Vitor Caetano da Silva Nº 9276999

Prova 2: Segurança da Informação

1. Um MAC é produzido com base no texto sem formatação e o texto sem formatação é criptografado sem o MAC. O MAC do texto simples e o texto cifrado são enviados juntos.

   O "encrypt-then-mac" criptografa a mensagem utilizando o sistema $\Pi_E = \langle Gen_E, E', D' \rangle$ em seguida gera um código de autenticação (MAC) utilizando o sistema $\Pi_M = \langle Gen_M, Mac, Ver \rangle$ gerando o sistema:

   $Gen(1^n) := k = \langle k_E, k_M \rangle$ tal que $Gen_E(1^n) := k_E$ e $Gen_M(1^n) := k_M$

   $E(k, m) := \langle c, t \rangle$ tal que $E'(k_E, m) = c$ e $Mac(k_M, c) = t$

   $D(k, c) := D'(k_E, c)$ se $Ver(k_M, c, t) = 1$ e $\perp$ caso contrário

   Caso Π_E seja seguro contra ataques "chosen plaintext"

   Caso Π_M seja seguro contra falsificação, esse sistema é seguro contra ataques "chosen ciphertext". O modo "encrypt-then-mac" não garante isso.

   O sistema MAC-then-encrypt não fornece nenhuma integridade no texto cifrado, pois não temos como saber, até descriptografarmos a mensagem, se ela é realmente autêntica ou falsificada.

   Mesmo que a abordagem "encrypt-then-mac" não tenha provado ser fortemente não falsificável em si, é possível algumas modificações no SSH para torná-lo fortemente não falsificável.
   Se o esquema cifrado for maleável, não precisamos nos preocupar, pois o MAC filtrará esse texto cifrado inválido.

   O MAC não fornece nenhuma informação sobre o texto simples, pois, assumindo que a saída da cifra parece aleatória, o mesmo acontece com o MAC.

2.

A Função Hash um algoritmo matemático para a criptografia, na qual ocorre uma transformação do dado (como um arquivo, senha ou informações) em um conjunto alfanumérico com comprimento fixo de caracteres.

A criptografia hash é utilizada para resumir dados, verificar integridade de arquivos e garantir a segurança de senhas, dos arquivos e das informações armazenadas dentro de um servidor.

Um hash H resistente contra colisão garante que qualquer adversário polinomial consegue gerar um par que gere H(x) = H(x') apenas com probabilidade desprezível. A resistência contra colisão também garante que o hash seja resistente contra pré-imagem.

Uma vez que o hash é resistente a uma pré-imagem, o melhor que se pode fazer para encontrar um elemento x tal que H(x) = y é um ataque força-bruta, chutando valores x até que encontre um x tal que H(x) = y .

3.

fecho: para qualquer $a, b \in \mathbb{Z}_n$ temos que $0 \leq a + b \ (mod \ n) \leq n$, portanto $a + b \ (mod \ n) \in \mathbb{Z}_n$

associatividade: a soma módulo n satisfaz associatividade

$\forall$ a,b,c Є $\mathbb{Z}_n$ temos que (a+b)+c $\equiv$ a + (b+c) (mod n)

elemento neutro: o zero é elemento neutro. a+0 $\equiv$ 0 +a $\equiv$ a (mod n)

para todo a Є $\mathbb{Z}_n$ temos que a +(n-a) $\equiv$ 0 (mod n), como n-a Є $\mathbb{Z}_n$ temos que (n-a) é o inverso de a.

A troca de chaves de Diffie-Hellman é um método de criptografia para trocas de chaves de maneira segura em canais públicos.

O método da troca de chaves de Diffie-Hellman permite que duas partes que não possuem conhecimento prévio uma da outra, compartilhem uma chave secreta sob um canal de comunicação inseguro. Tal chave pode ser usada para encriptar mensagens posteriores usando um esquema de cifra de chave simétrica.

O método Diffie-Hellman não é adequado para este grupo cíclico (como 1 gera todos os elementos do grupo), pois o problema do Logaritmo Discreto é um problema fácil.
Esse caso seria um gerador somado x vezes = g.x(mod n), mas como g é conhecido, bastaria dividir por g para recuperar x.

4.

O Certificado Digital garante não apenas a integridade, mas também a autenticidade e a confidencialidade às informações eletrônicas. Basicamente, é usado para identificar pessoas e empresas no mundo virtual, permitindo que documentos sejam assinados com validade jurídica.

O certificado digital garante e identifica o dono de uma chave pública. Ele é assinado digitalmente por uma autoridade certificadora. O Certificado Digital também pode ser usado para a autenticação em sistemas e sites, assinar documentos, retificar a declaração do imposto de renda, entre outras funcionalidades, o processo é feito de forma segura, confiável, prática e com custo reduzido, a tecnologia viabiliza a realização de operações virtuais que evitam a necessidade de deslocamento e burocracia.

O modelo rede de confiança qualquer um pode emitir certificados, cabendo ao usuário decidir e estabelecer confiança entre essas entidades certificadoras. O chamado ZERO TRUST SECURITY (Modelo de Segurança Confiança Zero), é um modelo de rede de confiança que cria um rigoroso processo de verificação de usuários e dispositivos conectados à rede uma política estrita de autenticação de usuários e dispositivos conectados em toda a rede, fornecendo a “chave” apenas para indivíduos e/ou dispositivos aprovados.