Departamento de Informática
Faculdade de Ciências e Tecnologia
UNIVERSIDADE NOVA DE LISBOA

Mestrado em Engenharia Informática

Segurança em Sistemas Informáticos Distribuídos

2º Semestre 2005/2006

Teste de Avaliação de Conhecimentos (Teste Nº 2 – 24/MAIO/2005)

Notas:

- O enunciado tem 5 questões, divididas em duas partes:
  - **Parte sem consulta** (Questões 1): 50 min
  - **Parte com consulta** (Questões , 2 e 3) : 50 min
- Leia completamente e com atenção cada questão antes de responder. A interpretação do enunciado é um factor de avaliação.

---------- A preencher pelos alunos ----------

Nº de aluno: _____ Nome: _____

Nº Total de páginas entregues: _____ (numere as páginas na forma Pág / TOTAL)

Classificação (a preencher pelo docente):

PARTE 1 (sem consulta)	**PARTE 2 (com consulta)**

1)	**2)**	**3)**
a)	a)	a)
b)	b)	b)
c)		c)
d)		
e)		
f)		
g)		
h)		

Questão 1)

a) Quais os requisitos e propriedades base que estão subjacentes à segurança de um sistema criptográfico ou algoritmo criptográfico assimétrico ? centre a sua resposta nas propriedades e relações entre os diversos componentes do modelo de criptografia assimétrica

b) Qual o interesse de se usar um esquema de *padding* como o OAEP (em vez de PKCS1 por exemplo) quando se utiliza criptografia assimétrica RSA ?

c) O método D-H permite o estabelecimento de um acordo de chaves criptográficas assimétricas entre dois principais. Este acordo permite ou não estabelecer princípios de autenticidade desses principais ? Justifique a sua resposta indicando o que proporia para ter um esquema de distribuição de chaves baseado em D-H prevenindo o pressuposto de autenticidade dos principais envolvidos.

d) Descreva o cenário tipo de um ataque "homem-no-meio" durante o protocolo de D-H entre duas entidades A e B. Sugestão: represente o ataque com base num diagrama temporal ou de sequência descrevendo a troca de mensagens entre A e B e a actuação-tipo do atacante para no final obter a mesma chave criptográfica simétrica que A e B pretendem partilhar. Com base nesse diagrama diga como a solução que avançou em c) evita esse problema.

e) Um possível esquema de MAC pode basear-se num algoritmo criptográfico simétrico de desempemnho rápido e uma sequência de blocos obtidos de amostras de relógio (uma stream obtida por concatenação de *timestamps* parciais). Em que consiste genericamente a obtenção de um MAC deste tipo ?

f) Em que consistem as propriedades de "*weak collision resistance*" e "*strong collision resistance*" num método de síntese ?

g) Refira as variantes de modos de autenticação em SSL que podem ser usados tanto em autenticação unilateral como bilateral (ou mútua) e indique qual o que considera mais seguro. Justifique.

Questão 2)

a) Os esquemas designados de assinaturas digitais com arbitragem permitem ultrapassar com vantagens eventuais alguns problemas que possas estar associados com o uso de esquemas de assinaturas directas (envolvendo apenas emissor e receptor). Comente a afirmação com base em eventuais requisitos associados à pragmática da utilização de aplicações ou de serviços distribuídos que adoptem assinaturas digitais para autenticar e validar a origem e efectivação de operações.

b) Um dos protocolos que permite resolver certos problemas de segurança na aplicação do modelo de Needhan-Schroeder consiste, entre outras, na variante do método de Denning-Sacco, com inclusão de timestamps derivados de relógios sincronizados, nos passos 1 e 2 do protocolo de referência de N-S. Contudo, a introdução desses timestamps implica noutro tipo de problemas. Quais ?

Questão 3)

a) Suponha os seguintes três traços anexos (*traces 1, 2 e 3*) observados numa interacção tipo entre um browser e um servidor WEB em HTTPS sobre conexão SSL. Num dos traços a sessão SSL foi normalmente restabelecida nos outrs não. Com base nos traços identifique que razões podem ter existido no caso das sessões SSL que não foram estabelecidas com sucesso.

b) Em SSL o método de troca de chaves com base no modo E-DH (Ephemeral Diffie Hellman) é considerado mais seguro do que o método base de troca de material para geração das chaves com assinaturas RSA. No entanto este último é na prática o mais adoptado. Se é mais seguro, que razões encontra em não se utilizar o primeiro face ao segundo ?

c) Considere o contexto das assinaturas duais usadas no protocolo SET e que permite que o cardholder possa autenticar de forma dual informação confidencial enviada independentemente ao Merchant e ao PaymentGateway (através do Merchant). Suponha um modelo em que um principal precisa de autenticar com os mesmos pressupostos partes confidenciais de informação enviadas a um grupo através de interacções P2P. Diga como construiria um esquema de assinaturas de N-Partes (e não apenas de 2 partes como as assinaturas duais do SET) no cenário referido.

TRACE 1

```
New TCP connection #1: guest-e-U-di-
10.171.96.43.in.di.fct.unl.pt(2762) <-> di157(443)
1 1  0.0376 (0.0376)  C>S SSLv2 compatible client hello
  Version 3.0
  cipher suites
  SSL_RSA_WITH_RC4_128_MD5
  SSL_RSA_WITH_RC4_128_SHA
  SSL_RSA_WITH_3DES_EDE_CBC_SHA
  SSL2_CK_RC4
  SSL2_CK_3DES
  SSL2_CK_RC2
  SSL_RSA_WITH_DES_CBC_SHA
  SSL2_CK_DES
  SSL_RSA_EXPORT1024_WITH_RC4_56_SHA
  SSL_RSA_EXPORT1024_WITH_DES_CBC_SHA
  SSL_RSA_EXPORT_WITH_RC4_40_MD5
  SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
  SSL2_CK_RC4_EXPORT40
  SSL2_CK_RC2_EXPORT40
  SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
  SSL_DHE_DSS_WITH_DES_CBC_SHA
  SSL_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA
1 2  0.0382 (0.0006)  S>C  Handshake
      ServerHello
        Version 3.0
        session_id[32]=
          61 fe 04 a1 a6 37 98 3a bd 14 3d aa 38 11 2e 19
          ce c2 e8 a4 75 f6 5b a3 74 72 0c 3b 09 fe 23 f2
        cipherSuite         SSL_RSA_WITH_RC4_128_MD5
        compressionMethod                     NULL
1 3  0.0382 (0.0000)  S>C  Handshake
      Certificate
1 4  0.0382 (0.0000)  S>C  Handshake
      ServerHelloDone
1 5  0.0515 (0.0132)  C>S  Handshake
      ClientKeyExchange
1 6  0.0515 (0.0000)  C>S  ChangeCipherSpec
1 7  0.0515 (0.0000)  C>S  Handshake
1 8  0.2498 (0.1982)  S>C  ChangeCipherSpec
1 9  0.2498 (0.0000)  S>C  Handshake
```

TRACE 2

```
New TCP connection #1: guest-e-U-di-
10.171.96.43.in.di.fct.unl.pt(2794) <-> di157(443)
1 1  0.0445 (0.0445)  C>S SSLv2 compatible client hello
  Version 3.0
  cipher suites
  SSL_RSA_WITH_RC4_128_MD5
  SSL_RSA_WITH_RC4_128_SHA
  SSL_RSA_WITH_3DES_EDE_CBC_SHA
  SSL2_CK_RC4
  SSL2_CK_3DES
  SSL2_CK_RC2
  SSL_RSA_WITH_DES_CBC_SHA
  SSL2_CK_DES
  SSL_RSA_EXPORT1024_WITH_RC4_56_SHA
  SSL_RSA_EXPORT1024_WITH_DES_CBC_SHA
  SSL_RSA_EXPORT_WITH_RC4_40_MD5
  SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
  SSL2_CK_RC4_EXPORT40
  SSL2_CK_RC2_EXPORT40
  SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
  SSL_DHE_DSS_WITH_DES_CBC_SHA
  SSL_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA
1 2  0.0452 (0.0006)  S>C  Handshake
      ServerHello
        Version 3.0
        session_id[32]=
          25 a7 27 e5 12 68 94 38 17 84 ad 8a 83 52 5e c0
          5e eb 97 df d7 ce 7a 5d d1 dc 5b 36 52 e8 57 bb
        cipherSuite         SSL_RSA_WITH_RC4_128_MD5
        compressionMethod                     NULL
1 3  0.0452 (0.0000)  S>C  Handshake
      Certificate
1 4  0.0452 (0.0000)  S>C  Handshake
      CertificateRequest
        certificate_types                   rsa_sign
        certificate_types                   dss_sign
      ServerHelloDone
1    0.2257 (0.1805)  C>S  TCP FIN
1    0.2259 (0.0002)  S>C  TCP FIN
New TCP connection #2: guest-e-U-di-
10.171.96.43.in.di.fct.unl.pt(2795) <-> di157(443)
2    0.5285 (0.5285)  C>S  TCP FIN
2    0.5288 (0.0002)  S>C  TCP FIN
```

TRACE 3

```
New TCP connection #1: guest-e-U-di-
10.171.96.43.in.di.fct.unl.pt(2825) <-> di157(443)
1 1  0.0031 (0.0031)  C>S  Handshake
      ClientHello
        Version 3.0
        resume [32]=
          1a b9 e3 fe f5 fb ad b4 df ed 00 19 3b 8e 9f b2
          9a 6a 40 3f 2e ec c8 53 7d 5b f9 0e d3 3c 2c 20
        cipher suites
        SSL_RSA_WITH_RC4_128_MD5
        SSL_RSA_WITH_RC4_128_SHA
        SSL_RSA_WITH_3DES_EDE_CBC_SHA
        SSL_RSA_WITH_DES_CBC_SHA
        SSL_RSA_EXPORT1024_WITH_RC4_56_SHA
        SSL_RSA_EXPORT1024_WITH_DES_CBC_SHA
        SSL_RSA_EXPORT_WITH_RC4_40_MD5
        SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
        SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
        SSL_DHE_DSS_WITH_DES_CBC_SHA
        SSL_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA
        compression methods
                  NULL
1 2  0.0038 (0.0006)  S>C  Handshake
      ServerHello
        Version 3.0
        session_id[32]=
          1a b9 e3 fe f5 fb ad b4 df ed 00 19 3b 8e 9f b2
          9a 6a 40 3f 2e ec c8 53 7d 5b f9 0e d3 3c 2c 20
        cipherSuite         SSL_RSA_WITH_RC4_128_MD5
        compressionMethod                     NULL
1 3  0.0038 (0.0000)  S>C  ChangeCipherSpec
1 4  0.0038 (0.0000)  S>C  Handshake
1 5  0.0096 (0.0058)  C>S  ChangeCipherSpec
1 6  0.0096 (0.0000)  C>S  Handshake
1    0.0537 (0.0441)  C>S  TCP FIN
1    0.0538 (0.0000)  S>C  TCP FIN
```