



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

Mestrado em Engenharia Informática
Segurança em Sistemas Informáticos Distribuídos
1º Semestre 2006/2007

Teste de Avaliação de Conhecimentos (Teste Nº 1 , 18/11/06)

Notas:

- O enunciado tem 5 questões, divididas em duas partes:
 - Parte sem consulta (Parte I, Questão 1): até min
 - Parte com consulta (Parte II , Questões 2 e 3) :até 60 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 folhas entregues: _____ (numere as folhas na forma Número / TOTAL) sem contar com esta capa

Classificação (a preencher pelo docente):

PARTE 1 (s/consulta)	PARTE 2 (com consulta)
-------------------------	---------------------------

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

Questão 1)

- a) Considere a *tabela T1* na qual se apresentam tipos de ataques (colunas) e serviços de segurança (linhas). Coloque um “Y” nos locais apropriados, de modo a que tal indique qual o serviço de segurança que actua como contra-medida ou defesa face aos ataques mencionados (tenha em conta a tabela suplementar já fornecida)
- b) Faça o mesmo que fez na alínea a) mas agora para a *tabela T2*, onde se encontram mecanismos básicos de segurança (colunas) e serviços de segurança (linhas). Tenha novamente em conta a tabela dada.
- c) Em que âmbito se utilizam os algoritmos de cifra simétrica em modo *Stream-Cypher* e porque é que nesse âmbito não é susceptível usar cifra por blocos, nem mesmo usando modos que actuam sobre bytes (ex: OFB, CFB) ?
- d) Indique em que consiste a implementação de um protocolo de cifra simétrica em cadeia bit-a-bit (*Stream-Cypher*) a partir de um método simétrico como AES em modo ECB e chave de 256 bits.

- e) Apresente vantagens e desvantagens dos modos seguintes de cifra simétrica, usados com o método AES, em termos dos seguintes critérios: (1) desempenho (*performance*) (2) recuperação face a erros de transmissão por troca de bits em blocos, (3) recuperação face a perda de bits na transmissão de blocos, (4) recuperação por perda de blocos inteiros na transmissão, (5) incremento do tamanho da cifra produzida, (6) condições de segurança face a criptanálise do tipo “chosen text” (7) utilização num cenário do tipo SSH (segurança numa aplicação interactiva de emulação de terminal) ou chat interativo.

Modos a considerar na comparação: EBC, CBC, CFB, e CTR.

Resposta de acordo com a tabela indicada. Pode incluir na sua resposta (verso da tabela) alguma justificação que ache ser relevante para a sua opção de classificação.

- f) Suponha que um gerador de chaves gerou, para utilização no algoritmo Triple DES com dupla chave DES (112 bits úteis) em modo ECB, a chave seguinte (representada em hexadecimal):

0xFE01FE01FE01FE01FE01FE01FE01

Encontra algum problema na utilização desta chave ? Justifique resumidamente.

- g) Qual a diferença entre as propriedades de “resistência fraca a colisões” e “resistência forte a colisões” numa função segura de síntese ou resumo de mensagens (*Secure Hashing*) ? Qual a outra propriedade base que estas funções devem respeitar ?

- h) Considere o método 3DES, que utiliza a sequência Cifra-Decifra-Cifra nos três passos de aplicação do algoritmo DES. Vê alguma vantagem em que o 2º passo seja a função de Decifrar em vez de Cifrar ?

Questão 2)

- a) Um método de distribuição de chaves como o método de Diffie Hellman é melhor do que o modelo de Needham-Schroeder com criptografia simétrica do ponto de vista de garantias de segurança futura perfeita ? Justifique a sua resposta.
- b) Como sabe, o método de Diffie-Hellman é susceptível de ataques do tipo homem-no-meio, não garantindo, por si só, autenticação entre os dois principais envolvidos numa troca de chaves. Proponha uma solução para prevenir autenticação complementando o protocolo de Diffie-Hellman com um esquema de autenticação e distribuição de chaves segundo o modelo de Needham-Shroeder com criptografia assimétrica de modo a evitar aquele ataque. Apresente numa folha, com um diagrama temporal, como se processaria o protocolo (indicando os passos de processamento ao longo do tempo considerando as entidades envolvidas: PKC, A e B).
- c) Suponha que implementava o protocolo de Needham-Shroeder para distribuição segura de chaves entre dois principais A e B, nas duas variantes estudadas: com criptografia simétrica e assimétrica. Suponha que, em ambas as implementações, a sua implementação omitiu as duas últimas mensagens da especificação do protocolo (ou seja, as duas últimas mensagens que são trocadas entre os principais A e B conforme a especificação de referência). A verdade é que sem essas duas mensagens, A e B estão aptos a usar uma chave secreta partilhada. Será que essas mensagens não são mesmo necessárias ?

Questão 3) A responder em folhas a anexar.

Considere o trabalho prático nº 1 e a implementação que está subjacente à entrega da sua implementação até à 1ª data de referência para entrega do trabalho.

- a) Considere a implementação do protocolo de autenticação e distribuição de chaves em grupo com base na utilização do protocolo de Needham-Schroeder (parte 1, com criptografia simétrica). Diga se, em todo o fluxo de mensagens e durante as sessões seguras de CHAT a sua implementação resiste a ataques à integridade das mensagens? Se sim, justifique porquê. Se não, diga o que deveria mudar para que a integridade das mensagens pudesse ficar assegurada.

- b) Justifique e critique as garantias (ou falta delas) associadas a prevenir segurança futura perfeita em grupo, tendo em conta todas as propriedades subjacentes a esse conceito.

Service	mechanism							
	Enciph- erment	Digital signature	Access control	Data integrity	Authenti- cation exchange	Traffic padding	Routing control	Notari- zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

Tabela fornecida: Relação entre serviços de segurança e mecanismos.

Tabela T1: Para preencher como resposta à questão 1 a):

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

Tabela T2: Para preencher como resposta à questão 1 b):

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						