 (30/Maio/2016)

T2: Teste sobre tópicos teóricos do programa
Teste sem consulta, duração: 1h45m

Questão 1

Considere o seguinte esquema que representa o processamento normalizado de uma assinatura digital RSA dos dados (DATA). É suposto interpretar corretamente o esquema e conhecer o processamento das funções no emissor (assinatura) e destinatário (verificação da assinatura).



a) Em que consiste a função *Padding()* que tem lugar antes da computação H(), para que serve e qual a sua importância nas garantias de segurança da assinatura ? Justifique.

b) Uma possível instanciação da função Padding() consiste em usar o processamento normalizado PKCS#1 que corresponde ao seguinte cálculo:

Padding(DATA) = 0x00 || 0x01 || F || DATA
Sendo F um array de bytes: 0xFF || 0xFF || 0xFF ... || 0x FF, de pelo menos 8 bytes

Trata-se do cálculo subjacente a uma assinatura digital do tipo RSA PKCS#1. Numa abordagem prática, uma assinatura digital usando o padrão PKCS#1 em Java (Programação com o suporte JCE), é resumidamente programada na forma seguinte a partir de um par de chaves RSA (KeyPair)

```
Signature signature = Signature.getInstance("SHA512withRSA”);
...
signature.initSign(keyPair.getPrivate());
...
signature.update(DATA);
```

Tendo em conta o esquema e a instanciação SHA512withRSA diga a que corresponde do lado do emissor a função H() o cálculo matemático da função RSAenc() - e do lado do receptor a função H(), o cálculo matemático RSAdec() e a função V() ?

c) Está a usar uma assinatura RSA-PKCS1, usando SHA-1 para a função H(). O par de chaves envolvido tem chaves RSA de 2048 bits, e os dados (DATA) são um bloco – array de bytes com 256 bits. Qual vai ser o tamanho em bytes de DataSig ? Justifique.

d) No exemplo de código acima em b) vamos modificar apenas a 1ª linha (na alínea b), de modo a ficar

```
Signature signature = Signature.getInstance("SHA1withRSAandMGF1”)
```

Do ponto de vista das propriedades de segurança esta assinatura é mais robiusta (mais segura) ou menos robusta (menos segura) em relação ao caso anterior ? Justifique.

Dica para o seu raciocínio teórico:
MGF-1 é uma função de síntese e está associada ao cálculo de *padding* OAEP.

e) Para que se possam garantir as propriedades de segurança da assinatura digital, de acordo com o esquema mostrado, independentemente dos algoritmos no esquema inicial instanciados na computação e verificação da assinatura, é sempre essencial que o canal seja um canal seguro com propriedades semelhantes a um canal TLS ou SSL).

Comente a afirmação indicando se é correta ou incorreta, justificando a sua resposta.

Questão 2

Apresente um esquema semelhante ao mostrado na questão 1, se o emissor quiser garantir a confidencialidade dos dados DATA na informação que passa no canal. O seu esquema deve usar processamento baseado na criação e processamento de envelopes de chave pública, utilizando criptografia simétrica para garantir confidencialidade.

Apresente apenas o esquema no processamento do lado do emissor, indicando as funções necessárias no esquema. Deve indicar qual a informação enviada no canal e como é protegida. Admita que na informação enviada no canal o emissor concatenará uma cadeia de certificação X509v3, em que a raiz dessa cadeia é da confiança prévia quer do emissor quer do receptor.

Questão 3

Pretende copiar ficheiros do disco do seu computador para uma *pen-drive*. Como receia perder a *pen-drive* decide usar criptografia RSA para cifrar cada ficheiro com uma chave pública. Guardará depois a chave privada do par em segurança, para poder recuperar os ficheiros. Os ficheiros têm dimensões variadas e vai cifrar cada ficheiro bloco a bloco, usando blocos de 2048 bits. A chave pública tem 1024 bits e não vai usar *padding* no processamento criptográfico. Do seu estudo teórico do processamento de cifras RSA, diga qual das seguintes afirmações é verdadeira, justificando a sua escolha.

AFIRMAÇÃO 1): Não consegue cifrar os ficheiros de acordo com o descrito.

AFIRMAÇÂO 2): Só consegue cifrar os ficheiros se usar *padding*

AFIRMAÇÃO 3): A operação de cifra não é possível como descrito, só sendo possível com chaves de 2048 bits ou mais e tendo obrigatoriamente que usar *padding*

AFIRMAÇÃO 4): A operação de cifra não é possível como descrito, apenas sendo possível se as chaves envolvidas tiverem 2048 bits ou mais.

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 de acordo com a CIPHERSUITE usada. Como é sabido, as configurações repercutem-se na operação do sub-protocolo HANDSHAKE, nomeadamente fluxo de mensagens e máquina de estado de processamento 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 esses modos ?

b) No caso de EDH com autenticação mútua, o que permite proteger um ataque de inpersonificação por interposição de um adversário do tipo "homem-no-meio" ? Justifique.

c) Se a *ciphersuite* escolhida usar EDH, então o cliente e o servidor não podem usar certificados de chaves públicas DSA. Verdadeiro ou Falso ? Justifique.

d) Dado um trace do protocolo Handshake-TLS (por exemplo obtido com uma ferramenta do tipo wireshark), como reconhece que se verificou autenticação unilateral só do cliente ?

e) Um servidor HTTPS está a usar o protocolo TLS (numa configuração considerada segura, ex: TLSv1.2, autenticação mútua e impondo uma *ciphersuite* considerada segura, por exemplo da seguinte: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

   Os clientes e o servidor usam certificados de chaves públicas de tamanho 2048 bitts assinadas por CAs de confiança e os certificados estão 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.

Questão 6

a) Explique as principais diferenças entre um modelo de controlo de acesso do tipo RBAC (*Role Based Access Control)* e ABAC (*Attribute-Based Access Control*). Exemplifique um cenário de utilização de um e outro

b) No caso do sistema de ficheiros UNIX (ou LINUX), qual o modelo de controlo de acessos subjacente ao modelo de permissões de operações sobre ficheiros ? Porquê ?