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

Mestrado em Engenharia Informática

Segurança em Sistemas Informáticos Distribuídos

1º Semestre 2003/2004

Teste de Avaliação de Conhecimentos (Teste Nº 1 – 19/Abtril/2005)

Notas:

- O enunciado tem 5 questões, divididas em duas partes:
  - **Parte sem consulta** (Questões 1 e 2): 50 min
  - **Parte com consulta** (Questões , 3 e 4) : 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)**	**4)**
a)	a)	a)	a)
b)	b)	b)	b)
c)	c)	c)	c)
d)	d)	d)	d)
e)	e)	e)	
		f)	
		g)	
		h)	

Questão 1)

a) Em que âmbito se utilizam os algoritmos de cifra simétrica da família de cifra em cadeia (*Stream-Cypher*)? porque é que nesse âmbito não é adequado o uso de métodos criptográficos simétricos da família de cifra por blocos mesmo com base em diferentes modos, como por exemplo ECB, CBC ou OFB?

b) Considere o código mostrado. Pretende-se que ao correr este programa se obtenha no ecrã a seguinte saída:

```
input : 000102030405060708090a0b0c0d0e0f
cipher: 61a1f886ff9bc709dd37cd9ce33adc6f bytes: 16
plain : 000102030405060708090a0b0c0d0e0f bytes: 16
```

Não pode modificar nada. Apenas pode preencher os espaços. Diga se é possível e no caso afirmativo apresente a sua implementação.

c) Diga em que consiste o conceito de chave fraca, semi-fraca ou potencialmente fraca num algoritmo criptográfico simétrico e porque é que essas chaves devem ser evitadas. Justifique a resposta e tente clarificá-la o melhor possível a partir do conhecimento que tem sobre da estrutura da cifra de Feistel e sua utilização na implementação interna do método DES ou 3DES.

d) Considere a tabela T1 na qual se apresentam tipologias de ataques (colunas) e suportes de serviços de segurança (linhas) num sistema distribuído. Coloque um "X" nos locais apropriados, de modo a indicar qual o suporte do serviço de segurança que está mais especificamente associado a contra-medidas em relação a cada um dos ataques mencionados.

e) Faça o mesmo que fez na alínea a) mas agora para a tabela 2, onde se encontram mecanismos básicos de segurança (colunas) e serviços de segurança (linhas), indicando quais os mecanismos (colunas) que estão associados ou combinados para se construírem os serviços indicados (linhas).

TABELA 1	Ataque Tipo					
Serviço de suporte de segurança	**Release of messages**	**Traffic Analysis**	**Masquerade**	**Reply**	**Tampering**	**Denial of Service**
Peer Authentication						
Data Origin Athentication						
Access Control						
Data Confidentiality						
Traffic Flow Confidentiality						
Data Integrity						
Non Repudiation						
High Availability						

Tabela 2	Mecanismo					
Serviço de suporte de segurança	**Método de Cifra/Decifra**	**Assinaturas Digitais**	**Controlo de Acessos**	**Métodos de hashing**	**Modelos de Autenticação e distribuição de chaves**	**Certificação X509 e Cas (PKIs)**
Peer Authentication						
Data Origin Athentication						
Access Control						
Data Confidentiality						
Traffic Flow Confidentiality						
Data Integrity						
Non Repudiation						
High Availability						

Questão 2) Responda a quatro das seguintes cinco perguntas. (Podem ser quaisquer).

a) Apresente a pilha TCP/IP e refira pelo menos 5 suportes de protocolos ou serviços de segurança que estejam associados às diferentes camadas da pilha. A sua resposta deve indicar suportes para todos os níveis da pilha.

b) Considere o quadro conceptual de referência OSI X.800:

   B1) Qual a diferença entre os conceitos associados aos mecanismos conhecidos por "Autenticação" (Authentication Exchange) e "Controlo de Acessos" (Access-Control). Como e a qual dos mecanismos associa a funcionalidade de LOGON num sistema LINUX de um dos laboratórios no DI?

   B2) Ainda com base no modelo e terminologia de mecanismos de segruabnça OSI X.800 , qual a diferença entre os chamados mecanismos específicos de segurança (*specific security mechanisms*) e os mecanismos pervasivos de segurança (*pervasive security mechanisms*) ?

c) Um dos aspectos importantes discutidos ao nível da concepção e estruturação de serviços e suportes de segurança é conhecido pelo problema da prevenção de um atacante ter acesso indevido a um perímetro, camada ou serviço devidamente protegidos pelo facto de poder por em causa outro perímetro, camada ou serviço com nível de abstracção inferior no modelo de segurança considerado (the *layer-below* problem). Dê um exemplo de uma aplicação que se baseasse num mecanismo de autenticação e controlo de acessos que possa ser atacada por um processo associado à ideia subjacente.

d) Explique qual a noção que está implícita a ataques do tipo "information leakage" – pode usar na sua resposta um exemplo de estratégia de ataque que pudesse ilustrar ou estar associada à noção desse ataque.

e) Está a construir um protocolo para distribuição de chaves simétricas 3DES para estabelecimento de um canal seguro entre dois sujeitos A e B. As chaves são distribuídas a partir de um centro de distribuição de chaves - KDC (segundo o modelo de Needham-Schroeder com criptografia simétrica). Acontece porém que as chaves de longa duração partilhadas entre os sujeitos A e B e o KDC são chaves simétricas AES, usando blocos de 256 bits e chaves de 256 bits.

   E1) Algum problema com a utilização do modelo de N-S ? Justifique.
   E2) Entre usar ECB e CBC como modo de cifra simétrica para AES no protocolo de N-S qual escolheria neste caso ? Justifique.

Questão 3)

Usando criptografia assimétrica e tendo como pressuposto que as chaves públicas de cada sujeito ou principal podem ser obtidas de forma segura e adequada, é possível estabelecer diferentes tipos de autenticação, normalmente definidos com base em diferentes níveis ou fases: autenticação unilateral ou a uma fase (*one way authentication*), autenticação bilateral em duas fases (*two way authentication*) e autenticação em 3 fases (*three-way authentication*). Considere o protocolo seguinte que ilustra a utilização sucessiva das 3 fases a seguir exemplificados e responda às questões das diversas alíneas.

Kab e Kba são sementes para derivação de chaves simétricas com base em algum gerador para um certo algoritmo criptográfico simétrico.

Fase 1: One Way Authentication

A>B : A {ta, ra, IDB, signedDataA, {Kab}KpubB }

Ta: timestamp gerado por A
IDB: identificador de B
Kab chave de sessão proposta por A

a) Neste round o que proporia que constituísse a parte SignedDataA da mensagem no pressuposto que vai utilizar na prática RSA com chaves de 512 bytes ?
b) Justifique porque é que B atesta neste round a autenticidade de A e da origem da mensagem em A, e que condições estão subjacentes à aceitação de Kab como uma chave simétrica para que B possa trocar mensagens confidenciais com A.
c) Justifique se B até esta fase tem hipóteses de garantir a autenticidade de B.

Fase 2: One Way Authentication

B>A : B {tb, rb, IDA, ra+1, signedDataB, {Kba}KpubA }

tb: timestamp gerado por B
IDA: identificador de A
Kba chave de sessão proposta por B

d) Neste round o que proporia que constituísse a parte SignedDataB da mensagem (vai usar RSA com chaves de 512 bytes)
e) Justifique porque é que A atesta neste *round* a autenticidade de B e da origem da mensagem em B, e que condições estão subjacentes à aceitação de Kba como uma chave simétrica para que A possa trocar mensagens confidenciais com B.
f) Na sua opinião Kab e Kba poderão ser iguais ou não ? Que diferença faria ? Justifique.

Fase 3: Three-Way Authentication

A>B: { rb+1 }Kba

g) Esta mensagem já não acrescenta nada ao protocolo de autenticação mútua ? Tente identificar o interesse desta mensagem no contexto da completude do protocolo de autenticação.
h) Proponha outro formato para esta última mensagem ter o mesmo efeito mas sem que se use cifra simétrica nem as chaves Kba ou Kab. Justifique a resposta.

Questão 4)

Para responder a esta questão tem que considerar o contexto de realização do trabalho prático nº 1 e reflectir nas respostas a partir da sua implementação.

a) Considera que a sua implementação do protocolo de autenticação e distribuição de chaves de sessão para as salas de chat (seja com base no protocolo de N-S com criptografia simétrica ou com base em eventual variantes de extensão do tipo PBEncryption ou geração de chaves com OneTimePads (ou sementes patilhadas – correspondendo às implementações de diferentes grupos) está bem protegida contra ataques de "*message replying*" e de "*message tampering*" ? Justifique a sua resposta com base no suporte e na concretização prática do suporte que concebeu e que vise garantir defesas contra esses ataques.

   Sugestão: apresente a sua implementação o mais detalhada possível num diagrama temporal e diga concretamente como e onde se encontram as defesas contra esses ataques. (No caso de não o ter feito, proponha como deveria ser melhorada a especificação do seu trabalho para a defesa ser mais eficaz). Faça uso da terminologia habitual para representar as mensagens do protocolo.

b) A partir da especificação inicial (geral) do protocolo de N-S com criptografia assimétrica, diga como implementou na prática o protocolo (apresentando a especificação mais detalhada tal como foi realizada na prática), justificando as suas opções de concepção a partir da apresentação geral do protocolo de N-S.

   Sugestão: apresente a sua implementação o mais detalhadamente possível num diagrama temporal. Faça uso da terminologia habitual para representar as mensagens do protocolo.

c) Um dos requisitos do trabalho é que a implementação fosse completamente configurável no que diz respeito à utilização da "suite" criptográfica a usar em cada sala. (Tal podia ser feito por configuração explícita ou por parâmetros passados aos programas, em vez da suite criptográfica ser estaticamente definida no código a compilar).

   Com base na implementação prática que fez, um dos parâmetros que deveriam fazer parte daquela "suite" está associado ao modo de cifra simétrica, sendo assim o modo válido, definido para cada sessão. Assim, o modo de cifra é utilizado dentro de cada sessão, em toda a comunicação confidencial protegida por cifra simétrica.

Justifique em que medida o modo de cifra configurado para uma sessão tem ou não vantagens face aos outros modos de cifra que foram estudados e que poderiam ser utilizados, tendo em conta os padrões de comunicação que estão envolvidos nas sessões. A sua resposta deve ter em conta as características de toda a comunicação confidencial que possa existir numa sessão de chat, de acordo com os requisitos do trabalho.

d)

Esta questão estende o contexto da discussão da alínea c)

Considere agora, no âmbito dos requisitos envolvidos no trabalho, que o ficheiro que pode ser enviado no âmbito das sessões poderia ser de qualquer tipo (texto, mp3, imagens, wma, wav, binários executáveis, etc). Suponha que a sua ferramenta de chat vai ser estendida no futuro para possuir *plugins* que processarão adequadamente as várias extensões, de um modo semelhante aos *plugins* ou suporte nativo de um browser WEB. Ou seja, os referidos plugins desencadearão imediatamente o processamento das diversas extensões do ficheiro transferido (por exemplo, ficheiros mp3 seriam automaticamente ouvidos em tempo real), ficheiros de texto poderiam continuar a ser copiados para disco, etc. Isso teria algum impacto na utilização dos modos de cifra associados às sessões ? Como proporia um suporte mais adequado para esta extensão ?