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
(Computer Systems and Networks Securty, MSc Level)

Exame – Época Normal 2010/2011

(Chamada 1, 21/Dez/2010)

Duração: 3h00
O exame está dividido em duas partes

- Parte 1 – Sem consulta, com duração de 1h30. Pode escolher 8 das 9 questões do enunciado.
- Parte 2 – Com consulta, com duração de 1h30. Pode escolher 4 das 5 questões do enunciado.

Student Number:	Name:	
LEI/MEI:	Group: SSTC-G____	Total number of pages:

You should number each page in the form: Page Number/TOTAL

EVALUATION TABLE (to be used by the teacher)

Parte I (Sem consulta)									

Parte II (Com consulta)									

Parte sem consulta

Questão 1
Pretende-se usar um algoritmo de cifra simétrica para cifrar muitos ficheiros de grande dimensão (por exemplo, para fazer um backup cifrado de muitos milhares de ficheiros de centenas de *Hosts* de um *DataCenter*). Pretende-se usar um modo de cifra de blocos, com características e propriedades de segurança semelhantes ao modo CBC, com blocos B correspondentes ao bloco base do algoritmo usado (ex., 128 bits de bloco, algoritmo AES).

Cada ficheiro terá que ser cifrado individualmente com uma chave diferente, obtida a partir da cifra do tamanho do ficheiro com uma chave mestra (ex., AES) sendo esta chave mestra a mesma para todos os ficheiros de um memo backup. A dimensão de cada ficheiro do arquivo não corresponde naturalmente a um múltiplo do bloco base do algoritmo usado, pelo que será necessário usar *padding*.

O problema de usar CBC é que, para cada ficheiro, será sempre adicionado mais um bloco (independentemente do método de *padding* a usar), adicionando-se assim NxB bits para obter a cifra de todos os ficheiros, em que N é da ordem de milhares.

Pretende-se no entanto que a cifra de todos os ficheiros tenha exactamente o mesmo tamanho dos ficheiros originais e cada ficheiro cifrado possua exactamente o mesmo tamanho do original. Mantendo as mesmas propriedades e características de segurança do modo CBC, que solução proporia para este problema, de modo que seja possível obter os ficheiros originais ? Justifique e argumente sobre a vantagem da solução proposta.

Questão 2
Qual a diferença (vantagens, desvantagens ou limitações) entre usar os seguintes métodos de *padding* no caso de utilizar um método de cifra simétrico com modo de cifra por blocos CBC:

a) *Padding* com bytes colocados a zero (0x00)
b) *Padding* PKCS#5
c) *Padding* PKCS#7

Questão 3
Apresente comparativamente vantagens e desvantagens entre os modos de cifra simétrica seguintes, em termos do seguintes critérios: (1) recuperação de erros de cifra, (2) desempenho (*performance*) (3) recuperação face a erros de transmissão por troca de bits em blocos, (4) recuperação face a perda de bits em blocos, (5) incremento do tamanho da cifra produzida e (6) maior robustez de segurança, face à utilização dos seguintes modos de cifra: EBC, CBC e CTR.

Questão 4
Usando a caracterização da *framework* OSI X.800, que diferença existe entre as seguintes noções, dando exemplos concretos das mesmas no que diz respeito a protecção por parte de protocolos e serviços de segurança à sua escolha que protejam face a cada uma das noções. Nota: pode utilizar exemplos de serviços e protocolos de segurança, a diferentes níveis da pilha TCP/IP (nível rede até nível aplicação).

a) *Peer Entity Authentication* vs. *Data Origin Authentication*
b) *Connection Confidentiality* vs. *Selective-Field Confidentiality*
c) Connection Integrity without recovery vs. *Connection Integrity with recovery*

Questão 5

a) Um algoritmo de cifra simétrica por blocos, operado no modo CBC, pode ser utilizado como componente para construir um método de cifra em cadeia, de modo a poder cifrar-se continuamente um fluxo de dados, quando esses dados têm que ser transmitidos bit a bit, para serem depois decifrados igualmente numa cadeia, bit a bit. Suponha por exemplo que se trata de um fluxo contínuo de dados, do tipo uma *stream* de vídeo transmitida e consumida em tempo real. Descreva como se pode implementar um tal algoritmo de cifra em cadeia para comunicação em tempo real, no pressuposto que o emissor e o receptor já possuem uma chave partilhada.

b) A solução em b) é mais ou menos adequada comparativamente a usar cifra de blocos OFB, CFB ou CTR.

Questão 6

Diga, para cada um dos eventuais ataques indicados, em que consiste o suporte de defesas no protocolo SSL:

A1) *Message Replaying* de records SSL
A2) *Man-In-the-Middle*, com ataque à autenticação, seja do tipo "*peer-entity authentication*" seja do tipo "*data-origin authentication*"
A3) IP *Spoofing*
A4) IP *Hijacking* com possibilidade de controlo da conexão SSL tomando o atacante o lugar do endereço IP de um dos extremos da sessão, após o estabelecimento da sessão.
A5) DoS provocado por um ataque do tipo *SYN-flooding* à conexão TCP subjacente ao protocolo SSL
A6) Message *tampering* de records SSL (RLP)
A7) Ataque provocando desordenação de *records* SSL no meio de uma sessão SSL (note que o transporte subjacente seja TCP ou UDP)

Questão 7

Uma função de síntese segura tem como propriedade importante a conversão de qualquer informação de entrada de tamanho arbitrário numa síntese de comprimento fixo.

É possível compatibilizar essa característica com o facto de se pretender que uma função de síntese segura deva ainda possuir propriedades de resistência fraca e resistência forte a colisões ? Justifique a sua resposta tendo por base as garantias destas propriedades.

Questão 8

Em que consistem as seguintes noções, no processamento e gestão de confiança de chaves públicas (chaveiro de chaves públicas) inerente ao sistema PGP e ao seu modelo de gestão de confiança *Web of Trust.*

a) Key legitimacy
b) Signature Trust
c) Owner Trust

Questão 9

Quando se usa o sistema PGP para garantir autenticação, integridade e confidencialidade de mensagens Email e se quer também usar compressão das mesmas, a compressão das mensagens para serem enviadas é sempre realizada depois da assinatura e antes da sua encriptação. Porquê ? Justifique adequadamente a sua resposta.

Parte com consulta

Questão 1

a) No sistema PGP como calcularia a probabilidade de um utilizador que possua vários pares de chaves públicas possa correr o perigo de se verificar uma colisão no *KeyID* usado por diferentes parceiros que lhe enviem mensagens e que possam estar a usar indiscriminadamente as várias chaves públicas dos seus pares.
b) Os primeiros 16 bits da síntese (*digest*) de uma assinatura numa mensagem PGP podem ser passados em claro. Em que medida esta situação compromete a segurança do algoritmo de síntese utilizado ? Justifique.
c) Porque é que a situação descrita em b) pode revelar-se importante para ajudar na determinação da chave correcta, no caso de utilizadores que estejam a usar diferentes pares de chaves, nos moldes inicialmente referidos em a) ?

Questão 2

Inspire-se o esquema de assinaturas duais do protocolo SET para sugerir como poderia fazer uma assinatura múltipla, em que uma mesma mensagem com várias partes seja enviada por PGP a N destinatários mas apenas fosse revelado a cada destinatário a parte que lhe diz respeito, mantendo-se intrinsecamente todas as propriedades de segurança do sistema PGP mas adicionando-se um mecanismo de controlo de privacidade das partes das mensagens reveladas aos diferentes subscritores.

Para responder a esta questão, represente como seria o formato estendido de uma mensagem PGP para integrar o mecanismo inspirado nas assinaturas duais, de forma a propor um formato estendido para a estrutura das mensagens.

Questão 3

Suponha que lhe pedem para fazer uma implementação de cifra de blocos de 512 bits e chave de 512 bits, tendo como bloco base uma função de síntese do tipo SHA-512. Neste caso, a ideia seria usar blocos de entrada de 512 bits e a chave de 512 bits, para obter um bloco *ciphertext* de 512 bits. Note que as funções de síntese possuem como propriedade importante a propriedade de irreversibilidade.

Apresente uma possível solução e argumente sobre a sua eficiência e segurança, comparativamente às propriedades usuais das cifras de blocos.

Questão 4

Entre os diversos modos de autenticação (*RSA, Fixed Diffie Hellman e Ephemeral Diffie Hellman*) normalizados em TLS (ou SSL), qual o que considera:

a) Ser mais eficiente (maior desempenho computacional)
b) Ser mais seguro
c) Ter melhores garantias de segurança futura e passada perfeitas

Justifique para cada caso a sua resposta.

Questão 5

a) Interceptou-se nu canal uma mensagem *ciphertext* (C) cifrada com RSA, tendo C uma representação em valor inteiro = 10. A mensagem foi enviada por A para B na forma {P}KpubB e sabe-se que a chave pública corresponde ao valor inteiro = 5, com módulo 35. Qual era a mensagem P ?
b) Considerando ainda o algoritmo RSA e conhecendo-se que a chave pública de um principal corresponde ao valor inteiro = 31, com módulo 3599, como poderia a partir destes dados saber qual a chave privada desse principal ?