

Departamento de Informática, FCT/UNL

Segurança de Sistemas Computacionais

Teste de Frequência #2

1º Semestre, 2013/2014

Nº	Nome:		
Grupo:	Nº Total de folhas (incluindo esta capa)		

Grelha de Avaliação:
a preencher pelo docente

PARTE I (Sem consulta)									

PARTE II (Com consulta)									

Duração do teste

Parte 1 (sem consulta): 10h00-11h20

Parte 2 (com consulta): 11h30-13h00

Parte 1 (Sem Consulta)

Nas questões 1 e 2, apenas uma das afirmações das alíneas está correcta. Indique qual assinalando V e F na segunda coluna da tabela.

Questão 1.

Uma assinatura digital de uma mensagem M , na sua forma mais geral, pode combinar um método criptográfico assimétrico, uma função de síntese e um esquema de *padding*. O esquema de *padding* revela-se importante do ponto de vista das propriedades de segurança da assinatura e em geral vários esquemas normalizados de padding podem ser usados na parametrização da assinatura, como por exemplo: PKCS#1 ou OAEP. Em assinaturas DSA ou RSA o esquema de *padding* permite:

a) Fazer com que a mensagem M a assinar juntamente com a informação <i>padding</i> adicional corresponda a um bloco de tamanho apropriado de forma a ser igual a um múltiplo do tamanho base do bloco base utilizado pelo algoritmo assimétrico.	
b) Transformar a representação da mensagem como valor inteiro de modo a que corresponda a um valor inteiro suficientemente grande comparativamente ao tamanho das chaves e módulo usados pelos algoritmos DSA ou RSA.	
c) Fazer com que a mensagem possua um tamanho apropriado para que se possa aplicar a função de síntese subjacente ao cálculo da assinatura digital.	
d) Fazer com que na validação da assinatura se possa implicitamente reconhecer que a mensagem M assinada não foi alterada.	

Questão 2.

Considere um protocolo em que o processo de estabelecimento de uma chave de sessão entre dois principais correctos se faz a partir de um acordo, usando o método *Diffie-Hellman*. No acordo, vários parâmetros têm que ser trocados e partilhados entre os principais.

Para evitar que um atacante do tipo “homem no meio” possa vir a quebrar a confidencialidade do canal a estabelecer entre os principais correctos que participaram no acordo, é condição necessária e suficiente que cada valor Y (Y_A e Y_B trocados pelos principais no acordo):

a) Seja cifrado com a chave pública do destinatário	
b) Seja assinado com a chave privada do emissor	
c) Seja assinado como em b), devendo no entanto a assinatura ser concatenada com o valor cifrado com a chave pública do destinatário (como em a).	
d) Seja assinado como em b), mas o valor que resulta da assinatura deve ser por sua vez cifrado com a chave pública do destinatário	

Questão 3.

- a) Quais os sub-protocolos associados à suite SSL ou TLS ? Para cada um resume num pequeno Parágrafo o seu propósito ou objectivo.
- b) Está a utilizar o modo de autenticação do tipo *ANONYMOUS DIFFIE-HELLMAN* em alguma suite criptográfica válida no protocolo SSL ou TLS. Nesse caso consegue garantir que dois principais são capazes de estabelecer uma canal SSL confidencial com base numa chave simétrica partilhada ? Justifique a sua resposta.

Questão 4.

No protocolo PGP, sempre que seja necessário enviar mensagens confidenciais, autênticas e com conteúdo comprimido, será necessário que o processamento seja feito pela seguinte ordem pelo emissor que vai enviar a mensagem.

- 01) 1º Assinatura da mensagem original; 2º Compressão da mensagem original e 3º Cifra da mensagem comprimida.
- 02) 1º Compressão da mensagem original; 2º Assinatura da mensagem comprimida e 3. Cifra da mensagem comprimida.
- 03) 1º Cifra da mensagem original; 2º Compressão da mensagem original e 3.º Assinatura da mensagem comprimida.
- 04) 1º Assinatura da mensagem original; 2º Cifra da mensagem original e 3º Compressão da mensagem original.
- 05) 1º Cifra da mensagem original; 2º Compressão da mensagem original e 3º Assinatura da mensagem comprimida.

- a) Qual ou quais das anteriores opções (01 a 05) estão correctas ?
- b) Porquê ?

Questão 5.

Dois dos modos de autenticação normalizados em SSL são designados por *FIXED DIFFIE HELLMAN (FDH)* e *EPHEMERAL DIFFIE HELLMAN (DHE)*. O segundo está na base de diversas suites criptográficas que podem ser usadas no protocolo, ex.:

```
SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
SSL_DHE_DSS_WITH_DES_CBC_SHA
SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA
```

O primeiro modo (DHE) embora normalizado não está habitualmente disponível nas suites criptográficas disponíveis para programação, como acontece por exemplo com o suporte JSSE (Sockets SSL em Java). Por outro lado, não é comum nas configurações suportadas e nas utilizações típicas do protocolo SSL em ambiente Internet.

- a) Qual a diferença principal entre as suites criptográficas subjacentes aos modos FDH e DHE ?

- b) Porque é que o modo FDH não é comum na utilização do protocolo SSL em ambiente Internet, como por exemplo, para suportar o protocolo HTTPS ou autenticação de servidores na Internet ? Justifique a sua resposta.

Questão 6

Responda Verdadeiro (V) ou Falso (F) na 2ª coluna .

a) Os mecanismos de segurança do protocolo SSL permitem minimizar e proteger conexões HTTPS de ataques <i>DoS</i> desencadeados ao nível do estabelecimento de sessões TCP do tipo <i>SYN-Flooding</i> durante o estabelecimento de conexões TCP (Protocolo <i>Three Hand Shake</i> no estabelecimento de conexões TCP).	
b) Numa conexão HTTPS, os cabeçalhos do protocolo HTTP são protegidos em confidencialidade tal como o conteúdo de páginas (exemplo conteúdos HTML) são mantidos confidenciais.	
c) A norma S/MIME está associada à definição de um modelo de confiança de certificados de chave pública semelhante ao que também é usado pelo sistema PGP (<i>Web-of-Trust</i>).	
d) Um cliente está a descarregar de um servidor um ficheiro transferido por blocos, com base numa conexão HTTPS e usando a suite TLS_RSA_WITH_AES_128_CBC_SHA256 no protocolo TLS. O cliente transfere do servidor os blocos fazendo pedidos HTTP/1.1. Em cada pedido GET feito em pipeline é pedido um bloco de 1K enviado na resposta. Os pedidos de cada bloco são feitos em sequência e de forma ordenada. Neste caso, a autenticação de cada bloco transferido em HTTPS é verificada pelo cliente reconhecendo a assinatura digital que o servidor faz sobre o bloco usando a sua chave privada e o servidor valida a autenticidade do bloco de pedido porque obteve e validou o certificado da chave pública do servidor.	
e) O protocolo Kerberos, nas versões normalizadas estudadas (V4 ou V5), só usa criptografia simétrica no processo de autenticação remota de utilizadores..	
f) Em TLS o uso de uma configuração de autenticação mútua, certificados de chaves públicas RSA de 2048 bits e suite TLS_DHE_RSA_WITH_AES_256_CBC_SHA , dependendo do tamanho dos valores públicos do acordo no algoritmo Diffie-Hellman a latência da fase de <i>handshake</i> será maior ou menor.	
g) A autenticação de utilizadores no sistema Kerberos (V4 ou V5) é imune a ataques que possam ser feitos para quebrar passwords de utilizadores com base em ataque do tipo dicionário.	
h) No sistema PGP, ao receber-se uma mensagem de um endereço X com um pedido de revogação de uma chave pública em que essa mensagem vem assinada pela respectiva chave privada, não deve revogar-se imediatamente a chave pública, nomeadamente quando o endereço Email associado à chave pública em causa que consta do chaveiro de chaves públicas (<i>pub key ring</i>) não seja o endereço X.	

Parte 2 (Com Consulta)

Questão 7

Pretende conceber-se uma variante do sistema Kerberos (apenas com as modificações mínimas necessárias propostas em relação à versão 5 estudada do protocolo Kerberos), de modo a evitar possíveis ataques às passwords dos utilizadores (por exemplo, ataques por dicionário).

Condições para a sua proposta:

- O Servidor de Autenticação (Kerberos AS) possui dois certificados: C1 e C2. C1 é um certificado X509 de uma chave pública DSA emitido por uma CA (reconhecida confiável pelos clientes). C2 é um certificado de uma chave pública RSA auto-assinado que apenas usa internamente (ver à frente).
- Os clientes possuem um certificado X509 (CertC) de uma chave pública DSA emitido por uma CA (reconhecida confiável pelo Kerberos AS);
- Os clientes possuem um identificador único (ClienteID) ao qual continua a estar associada uma password pedida aos utilizadores no momento da autenticação. Esta password está mantida (armazenada) do lado do servidor na forma $\{H(PWD)\}_{K_{pubRAS}}$, sendo K_{pubRAS} a chave pública respeitante ao certificado C2.
- A primeira ronda de mensagens a considerar na variante deve ser obrigatoriamente a seguinte;

C > S:

ClienteID || CertC || Na { H (Cliente ID, Na, H(PWD)) } KprivC || HmacK1(M)

S > C:

Ciphersuite || C1 || {Na+1, Nb} KprivAS || HMacK2 (M) ||
..... resto do protocolo que proporá.

Na é um desafio (*nonce*) inicialmente gerado pelo cliente.

Nb é m desafio (*nonce*) gerado pelo servidor.

Nas restantes mensagens do protocolo os *nonces* trocados nestas duas mensagens serão relevantes para proteger a integridade do fluxo restante do protocolo, devendo haver ainda controlo de integridade e protecção contra *replaying*, por parte de qualquer atacante no canal.

- a) Desenhe o protocolo usando a mesma notação da bibliografia estudada (tendo por base uma especificação do fluxo de mensagens. Pode acrescentar uma legenda para clarificar o processamento criptográfico. Note que as modificações ao restante da variante do protocolo Kerberos V5 devem ser as mínimas para adequar os requisitos acima.
- b) Com base na sua especificação indicar como vai usar os seguintes elementos das duas primeiras mensagens:

HMacK1 (M): o que será M e como será gerada a chave K1 deste HMAC.

Idem para HMacK2 (notar que K2 e K1 devem ser diferentes)

Conteúdo de *Ciphersuite*.

Questão 8

- a) Se em SSL se está a usar uma *ciphersuite* do tipo TLS_DHE_RSA_WITH_AES_256_CBC_SHA256, num modo de autenticação mútua, os valores públicos do acordo de Diffie Hellman serão assinados pelo cliente e servidor usando assinaturas digitais RSA. Se os respectivos certificados de chave pública RSA (do cliente e do servidor) têm chaves públicas de 1024 bits, seria possível que os valores públicos e privados utilizados no acordo de Diffie Hellman fossem de 2048 bits? Justifique a sua resposta.
- b) Na análise de tráfego da fase de *handshake* SSL ou TLS, as mensagens CHANGE_CIPHER_SPEC são trocadas no decurso do protocolo *handshake*, antes de este terminar. Numa primeira análise poderá parecer que são apenas duas mensagens do sub-protocolo *handshake* do protocolo SSL. No entanto, na definição do protocolo, são mensagens pertencente a outro sub-protocolo da pilha SSL: *change cipher spec protocol*. Qual a razão e vantagem de haver essa diferenciação?
- c) Considere o fluxo de mensagens do *handshake* do protocolo SSL ou TLS. Se a *ciphersuite* usada no *handshake* for SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA, em qual das mensagens do fluxo *handshake* viajam os valores públicos de Diffie-Hellman e as respectivas assinaturas?
- d) Se o cliente SSL usar o certificado anexo, poderia usar a *ciphersuite* em c em modo de autenticação mútua? Justifique.
- e) Se os respectivos certificados de chave pública RSA (do cliente e do servidor) têm chaves públicas de 1024 bits, seria possível em qualquer *ciphersuite* que use Diffie-Hellman que os valores públicos e privados utilizados no acordo de Diffie Hellman fossem de 2048 bits? Justifique a sua resposta.

Questão 9

Considere os valores desta questão apenas exemplificativos para a resposta teórica pretendida que pode ser calculada manualmente, já que são valores muito pequenos para a segurança dos métodos indicados.

- a) Interceptou-se no canal uma mensagem *ciphertext* (C) cifrada com RSA, tendo C uma representação cujo valor inteiro = 18. A mensagem foi enviada de A para B na forma $\{P\}_{K_{pubB}}$. Sabe-se que a chave pública do emissor corresponde ao valor inteiro = 5, com módulo 35. Qual era a mensagem P?
- b) Você é um atacante que está a tentar obter uma chave que está a ser negociada por dois principais A e B com base no acordo de Diffie Hellman não autenticado (ou anónimo). Você sabe que A e B estão a usar uma raiz primitiva G para o cálculo de valores do acordo de Diffie-Hellman $G = 2$ e que estão a usar o valor do módulo = 11. Durante o acordo você viu passar o valor 9 de A para B e de seguida viu passar o valor 5 de B para A. Apenas com esta observação, qual vai ser o valor da chave partilhada por A e B no final do acordo?

Questão 10

Considere o formato de uma mensagem PGP.

- a) Para que serve o campo KeyID do componente da assinatura? Porque é que o mesmo é necessário para o processamento das mensagens?

- b) Para que serve o campo KeyID do componente de envelope de chave de sessão ? Porque é que o mesmo é necessário para o processamento das mensagens ?
- c) Como faria para utilizar o formato das mensagens PGP e otimizar o envio de uma mesma mensagem autêntica e confidencial para uma *mailing list* de múltiplos subscritores ?
- d) Para que servem os dois octetos mais significativos da síntese que está assinada (*leading two octets*) passados no formato das mensagens PGP no processamento de validação de uma mensagem assinada ?

Questão 11

No sistema PGP um utilizador possui um certificado de uma CA na qual confia e pretende colocar a respectiva chave pública no seu chaveiro de chaves públicas (ou *public key ring*). A ideia é que qualquer mensagem que lhe seja enviada futuramente assinada por essa CA e que anuncie uma chave pública de qualquer principal P, lhe permita adicionar uma entrada para P no seu chaveiro de chaves públicas, de modo que fique imediatamente reconhecida a legitimidade da chave pública de P como pertencendo ao principal P.

Para este efeito, como deve ser adicionada a chave pública da CA no chaveiro de chaves públicas em relação aos outros campos da tabela que representa o chaveiro de chaves públicas ? Na sua resposta use o significado e processamento implícito ao chaveiro de chaves públicas e os seus parâmetros, para explicar a lógica de inserção da chave pública da CA no chaveiro de chaves públicas para o fim em vista.

Questão 12

Observe no seu browser o certificado de chave pública do serviço <https://www.facebook.com> e a respectiva cadeia de certificação X509v3. Verifique o certificado obtido desse servidor (HTTPS) e a CA que o emitiu.

- a) Quantos bits tem a chave pública do certificado X509v3 do *Facebook* ?
- b) A síntese subjacente à assinatura RSA do certificado por parte da CA que emitiu o certificado é calculada com o algoritmo SHA-1, que produz sínteses de 160 bits. Não obstante, como pode verificar, a assinatura possui 256 bytes. Isto faz sentido ? Porquê ?
- c) De acordo com a política de emissão do certificado em causa e de acordo com a política de utilização da chave pública certificada, poderá o certificado ser usado para estabelecimento de conexões SSL ao servidor Facebook e as operações criptográficas envolvidas ? Justifique verificando o campo KeyUsage e Key-Usage Extensions tal como expressos no certificado emitido pela CA.
- d) Poderá a entidade Facebook usar este certificado para emitir novos certificados ? Justifique a sua resposta verificando e comparando os respectivos campos na cadeia de certificação observada.
- e) Ao estabelecer a conexão SSL com base na cadeia de certificação em causa, o seu browser usou uma validação do tipo cadeia directa (ou *direct chaining*) ou cadeia inversa (*reverse-chaining*) ?

ANEXO

Certificado da questão 8 d).

```
machj:xxx hj$ keytool -printcert -file xx.cer
```

Owner: CN=Henrique Domingos, OU=Faculdade de Ciencias e Tecnologia,
O=Universidade Nova de Lisboa (UNL), L="Campus da FCT, Caparica",
ST=Almada, C=PT

Issuer: CN=Henrique Domingos, OU=Faculdade de Ciencias e Tecnologia,
O=Universidade Nova de Lisboa (UNL), L="Campus da FCT, Caparica",
ST=Almada, C=PT

Serial number: 52b347d2

Valid from: Thu Dec 19 19:24:02 WET 2013 until: Wed Mar 19 19:24:02 WET 2014

Certificate fingerprints:

MD5: 32:A1:BB:B4:AE:33:00:91:24:C6:3C:7A:38:64:DE:D7

SHA1: 96:FF:01:04:00:32:1C:B6:C8:7D:47:C7:36:97:3E:AD:3B:3C:93:07

Signature algorithm name: SHA1withDSA

Version: 3

Nota:

Este certificado gerado com a ferramenta keytool é um certificado auto-assinado.