Instituto Superior de Engenharia de Lisboa
Área Departamental de Engenharia da Eletrónica e Telecomunicações e de Computadores
MEIC/MEET/MERCM/LEIM - Segurança em Redes de Computadores (SRC) - 2017/07/20

Exame de 2ª época

Nome:_____; Número_____

Docente: Vítor Almeida Curso: LEIM ☐ MEIC ☐ MEET ☐ MERCM ☐

Nas questões de resposta múltipla assinale com um V (verdadeira), um F (falsa) ou não ponha nada (neste caso nem conta nem desconta na cotação).

V F

1) **Como funciona o One Time Pad (OTP) e porque é que não é mais utilizado?** É um *xor* entre o texto em claro que se pretende cifrar e uma sequência aleatória com a mesma dimensão do texto em claro a cifrar. Devido ao facto de ser necessário gerar uma sequência aleatória da mesma dimensão do texto em claro a cifrar e ser necessário enviar essa sequência aleatória para o destino onde vai ser decifrado o texto cifrado esta forma de cifrar não é muito prática.
2) **Um ataque de *phising*, por vezes também referido como *phishing*, é um ataque à segurança:**

☐☐ Passivo
☐☐ Ativo #
☐☐ Por interceção
☐☐ Por interrupção
☐☐ Por modificação
☐☐ Por fabricação #

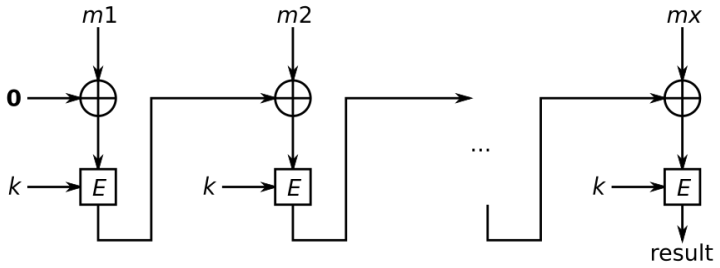
3) **O princípio de Kerckhoffs sobre "segurança através da obscuridade" é utilizado atualmente nos sistemas criptográficos?**
   Sim, hoje em dia segue-se cada vez mais o princípio de Kerckhoffs divulgando os algoritmos mantendo secretas as chaves usadas. A força de uma cifra deve estar no algoritmo usado, o qual pode e deve ser público, e nas chaves usadas as quais se devem manter secretas e não no secretismo do algoritmo usado.
4) **Qual o requisito para que a cifra de Vernam pudesse ser considerada *one-time pad*?**
   Chave aleatória usada uma única vez
5) **Tendo em consideração as cifras clássicas indique quais das seguintes afirmações estão corretas:**

☐☐Numa cifra de substituição mona alfabética a modificação aplicada aos diferentes símbolos do bloco é sempre a mesma #
☐☐Numa cifra de polialfabética a permutação difere de símbolo para símbolo dentro do mesmo bloco #
☐☐A cifra de Vigenère não mantém a frequência dos caracteres e por isso é uma cifra de substituição monoalfabética
☐☐A difusão através de transposição é um método usado para dissipar a estrutura estatística do texto em claro no texto cifrado #

6) **Indique duas vantagens do uso do MAC em relação ao uso de uma função *hash*?**

Um MAC é um *hash* protegido com uma chave.
1) O MAC fornece autenticação, desde que a chave de autenticação seja conhecida apenas por emissor e recetor.
2) Maior proteção nos ataques de força bruta mais difíceis, já que eles não podem necessariamente ser pré calculados.

7) **O modo CBC-MAC é uma forma de garantir confidencialidade, autenticação e/ou integridade de mensagens? A dimensão do resultado depende da dimensão do texto em claro?**



Fornece autenticação entre pares (os quais conhecem a chave k). Para calcular CBC-MAC de uma mensagem m, divide-se a mensagem m em x blocos e para cada bloco faz o xor deste com um vetor de inicialização, o primeiro é zero. O resultado de cada xor é cifrado com uma chave secreta k numa cifra de bloco E, dando origem ao próximo vetor de inicialização. O resultado tem sempre a mesma dimensão fixa e depende apenas da cifra usada.

8) Tendo em consideração os algoritmos de *hash* indique quais das seguintes afirmações estão corretas:

☐☐ Uma das características de uma função *hash* segura é produzir uma saída com comprimento fixo #

☐☐O resultado da aplicação de uma função *hash* é facilmente invertido se a chave usada estiver disponível

☐☐ Uma função de *hash* h=H(m), por exemplo SHA1, aplicada a um texto em claro m1 gera um *hash* com 160 bits. A mesma função de *hash* aplicada a um texto m2 com o dobro da dimensão de m1 gera uma *hash* de 320 bits

☐☐Uma das razões de usar um protocolo de autenticação de mensagens derivado de uma função de *hash* criptográfico em oposição a um derivado de uma cifra simétrica, deve-se ao fato das funções *hash* criptográficas, como MD5 e SHA, serem geralmente mais rápidas em software do que cifras de cifra simétricas, como DES

9) O *Diffie-Hellman*:

☐☐ Permite gerar uma chave simétrica #

☐☐ Permite gerar a chave privada para um certificado digital

☐☐ Utiliza certificados digitais para passar o valor dos parâmetros necessários à sua geração

☐☐ Usa IPSec quando se pretende fazer passar uma chave de modo criptograficamente seguro

10) Responda às seguintes questões assumindo o algoritmo de criptografia assimétrica. Considere que se escolhe como nº primos 29 e 17 e que se usa a tabela anterior de conversão de letras para números (Nota: O *padding* usado no RSA evitaria algumas fragilidades no uso da tabela acima mas neste exercício ignore-se).

a) Determine o totiente de n.

$$\Phi(n) = (p-1)(q-1) = 28 \times 16 = 448$$

b) Verifique se o valor 3 é primo relativo de Φ(n).

n=pq=29x17=493

Φ(n) = (p-1)(q-1) = 28 x 16 = 448

'3' é primo relativo do totiente, isto é gcd(448,3)=1, 448 é divisível por 1,2,4,7,8,…. O único divisor entre primos relativos deve ser o 1, o que é verdade neste caso pois 3 é divisível por 1 e 3 apenas.

c) Determine qual a informação a publicar para que terceiros possam enviar mensagens cifradas usando este algoritmo. Assuma e=3.

Corresponde ao n=pxq=17x29=493 e ao e=3; (e=3, n=493)

d) Verifique se a chave privada pode ser d=299.

Ou seja $d = e^{-1} \bmod \Phi(n)$

299 e 448 são primos relativos se 299xe=1 mod (448) ou seja 299x3=897=1 mod (448) pois 448x2=896

e) Qual a informação a publicar para que um destinatário possa verificar a autenticidade de um texto que receba autenticado usando um *hash* bem definido e a cifra assimétrica do exemplo?

e=3 e n=493, o destinatário necessita conhecer a chave pública do emissor e o valor n resultante da multiplicação dos dois números primos p e q.

11) Considere que Alice pretende enviar uma foto pelo Facebook, de forma a que seja vista apenas por um grupo de amigos (N) e não por todos. Tanto a Alice como cada um dos seus amigos possuem chaves privadas e públicas. Indique quais as respostas que são verdadeiras:

☐☐ Alice deve cifrar uma cópia com a sua chave pública

☐☐ Alice deve cifrar uma cópia com a sua chave privada

☐☐ Alice deve cifrar N cópias com a chave pública de cada um dos seus amigos #
☐☐ Alice deve cifrar N cópias com a chave privada de cada um dos seus amigos

12) Considere o uso do HMAC-SHA1 com a chave K:

☐☐ A chave K serve para cifrar o resultado do *hash*
☐☐ O HMAC-SHA1 permite a verificação de integridade e autenticação #
☐☐ O HMAC-SHA1 é tão seguro como calcular o SHA-1 (chave | mensagem)
☐☐ O tamanho da saída do HMAC não depende do tamanho da chave K usada #
☐☐ Se possuir a chave é possível obter o texto em claro a partir do valor do HMAC

13) Tendo em consideração os certificados digitais indique quais das seguintes afirmações estão corretas:

☐☐No certificado está disponível a chave pública do dono do certificado #
☐☐Um certificado público x.509 é assinado com a chave pública do utilizador
☐☐Um certificado público x.509 é assinado com a chave privada da autoridade de certificação #
☐☐Uma assinatura realizada antes da revogação de um certificado mantém-se válida para testar a autenticação após a revogação do mesmo #, para verificação apenas; não serve para assinar
☐☐Um certificado digital de chave pública serve para atestar a chave pública do utilizador cujo certificado é assinado com a chave privada do emissor #

14) IEEE 802.1x:

☐☐ As mensagens IEEE802.1x "correm" sobre IP
☐☐ Utiliza como protocolo de autenticação o EAP
☐☐ As mensagens EAP enviadas pelo servidor de autenticação terminam no Suplicante #
☐☐ As mensagens EAP enviadas pelo servidor de autenticação terminam no Autenticador
☐☐ Todos os pacotes IP que chegam a uma porta de um *switch* que use IEEE802.1x têm de estar devidamente autenticados para que a porta os deixe passar

15) RADIUS:

☐☐ A *user-password* P é cifrada através de P XOR MD5(Request Authenticator)
☐☐ As mensagens access-request são autenticadas através do campo Request-Authenticator
☐☐ O Request-Authenticator deve ser temporalmente e globalmente único (sem haver repetições)
☐☐ As mensagens access-accept e access-reject enviadas pelo servidor de autenticação vão autenticadas
☐☐ É possível lançar um ataque ao segredo partilhado S se o atacante conseguir efetuar uma tentativa de autenticação com uma *user-password* conhecida #

16) Tendo em consideração as seguintes afirmações indique quais é que estão corretas:

☐☐ O 802.1x permite utilizar vários protocolos de cifra
☐☐ No protocolo PPTP, o canal de dados do PPP corresponde a um canal GRE sobre IP #
☐☐ Quando se utiliza PPP e se pretende autenticação, se usar CHAP não pode usar EAP #
☐☐Quando se utiliza o PPP uma máquina recebe o seu endereço IP através de NCP-IPCP #
☐☐ No 802.1x o suplicante e o servidor de autenticação têm de ter conhecimento da chave secreta do utilizador #

17) Quais as principais fragilidades do PPTP?

☐☐ Utilização de MD4 #
☐☐ Mensagens não autenticadas #
☐☐ Só suporta IP como protocolo acima
☐☐ Utilização do canal de controlo da ligação sobre TCP sem segurança #

18) Para que a criação de um novo SA IKEv2 com PFS (*Perfect Foward Secrecy*) devem obrigatoriamente ser trocados:

☐☐ Novos *nonces*
☐☐ Novos certificados
☐☐ Novas chaves privadas
☐☐ Novas chaves de sessão
☐☐ Novos valores para o Diffie-Hellman #

19) Pretende criar uma VPN que permita evitar a análise de tráfego utilizando IPSec escolheria:

☐☐ ESP com cifra
☐☐ Modo Túnel #
☐☐ Modo Transporte
☐☐ Números de sequência aleatórios
☐☐ Security Parameters Index cifrados
☐☐ ESP com autenticação em detrimento do AH

20) Quando chega um datagrama IPsec, usando o protocolo ESP, como é que o destino sabe se é ESP com confidencialidade, com autenticação ou com autenticação e confidencialidade:

☐☐ Pelo SA negociado #
☐☐ Pelo campo protocolo do cabeçalho ESP
☐☐ Pelo valor campo protocolo do cabeçalho IP
☐☐ Pela existência, ou não, do campo "authentication data" na mensagem ESP

21) A pesquisa na base de dados das SA (SAD) quando chega um datagrama IPsec utiliza:

☐☐ O SA negociado
☐☐ O *sequence number*
☐☐ O *security parameter index* #
☐☐ O valor do *socket* do datagrama (IP origem, porto origem, IP destino, porto destino, protocolo)

22) Para fornecer integridade o WEP utiliza:

☐☐ Um CRC protegido pelo RC4 #
☐☐ RC4 sobre o campo de dados da trama
☐☐ O WEP não dá nenhuma garantia de integridade
☐☐ HMAC-MD5 da concatenação da trama com a chave partilhada

23) Qual dos protocolos que compõem o SSL/TLS fornece o mecanismo de garantia de integridade?

☐☐ Alert Protocol
☐☐ SSL Record Protocol #
☐☐ SSL Handshake Protocol,
☐☐ Change Cipher Spec. Protocol,

24) Em SSL/TLS como são decididos quais os algoritmos criptográficos a usar numa ligação?

O servidor escolhe do conjunto de *suites* criptográficas que o cliente indica aquela que pretende usar.

25) Como é que um destinatário de um *email* no formato S/MIME tem acesso à chave de sessão, assumindo que o conteúdo vem cifrado?

☐☐ É enviada em claro no corpo do *email*
☐☐ É obtida a partir dos certificados ISO/ITU-T X.509v3
☐☐ Vem cifrado no corpo do *email* com a chave privada do recetor
☐☐ Vem cifrado no corpo do *email* com a chave pública do recetor #
☐☐ Vem cifrado no corpo do *email* com a chave privada do emissor

26) Se utilizar SPF (*Sender Policy Framework*) o servidor de *email*:

☐☐ É garantida a confidencialidade das mensagens entre servidores de *email*
☐☐ Obriga os clientes a utilizar SMIME para garantir a autenticação das mensagens
☐☐ Verifica no DNS qual a chave pública do servidor remetente e verifica a assinatura das mensagens recebidas
☐☐ Consulta o DNS para verificar se o servidor que lhe está a enviar a mensagem de *email* está autorizado a fazê-lo em nome do domínio do remetente #.