

**DI/FCT/UNL**  
**Mestrado Integrado em Engenharia Informática**  
**Segurança de Redes e Sistemas de Computadores**  
**2º Semestre, 2016/2017**  
**Teste de frequência nº 1 (26/Abril/2017)**

**Parte I (parte sem consulta) - Duração: 1 hora**

**Questão 1**

No processamento do modo CFB em operações de cifra com algoritmos simétricos de bloco (ou *block-ciphers*), a cifra com a função de cifra  $E(\cdot)$  de um bloco de dados  $P_i$  (*plaintext*) de qualquer tamanho superior a 8 bits, com a chave  $K$  é obtida da seguinte forma:

$$C_i = P_i \text{ XOR } \{ E_K ( S ( P_{i-1} ) ) \}$$

Recorde que que a função  $S ( P_{i-1} ) = P_{i-1}$  no caso de  $P_{i-1}$  for um bloco de 8 bits.

- a) Em que consiste o processamento  $S(\cdot)$  em geral para blocos de tamanho diferente de 8 bits ?
- b) Escreva a expressão para obter na decifra um bloco  $P_i$  (*plaintext*) dado o bloco  $C_i$  (*ciphertext*).
- c) Uma das vantagens de usar o modo CTR para além da sua eficiência e da possibilidade de uso para cifrar tráfego iterativo (exemplo em sessões do tipo SSH) é: (i) a possibilidade de cifrar e decifrar usando apenas a implementação da função de cifra de qualquer algoritmo criptográfico simétrico de bloco (não sendo preciso a função de decifra) e (ii) permitir processar qualquer bloco  $i$  da informação *plaintext* e *ciphertext* com acesso aleatório e paralisável aos blocos cifrados.

VERDADEIRO OU FALSO ? Justifique, com base no referido em i) e ii).

**Questão 2**

**AES, Blowfish, RC4, Triple DES, RC5, A5/1, A5/2, RC6, Toofish, Camelia**

- a) Dos algoritmos criptográficos simétricos apresentados, indique os que não identifica como sendo algoritmos de cifra de blocos (block cipher).
- b) De entre os algoritmos de cifra de blocos apresentados, apresente pelo menos três que podem ser utilizados com chaves de diferentes dimensões.

**Questão 3**

No algoritmo Triple DES, a ordem das operações básicas DES na estrutura do algoritmo seguem a seguinte ordem: E-D-E (*Encryption-Decryption-Encryption*).

- a) Supondo que se usa uma chave de 112 bits, como é operada a chave nessa estrutura ?
- b) Que vantagens tem a ordem indicada comparativamente a usar outras, como por exemplo: E-E-E ou E-D-D ? Justifique.
- c) Pode o algoritmo Triple DES sofrer do mesmo problema de diminuição de segurança do algoritmo DES conhecido como problema das chaves fracas, sem-fracas ou potencialmente fracas? Justifique.

**Questão 4**

Considere especificação do trabalho prático nº 1 - FASE 2 - referente ao suporte criptográfico usado para autenticação de utilizadores e obtenção de *ciphersuites*, parâmetros e chaves para as sessões de comunicação segura multi-ponto (com base em IP *multicast*).

- a) De acordo com a especificação ou a sua implementação assegura-se os critérios de segurança futura perfeita e segurança passada perfeita na confidencialidade da comunicação multicast ? Justifique.

- b) Independentemente de ter ou não ensaiado na sua avaliação experimental o uso de algoritmos simétricos do tipo cifras em cadeia (ou *stream-ciphers*), vê alguma limitação em que a sua implementação possa utilizar um algoritmo desse tipo, por exemplo, RC4, em vez dos algoritmos simétricos de cifra de blocos? Justifique, indicando no caso de ser possível como configura o ficheiro de ciphersuite.conf com uma ciphersuite válida para uso do algoritmo RC4.

*Sugestão: Para responder a b) pode ter em conta o programa em JAVA abaixo que demonstra uma operação de cifra e decifra com RC4, usando código similar ao usado nas aulas práticas.*

- c) No seu trabalho deverá ser possível utilizar como funções MAC para autenticidade e integridade de mensagens, quer construções de algoritmos HMAC , quer construções CMAC. Que diferenças têm estas duas opções do ponto de vista de segurança e desempenho
- d) Na utilização de vários esquemas normalizados de HMAC podem usar-se combinações de duas (ou mais) funções de síntese seguras como base de suporte de segurança para autenticidade rápida e integridade de mensagens num canal seguro ? Qual a vantagem prática em usar esquemas que permitem combinar funções de síntese diferentes ?

```
public class SimpleStreamExample
{
    public static void main(
        String[] args)
        throws Exception
    {
        byte[] input = new byte[] {
            0x00, 0x11, 0x22, 0x33, 0x44, 0x55, 0x66, 0x77,
            (byte)0x88, (byte)0x99, (byte)0xaa, (byte)0xbb,
            (byte)0xcc, (byte)0xdd, (byte)0xee, (byte)0xff };
        byte[] keyBytes = new byte[] {
            0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07,
            0x08, 0x09, 0x0a, 0x0b, 0x0c, 0x0d, 0x0e, 0x0f };

        SecretKeySpec key = new SecretKeySpec(keyBytes, "ARC4");
        Cipher cipher = Cipher.getInstance("ARC4","BC");
        System.out.println("input text : " + Utils.toHexString(input));

        // encryption
        byte[] cipherText = new byte[input.length];
        cipher.init(Cipher.ENCRYPT_MODE, key);
        int ctLength = cipher.update(input, 0, input.length, cipherText, 0);
        ctLength += cipher.doFinal(cipherText, ctLength);
        System.out.println("cipher text: " + Utils.toHexString(cipherText) + " bytes: " +
            ctLength);

        // decryption pass
        byte[] plainText = new byte[ctLength];
        cipher.init(Cipher.DECRYPT_MODE, key);
        int ptLength = cipher.update(cipherText, 0, ctLength, plainText, 0);
        ptLength += cipher.doFinal(plainText, ptLength);
        System.out.println("plain text : " + Utils.toHexString(plainText) + " bytes: " +
            ptLength);
    }
}
```

**Parte II (parte com consulta) - Duração: 30 m****Questão 5**

- Comparativamente ao uso de um único serviço KDC num protocolo de autenticação e distribuição de chaves, como é por exemplo o caso do protocolo de Needham-Schroeder para utilização com criptografia simétrica, que vantagens encontra em desdobrar esse papel nas entidades AS e TGS no caso de um protocolo como o Kerberos V4 ? Note que nesta versão não possui ainda a noção de reinos ou domínios Kerberos
- Na comparação entre os protocolos Kerberos V4 e V5, várias alterações relevantes foram consideradas, sendo uma delas o abandono de uso de TIMESTAMPS, passando a usar-se controlos de desafios baseados em NONCES. Que vantagens essa alteração propicia do ponto de vista do modelo de hipóteses do atacante, na tentativa de atacar o protocolo ? Justifique.
- Considere que pretende substituir no sistema Kerberos o processo de geração da chave simétrica na fase de *authentication-exchange* (entre o cliente e o servidor AS), de modo a poder usar um esquema do tipo Password Based Encryption. Diga como proporia fazer essa alteração indicando que setup ou que alterações seriam necessárias para acomodar essa solução.

**Questão 6**

- Alice envia a Bob mensagens  $M$  cifradas (com base no algoritmo AES e modo CBC) com proteção de provas de autenticidade e integridade usando uma de duas possibilidades: baseada numa construção HMAC (implementando o standard RFC 2104) (
 
$$\{M\}_{K_1} \parallel \text{HMAC}_{K_2}(M) \quad \text{ou} \quad \{M\}_{K_1} \parallel \text{CMAC}_{K_2}(M)$$

Na utilização das provas de autenticidade e integridade de mensagens usando HMAC é importante que as funções de síntese seguras implícitas à parametrização do esquema HMAC tenham a propriedade de resistência forte a colisões ou bastará que garantam resistência fraca a colisões ? Justifique a sua resposta.

**Parte III (contexto do trabalho prático nº 1) - Duração: 30 m****Questão 7**

Indique no seu trabalho como configuraria o sistema implementado (ao nível dos vários ficheiros de configuração) de modo a utilizar o algoritmo criptográfico CAMELIA, usando o modo CTR, Padding PKCS7 e com uma chave de 128 bits. Indique como é que fornece o vetor de inicialização (ou contador inicial) para este modo na sua implementação.

**Questão 8**

Pretendia substituir a especificação e implementação da FASE 2 do seu trabalho, com base na integração na sua solução do sistema Kerberos V5. Para o efeito, o seu servidor de autenticação irá ser substituído por um servidor Kerberos, nomeadamente pelo componente AS (Authentication Server), mantendo inalteráveis as rondas Authentication Exchange e do protocolo Kerberos bem como a ronda de Ticket-

Como se proporia integrar esse sistema de modo a suportar as sessões de CHAT seguras, com as mesmas garantias providenciadas pela atual solução ?