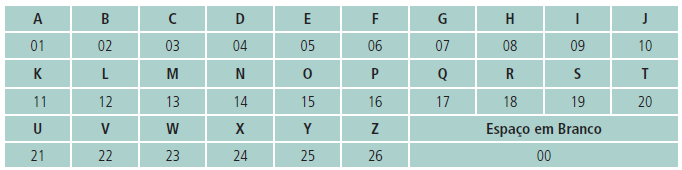
Exercício

Para as três primeiras questões, vamos tentar pôr em prática o método de criptografia proposto por Marçula e Benini Filho. Para a solução dos problemas propostos, você deverá utilizar a tabela a seguir para codificar e decodificar as mensagens.



1) De férias nos Emirados Árabes, a conselheira Trace recebe uma caixa de seu chocolate Cretariano favorito, juntamente com uma mensagem criptografada do remetente revelando sua identidade. Usando o exemplo de

criptografia citado por Marçula & Benini Filho, decodifique a mensagem MPHKCESEVGUGSRKVVECB, cuja chave é: 00 07 05 03 02. Decodifique para saber o nome do remetente.

**2.** Em seu primeiro contato com um planeta Zomour com que a Retamatemil deseja estabelecer relações diplomáticas, os oficiais da UCorporation foram convidados para um banquete. Infelizmente, há um grupo dissidente no plano Zomour que deseja apoiar os Crodapon e não a Retamatemil. Um espião desta facção é instruído a envenenar um dos oficiais da UCorporation. O traidor é descoberto, mas foge a tempo. Em seu alojamento é encontrada a mensagem codificada KWUXWVVCKN que contém o nome do oficial envenenado

e um pedaço de papel com o números 0822031114 usados na codificação. Como o veneno é seu próprio antídoto é preciso saber exatamente quem foi envenenado. Trabalhando contra o tempo, um especialista em segurança verificou que se tratava de um código muito simples, o código proposto por Marçula & Benini Filho. Qual o nome do Oficial envenenado?

**3.** Você faz parte de uma equipe de segurança de seu país, o Janbolala, e precisa enviar a mensagem ao seu espião secreto que se encontra no país vizinho, o Kongololo. Mas, para isso, a mensagem precisa ser codificada.

Usando o método de Marçula e Benini Filho, codifique a mensagem: Abortar operação. A Chave a ser utilizada para codificar é: 00 07 05 03 01

**4.** Explique como funciona a assinatura digital.

Para assinar digitalmente um documento, é necessário que o documento primeiramente esteja já digitalizado e esteja de posse da chave pública de quem vai receber o documento, podendo ser pessoa física ou jurídica.

Em seguida, a partir de um programa específico, o documento será criptografado de acordo com a chave pública que você tem para poder enviar o documento, gerando um resumo do mesmo tamanho que será criptografado,

denominado hash, garantindo autenticidade e o não repúdio.

Quando a mensagem chegar ao destinatário, o receptor deverá utilizar sua chave privada para decodificar/decriptografar o documento, gerando um novo resumo a partir da mensagem que está armazenada, para em seguida, comparar com a assinatura digital.

Caso o documento tenha sido alterado, a chave privada não vai conseguir decodificar o arquivo, pois consequentemente a assinatura é corrompida, não reconhecendo o documento. Ou seja, se o hash original for igual ao hash gerado na recepção do documento, a mensagem está íntegra.

A função hashing avalia completamente o documento baseado num algoritmo matemático que calcula um valor, tendo como parâmetro os caracteres do documento, obtendo um valor de tamanho fixo para o arquivo, conhecido

como valor hash.

**5.** O que é hash?

A função hashing avalia completamente o documento baseado num algoritmo matemático que calcula um valor, tendo como parâmetro os caracteres do documento, obtendo um valor de tamanho fixo para o arquivo, conhecido

como valor hash.

**6.** De que é composto o certificado digital?

Essa tecnologia é composta por um conjunto de informações referentes à entidade para a qual o certificado foi emitido, baseando-se na criptografia de chave pública, garantindo assim outros aspectos da segurança da informação como: autenticação e o não repúdio.

**7.** Explique o funcionamento do certificado digital.

Na identificação digital, é utilizada a técnica de criptografia assimétrica que dispõe de duas chaves relacionadas, uma chave pública e outra privada.

Tanto um nome de usuário como outras informações que identificam o usuário são vinculadas a um par de chaves, e isso funciona como um credenciamento eletrônico que, quando instalado em um navegador da Web, permitem a autenticação.

Em uma única mensagem, podemos anexar várias identificações digitais, formando “uma cadeia de certificados digitais em que cada identificação digital confirma a autenticidade da anterior e essa identificação digital é

assinada pela Autoridade Certificadora que a emitiu” (SERPRO).

**8.** Cite os modelos de certificado digital.

**Modelo Web Oftrust (malha de confiança)**

**Modelo Hierárquico**

**Modelo de Autoridade Central**