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

Curso de Engenharia Informática (2º Ciclo)

Segurança em Sistemas e Redes de Computadores

SSRC-0910-EN-1.2-A

1º Semestre 2009/2010

TESTE DE AVALIAÇÃO / FREQUÊNCIA Nº 1

2ª Chamada, 17/11/09

Teste sobre os aspectos e tópicos relacionados com a realização do Trabalho Prático nº 2

Notas:

- O enunciado tem 2 Grupos:
  - PARTE I: Constituído por 3 questões sem consulta (10 valores)
  - PARTE II: Constituído por 3 questões com consulta (10 valores)
- Duração: 1 hora para cada uma das partes. As partes serão separadas por um intervalo.

---------- A preencher pelos alunos no final do teste ----------

Nº de aluno: _____ Nome: _____

Nº TOTAL de páginas entregues (exceptuando esta capa): _____

Obs: numere as páginas na forma nº da página /Nº TOTAL e coloque o nº e nome em cada folha.

---------- A preencher pelo docente ----------

Parte 1	**Parte II Q5**	**Parte II Q6**	**Parte II Q7**	**TOTAL**
Q1 Q2 Q3 Q4				

INF Controlo:

PARTE SEM CONSULTA (até 60 min no máximo)

Questão 1)

O método 3DES (ou TDEA), consiste na aplicação encadeada de três operações de cifra de blocos DES (ou DEA), pela ordem CIFRA-DECIFRA-CIFRA. Numa Framework de suporte de programação com criptografia (ex., JAVA/JCE), podem aplicar-se chaves de 112 ou 168 bits à implementação 3DES.

a) Como se processa a chave no encadeamento das operações de cifra, quando se utiliza uma chave de 112 bits?
b) Como se processa a chave no encadeamento das operações de cifra, quando se utiliza uma chave de 168 bits?
c) Qual a razão de ser do encadeamento CIFRA-DECIFRA-CIFRA ? Ou porque é que não se aplica o encadeamento na forma CIFRA-CIFRA-CIFRA, por exemplo ?
d) Uma variante mais leve será usar 3DES ou TDEA apenas com duplo encadeamento de cifra, por exemplo CIFRA-CIFRA com uma chave de 112 bits. Porque é que essa opção não é assim tão interessante ?
e) Um método como o 3DES pode ser usado, de forma similar, sobre qualquer outro algoritmo criptográfico simétrico por blocos. Que razão encontra para o facto de não ser usual este método ser aplicado, por exemplo a outros algoritmos, como por exemplo o AES (sob a forma de um 3AES?

Questão 2)

a) No processamento HMAC (RFC 2104) para cálculo de códigos de autenticação de mensagens entre dois principais, aplica-se um encadeamento de duas funções de síntese. A estrutura interna do cálculo permite a sua utilização com quaisquer funções de síntese, desde que usadas chaves partilhadas de dimensão adequada. Qual a principal vantagem desta flexibilidade ? Justifique.
b) Diga qual a diferença entre as propriedades de resistência forte a colisões e resistência fraca a colisões de um algoritmo de síntese segura de mensagens. Qual das propriedades é particularmente importante no caso de utilizar um método de síntese subjacente a uma assinatura digital de chave pública para efeitos de se produzirem assinaturas de código executável (exemplo distribuição de pacotes de software descarregáveis da internet para instalação num computador). Justifique.

Questão 3)

Uma forma de proteger um acordo contributivo de estabelecimento de chaves baseado no método de Diffie-Hellman de um ataque à autenticação e integridade do tipo "homem no meio" é apresentada no seguinte protocolo:

A > B: A || B || Ya || nA || NULL || { H(A ,B, Ya, nonce A, NULL)} KprivA
B > A: B || A || Yb || nA+1 || nB || { H(B, A, Yb, nonceA+1, NonceB)}KprivB

a) Na sequência da troca de mensagens A e B poderão calcular e partilhar uma chave de sessão Ks, por exemplo para utilziação do método AES durante a sessão a estabelecer. Como seria calculada a chave de sessão ?

b) Para que o "homem no meio" conseguisse o intento de quebrar a autenticação entre A e B e vir a apoderar-se da chave de sessão Ks, o que teria que fazer ? Justifique referindo como poderia ter lugar um possível ataque que fosse desencadeado com sucesso para o efeito desejado.

c) Suponha que, no protocolo anterior, A e B possuem mais do que um certificado de chave pública emitido por diferentes CAs e que utilizam habitualmente as diferentes chaves públicas. Neste caso, o que seria necessário adicionar ao protocolo ? Justifique

d) Suponha que numa aplicação que está a desenvolver e que utiliza o acordo de estabelecimento de chaves referido, precisa de limitar o tamanho das mensagens trocadas a 1 Kbyte e serem enviadas num único datagrama UDP. Considere que cada certificado de chave pública possui 2 Kbits para atestar chaves públicas de 1Kbit. Como resolveria o problema ? Justifique.

Questão 4)

Considere que precisa de estender o acordo de D-H a quatro entidades (que representam 4 nós na rede Internet) e que necessitam de realizar um acordo do tipo contributivo para distribuição e estabelecimento de chaves, com base no método de Diffie-Hellman. Os quatro nós não podem comunicar por broadcast ou multicast, apenas podendo realizar interacções par-a-par.

Apresente uma solução para um protocolo que permitisse resolver o problema. Apresente a sua solução justificando o funcionamento do protocolo, demonstrando que o mesmo funciona para o fim em vista. Na sua justificação faça as considerações que achar necessárias para a demonstração do funcionamento do protocolo.

PARTE COM CONSULTA (até 60 min no máximo)

Questão 5

O seguinte código exemplifica o estabelecimento do acordo de D-H com base no suporte JAVA/JCE, estendido a três entidades (A, B e C).

http://asc.di.fct.unl.pt/ssrc/classes/other-materials/SSRC/aprat/DH/

ThreeWayDHExample.java

Apresente uma solução para estender o acordo a 4 entidades.

Questão 6

Considere que pretende conceber uma solução para proteger um protocolo como o ARP ou RARP de ataques com a tipologia referente ao modelo OSI X.800.

Apresente como conceberia uma solução para o protocolo. Tenha como referência para a sua solução o protocolo ARP.
Tenha por base o seu conhecimento prévio de operação do protocolo ARP
(ex., http://en.wikipedia.org/wiki/Arp_protocol)

Questão 6

Considere o contexto do trabalho prático e a solução para a fase II.

Considere que a sua implementação vai ser transportada para UDP, passando todas as entidades envolvidas a comunicar com base em sockets UDP.

a) As propriedades de segurança (protecção contra adversários do tipo Dolev-Yao ou modelo de ataques OSI X.800 ou RFC 2828 ao canal de comunicação entre todos os processos envolvidos) do seu protocolo mantêm-se ? Justifique
b) Se respondeu negativamente a a), que diferenças proporia para garantir as mesmas propriedades de segurança.