DI/FCT/UNL
Mestrado Integrado em Engenharia Informática
Segurança de Redes e Sistemas de Computadores 1º Sem, 2020/2021
Teste de frequência nº1, 14/NOV/2020

Copie o seguinte código em cada uma das suas folhas de resposta que devem ser entregues agrafadas com o enunciado

T1-R1-AB37CF

PARTE I - PARTE SEM CONSULTA

Questão 1

Apresente em a) e b) definições que caracterizem e permitam diferenciar com clareza as seguintes propriedades de segurança, a partir das noções da Framework conceptual X.800 e que podem estar associadas a protocolos e canais de comunicação seguros. Se entender, pode apresentar opcionalmente, para além da definição, mecanismos criptográficos, exemplos ou casos concretos que ilustrem e complementem a sua definição.

a)
- A1) Integridade seletiva orientada à conexão (*selective field connection integrity*)
- A2) Confidencialidade não orientada à conexão (*connectionless integrity*)

b)
- B1) Confidencialidade de tráfego (*traffic-flow confidentiality)*
- B2) Confidencialidade de dados ou mensagens (*message or data confidentiality)*

c) A utilização de um mecanismo baseado numa construção criptográfica do tipo CMAC garante integridade de tráfego num protocolo com múltiplas rondas de mensagens trocadas entre dois principais? Verdadeiro ou falso? Argumente.

d) Um algoritmo criptográfico assimétrico envolvendo curvas elípticas, como é o caso da construção ECDSA, permite o seu uso para assegurar confidencialidade de tráfego? Verdadeiro ou falso? Argumente.

e) A utilização de construções HMAC em mensagens trocadas entre dois principais que usam chaves partilhadas (MAC *keys*) previamente distribuídas em segurança, permite assegurar propriedades de não-repudiação. Verdadeiro ou Falso? Justifique.

Questão 2

Considere uma mensagem M trocada entre dois principais (correspondendo ao envio de A para B) e que foi protegida com as seguintes construções criptográficas nos componentes C_i apresentados:

$$IV \,||\, E_{K1}(\, M \,||\, Nonce_A \,||\, HMAC\text{-}SHA\text{-}384_{K2}\,(M)\,) \,||\, SHA\text{-}512\,(\,C4\,)$$

$$\underbrace{\quad}_{C1} \quad \underbrace{\qquad\qquad}_{C2} \quad \underbrace{\qquad\qquad\qquad}_{C3} \quad \underbrace{\qquad\qquad}_{C5}$$

$$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{C4}$$

Sabendo que:

- || representa concatenação;
- IV : é um vetor de inicialização;
- E_K (...) : resultado de uma cifra simétrica AES, sendo usado em modo GCM, com uma chave K de 256 bits e sem utilização de *padding*. Notar que este algoritmo processa blocos de 128 bits. A chave K foi estabelecida previamente através de um protocolo de distribuição de chaves, que usou um acordo *Diffie-Hellman* pcom autenticação de A e B nesse estabelecimento.
- $Nonce_A$: é um *nonce* com 128 bits, gerado pelo emissor A, a partir de uma função baseada num algoritmo de geração pseudo-aleatória e que será memorizado pelo recetor para controlo de não retransmissão ilícita da mensagem
- SHA-512: é a função de síntese de segurança SHA-512.
- HMAC-SHA-384_{K2}: resultado da computação HMAC, utilizando uma função de síntese SHA-384 e utilizando K2 como a chave Kmac. A chave Kmac foi gerada na forma K2 = SHA-512(K1)
- C4: Corresponde a C2 || C3

a) Poderá o componente C5 ser usado de forma a que o destinatário possa mitigar ataques DoS por simples modificação (*tampering*) da mensagem por parte de um atacante no canal que apenas pretende levar o destinatário a realizar computações criptográficas inúteis para fazer a deteção do ataque de *tampering*? Justifique.

b) A partir dos dados, qual será o tamanho do componente C1? Justifique.

c) Se a mensagem M tiver 2048 bits qual será o tamanho do componente *ciphertext* C4? Justifique.

d) Se a mensagem M tiver 824 bits, qual será o tamanho global da mensagem (correspondente à concatenação de C1, C4 e C5)? Justifique.

e) Dados os componentes do processamento criptográfico, que componentes seriam dispensáveis de modo a diminuir o tamanho da mensagem total a transmitir, garantindo, no entanto, as mesmas propriedades de segurança da especificação indicada? Justifique.

f) O IV está a ser passado em claro. Isso constitui uma fraqueza que coloca em perigo a proteção de confidencialidade? Argumente.

Questão 3

Considere o sistema e protocolo Kerberos (considerando as versões 4 ou 5).

a) O protocolo Kerberos assegura propriedades de segurança futura e passada perfeitas? Justifique.

b) Nas mensagens das diferentes rondas do protocolo Kerberos, são usadas *timestamps* e *nonces*. Que vantagem de segurança vê na utilização dos *nonces* uma vez que já se faz a utilização de *timestamps* - o que também permitiria controlar a frescura das mensagens no controlo *anti-replaying*? Argumente.

PARTE II - PARTE COM CONSULTA

Questão 4

a) Se usar chaves RSA de 4049 bits, qual o tamanho máximo dos dados (ou mensagens) que podiam ser cifradas em RSA com reforço de *padding* com padrão OAEP ? Justifique.

b) Se usar chaves RSA de 4049 bits, qual o tamanho máximo dos dados (ou mensagens) que podiam ser assinadas em RSA com reforço de *padding* com padrão PSS ? Justifique.

c) "Assinou-se duas vezes uma mesma mensagem M usando o algoritmo ECDSA. Das duas vezes utilizou-se sempre a mesma chave privada e sempre a mesma construção ECDSA (com a mesma curva elíptica). Mesmo assim, o conteúdo da assinatura será diferente e até poderá ter tamanho diferente". Verdadeiro ou Falso?

d) Temos um par de chaves RSA com 2048 bits. Vamos usar a chave privada para produzirmos uma assinatura RSA normalizada que usará PSS como esquema de *padding* e uma função de síntese de segurança SHA-512. Se assinarmos uma mensagem M, independentemente do tamanho de M, qual será o tamanho em bytes da assinatura digital? Justifique.

Questão 5. A utilização parametrizável de diferentes modos de operação com algoritmos de cifra simétrica de blocos permite garantir confidencialidade de mensagens trocadas entre um emissor e um recetor. Dependendo do modo usado, podem ter-se propriedades diferentes:

P1: permitir que o tamanho das mensagens cifradas (*ciphertext*) seja igual ao das mensagens originais (*plaintext*), evitando a utilização de *padding*, mesmo quando as mensagens originais (*plaintext*), não tenham tamanho igual ou múltiplo do tamanho de bloco base do processamento do algoritmo simétrico usado P1: maior reforço de confidencialidade da mensagem enviada, independente do seu conteúdo;
P2: possibilidade de melhorar ainda mais a eficiência da cifra, explorando possibilidade de pré-processamento
P3: maior tolerância a perda de blocos completos cifrados que sejam enviados;
P4: maior tolerância a perda de bits em blocos cifrados enviados;
P5: vantagem em incluir prova implícita de autenticidade e integridade das mensagens enviadas;
P6 possibilidade de se fazerem cifras orientadas a bytes (*byte-based encryption*).
P7: possibilidade de evitar o uso de vetores de inicialização.
P8: maior eficiência das operações de cifra e decifra com possibilidade de paralelização das operações de cifra ou decifra
P9: simplificação do emissor e recetor por não terem necessidade da função para decifrar, podendo usar-se a implementação da função de cifra, para conseguir recuperar mensagens *plaintext* a partir das mensagens cifradas
P10: possibilidade de decifrar qualquer bloco cifrado numa mensagem cifrada, com acesso aleatório a esse bloco cifrado na ordem dos blocos recebidos

Coloque ***V*** nas células da seguinte tabela em que cada propriedade Pi se verifica ou é vantajosa. Note que pode haver mais do que ***V*** em cada linha, mas um ***V*** mal colocado descontará a valorização de um V numa posição correta.

Propriedade	Modos de operação de cifras simétricas						
	ECB *Electronic Code Book*	CBC *Cipher-Block Chain*	CTR *Counter Mode*	Cipher *Feedback Mode*	Cipher *Output Feedback*	GCM *Galois Counter*	CTS *Cipher Stealing*
P1							
P2							
P3							
P4							
P5							
P6							
P7							
P8							
P9							
P10							

Questão 6.

Esta questão só deve ser respondida por alunos que estão a realizar avaliação prática no presente ano letivo de 2020/2021.

Considere o trabalho prático nº 1 e o seu domínio e conhecimento do contexto e componentes do trabalho.

Responda às seguintes alíneas, independentemente de ter ou não realizado a FASE 2. Note que as respostas às alíneas relacionadas com a fase 2 não obrigam necessariamente que tenha feito a implementação, apenas o entendimento da análise da especificação do protocolo.

a) No protocolo SSP (FASE 1, poder-se-ia utilizar uma configuração como indicada a seguir?

```
CRYPTO-CIPHERSUITE:DESede/CTR/NoPadding
MAC1-CIPHERSUITE:HMAC-SHA2-256
MAC2-CIPHERSUITE:NULL
IV:0x07,0x06,0x05,0x04,0x03,0x02,0x01,0x00
SESSION-KEYSIZE:168
SESSION-
KEY:0x01,0x23,0x45,0x67,0x89,(byte)0xab,(byte)0xcd,(byte)0xef,0x01,0x23,0x45,0x67,0x89,
(byte)0xab,(byte)0xcd,(byte)0xef,0x01,0x23,0x45,0x67,0x89
MAC1-KEYSIZE:NULL
MAC1-KEY:NULL
MAC2-KEYSIZE:16
MAC2-
KEY:0x80,0x70,0x60,0x50,0x40,0x30,0x20,0x10,0x99,0x98,0x97,0x96,0x95,0x94,0x93,0x92
```

b) No formato da mensagem do protocolo SSP, existe proteção de segurança futura e passada perfeitas? Justifique.

c) Podemos dizer que o protocolo da FASE 2 protege a confidencialidade do tráfego (TRAFFIC-FLOW CONFIDENTIALITY), tal como esta propriedade de segurança é definida na Framework OSI X.800? Justifique.

d) Na interpretação que faz do protocolo SHP (FASE 2), considera que existe proteção do tipo *Peer-Authentication*? Justifique.

e) O que garante em concreto segurança futura e passada perfeitas no protocolo SHP (FASE 2)?