**Tarefa 7M   
Funções criptográficas de Hash, HMAC  
Assinaturas Digitais.   
Certificados.**

**Questões:**

1. Para que serve, em segurança, o uso das funções hash ?
2. Vamos supor que uma mensagem M chegue a você e que um hash da mensagem H(M) (resumo da mensagem ou impressão digital) chegue **separadamente**. Como podemos fazer para verificar se a mensagem foi modificada ?
3. Existem alguns algoritmos disponíveis, mais usados, para hash de mensagens: MD5 (128 bits, considerado ótimo) e o SHA-1(160 bits, considerado excelente). Normalmente, os sites que fornecem arquivos longos para serem transferidos, mencionam estes algoritmos e fornecem os cálculos dos hash para esses arquivos. Que outros algoritmos padronizados hash SHA existem para expandir o resultado da função ?

1. Suponha o algoritmo de hash SHA-1 que gera um único resumo de 20 bytes. Diante da resposta da questão 2, pode-se afirmar que a verificação de integridade da mensagem é seguro ?
2. Java possui o pacote Java.security.\*. E assim, podemos obter uma impressão digital a partir de uma mensagem. A classe **MessageDigest** é, de fato, uma classe abstrata, mas podemos continuar obtendo uma instância dela, usando o método **getInstance()**. Neste método, incluímos uma string, indicando o algoritmo que gostaríamos de usar. Quando o nosso programa já tiver uma instância de MessageDigest, ele poderá começar a leitura de nossa mensagem, um byte por vez, ou como um array de bytes. Quando todos os bytes da mensagem tiverem sido lidos , o método digest() poderá ser chamado para invocar o algoritmo de hash e retornar uma impressão digital (resumo de mensagem). Veja o programa Java:

import Java.security.\*;  
public class Fingerprint {  
 public static void main(String [] args){  
 MessageDigest md = null;  
 String message = “”;  
 for (int i=0; i<args.length;i++)  
 message = message + “ “ + args[i];  
 try {  
 md = MessageDigest.getInstance(“SHA-1”);

} catch (NoSuchAlgoritmException ae) {}

md.update( message.getBytes());  
 byte [] fingerprint = md.digest();

System.out.print(“Fingerprint: “);  
 for(int j=0; j<fingerprint.length; j++)  
 System.out.print( (fingerprint[j] + 128) + “ “);  
 }  
}

Execute este programa, entrando com uma mensagem M, usando argumentos de linha de comando. Anote seu hash. Entre com a sua mensagem M’, ligeiramente alterada em M. O que você observa, comparando os valores hash calculados ?

1. Uma deficiência para este método de verificação está relacionada à impressão digital H(M), que é enviada **separadamente** da mensagem M. Os algoritmos SHA-1, MD 5 ou outros (SHA-256, SHA-384, SHA-512) estão disponíveis publicamente e, portanto, se alguém interceptar a mensagem M e o H(M), poderá modificar a mensagem M para M’, gerar um nova impressão digital H(M’) e enviar ambas para você. Você não poderá supor que a mensagem M tenha sido alterada.
2. Qual a causa do problema de segurança existente ?
3. O que você pode fazer para resolver o problema de segurança ?

**Assinaturas Digitais**

(Verdade / Falso) Também importante para a confidencialidade como medida de segurança é a autenticação.

(Verdade/Falso) No mínimo, a autenticação, garante que uma mensagem provém da origem alegada. Autenticação pode prover proteção contra modificação, atraso, repetição e reordenação.

(Verdade/Falso) Criptografia de chave pública contribui no sentido de resolver o problema da distribuição de chaves simétricas na geração de assinaturas.

(Verdade / Falso) Funções criptográficas de hash são usadas para assinaturas digitais, ao invés de se usar a chave privada em toda a mensagem.

Por que não é uma boa idéia assinar o texto legível inteiro, para gerar assinaturas digitais ?

Como integridade pode ser verificada através de assinaturas digitais ?

Para que serve, em segurança, o uso de resumos de mensagens ?

Um mal intencionado lê e altera parte da informação transitando numa linha de comunicação antes desta chegar ao destino. O destinatário gostaria de detectar se alguma alteração parcial foi feita na informação. Que **requisito de segurança** deve ser verificado para garantir que nenhuma anomalia de alteração de mensagem ocorreu ?

Um falso remetente envia informação para um destinatário. Este deseja ter certeza de que foi um remetente verdadeiro que enviou a informação. Que **requisito de segurança** precisa ser garantido para que o destinatário tenha plena certeza de quem partiu a informação ?

**Certificados (Ver página da disciplina)**  
Cite as partes fundamentais de um certificado digital.  
Para que serve o uso de certificados digitais  
  
Existem certificados para algumas finalidades importantes. Que tipos de certificados, são mais comuns e importantes no contexto da certificação digital ?

HMAC







 