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

Curso de Mestrado em Engenharia Informática (2º Ciclo)

Segurança em Sistemas e Redes de Computadores

1º Semestre - 2011/2012

TESTE DE FREQUÊNCIA Nº 1

Teste individual
Duração do teste: 2 horas

- **Questões do grupo I: sem consulta (1 hora)**
- **Questões do grupo II: com consulta (1 hora).**
  - Apenas podem ser consultados elementos individuais, não sendo permitida nenhuma forma de comunicação entre os alunos.

Nº de aluno	Nome:	
LEI/MEI:	Grupo (trabalho prático):	Nº de páginas entregues:

As páginas devem ser numeradas, no canto superior direito, na forma: Nº Página / Total de Páginas, não contando com esta página.

Tabela e critérios de avaliação (a ser preenchido pelo docente)

GRUPO 1 (respostas sem consulta)					

GRUPO 2 (respostas com consulta)					

GRUPO I – Questões para resposta sem consulta

Questão 1

Considere a utilização de um esquema do tipo PBE (*Password-Based Encryption*), tal como foi estudado ou exemplificado em aula e tendo em conta a forma como possa ter sido usado na implementação do seu trabalho prático TP1.

a) Em que se baseia genericamente este esquema e qual o objetivo do mesmo? Exemplifique com o contexto do uso na sua implementação do trabalho prático TP1.
b) A partir da sua resposta anterior, esquematize (por exemplo, com recurso a um diagrama de blocos genérico o respectivo processamento criptográfico e os parâmetros de entrada e resultado do processamento), do modo como foi usado no seu trabalho prático.
c) De acordo com o suporte JAVA-JCE, o esquema apresentado em b), refere-se a um modelo do tipo *PBE-Encryption* com Parâmetros (ou parâmetros explícitos) ou *PBE-Encryption* sem Parâmetros (ou parâmetros implícitos). Justifique.
d) Repetindo o diagrama de blocos e a partir da sua resposta a b) e c), tente instanciar e antecipar que tipo de algoritmos e operações criptográficas específicas bem como respectivos parâmetros ou resultados (entrada/saída dos blocos) terão lugar, se parametrizar o esquema com base nas seguintes opções (configurações disponíveis numa base real de instalação JAVA-JCE com diversos provedores criptográficos instalados):

   D1) PBEWITHSHA256AND256BITAES-CBC-BC
   D2) PBEWITHSHAAND2-KEYTRIPLEDES-CBC

Questão 2

a) Comparativamente entre usar *padding* PKCS5 ou PKCS7 qual o que considera mais seguro? Na implementação do seu trabalho isso tem relevância ? Justifique.
b) Em que circunstâncias deve privilegiar o uso do modo de cifra ECB em vez de CBC ? Na implementação do seu trabalho a configuração de um ou outro modo tem relevância ? Justifique.
c) Em que circunstâncias ou com que vantagens acha que será preferível o uso do modo de cifra CTR em vez de CFB? Na implementação do seu trabalho isso tem relevância? Justifique.
d) Na sua implementação do TP1, está garantido que mesmo que um utilizador legítimo numa sala e CHAT envie uma mesma mensagem, a mensagem cifrada (*ciphertext*) enviada pela rede seja sempre diferente ? Porquê ou em que circunstâncias isso é ou não é garantido? Porquê?

Questão 3

a) Nas aulas foi abordado como se pode usar uma técnica designada por *KeyWrapping*. No contexto do seu trabalho um esquema do tipo *KeyWrapping* poderia substituir o uso do esquema *PBE* tendo em vista o fim para o qual este foi usado? Se sim, teria vantagens ? Teria desvantagens ? Justifique.
b) Suponha que o seu trabalho (TP1) vai executar num ambiente em que algumas máquinas dos utilizadores possuem provedores criptográficos instalados (JAVA-JCE) que incluem apenas o algoritmo DES. No entanto, o servidor onde vai executar o KDC tem sessões configuradas para a *ciphersuite*: 3DES/192/CBC/PKCS#1. Se toda a restante suíte criptográfica (CBC e PKCS#1) estiver garantida, seria possível propiciar àqueles utilizadores, uma vez autorizados e autenticados, poderem participar nessas sessões (sem atualizar o seu software)? Indique como.

GRUPO II – Questões para resposta com consulta

Entre as questões 6 e 7 deve escolher e responder a apenas uma delas durante o teste e fazer outra como trabalho de casa (a entregar por Email).

Questão 4

Considere a implementação do seu trabalho TP1.

Suponha que um utilizador que pretende usar a sua a implementação lhe pede informação sobre boas práticas ou fundamentos para configurar *ciphersuites* adequadas de acordo com o suporte JAVA (JCE) disponível, nomeadamente cifras, modos de operação de blocos, *padding* e modos a utilizar, para:

- C1) A configuração do suporte JAVA (JCE) para o protocolo de autenticação e distribuição de chaves subjacente à entrada nas sessões (de acordo com o modelo e protocolo de distribuição de chaves implementado)
- C2) Para configuração do protocolo de comunicação referente ao suporte de segurança das sessões de CHAT

Que princípios ou boas práticas de configuração aconselharia na escolha comparativa de *ciphersuites* para C1 e C2 ? Justifique.

Questão 5

Consulte o exemplo de código JAVA que usa o suporte JAVA/JCE que se encontra em:
http://asc.di.fct.unl.pt/ssrc/classes/labmaterials/SSRC/aprat/hashing-macs/TamperedExamples-DigestSchemes/TamperedWithDigestExample.java

Este programa simula uma demonstração prática de um ataque com sucesso à integridade de uma mensagem confidencial trocada entre dois principais (A – emissor e B – receptor) que partilham uma chave simétrica e usam o algoritmo AES em modo CTR (sem *padding*). Os dois principais pretenderiam que a sua mensagem fosse verificável na sua integridade, uma vez que para o efeito usam SHA-1 para proceder a uma síntese criptográfica da mensagem enviada.

Este tipo de ataque poderia ter sucesso em relação a uma atacante externo (nas condições de um adversário com a capacidade de produzir ataques conforme a framework X.800 e que pudesse atuar como "*homem-no-meio*") em relação às mensagens trocadas pelos utilizadores legítimos das sessões seguras de chat, na sua implementação do trabalho TP1? Justifique.

Questão 6
Consulte o exemplo de código JAVA que usa o suporte JAVA/JCE que se encontra em:
http://asc.di.fct.unl.pt/ssrc/classes/labmaterials/SSRC/aprat/hashing-macs/MacExample/CipherMacExample.java

a) O tipo de ataque simulado anteriormente (questão 5) poderia ser também realizado com o modelo CMAC e um tipo de configuração de *ciphersuites*, tal como o programa sugere? Se não, justifique porque não. Se sim, justifique porquê e que providências tomaria para o evitar.
b) Que vantagens ou desvantagens haveria em usar um modelo do tipo CMAC em vez de HMAC para implementação de códigos de autenticação de mensagens e provas da sua integridade, na sua implementação do TP1.

Questão 7
Considere uma vez mais a implementação do seu trabalho TP1.
Considere também o código exemplificado em:
http://asc.di.fct.unl.pt/ssrc/classes/labmaterials/SSRC/aprat/EX6/SimpleStreamExample.java

a) Com base na interpretação que faz deste programa e *ciphersuite* usada (ARC4/BC, sem *padding* e sem modo), acha que este tipo de implementação e ciphersuite poderia ser usada para suportar a segurança nas suas salas de chat? Teria vantagens ou desvantagens? Porquê?
b) Mantém a anterior argumentação, mesmo face a uma possível configuração da *ciphersuite* do seu trabalho que envolvesse cifra de blocos e um modo de cifra de blocos do tipo CTR? Justifique.