SEGURANÇA DA INFORMAÇÃO

INFORMAÇÃO é um recurso (ativo) que, como outros importantes recursos de negócios, tem valor para uma organização e, por conseguinte precisa ser protegido adequadamente.

SEGURANÇA DA INFORMAÇÃO - protege a informação de uma gama extensiva de AMEAÇAS para assegurar a **continuidade** dos negócios, **minimizar** os danos empresariais e **maximizar** o retorno em investimentos e oportunidades. A Segurança da Informação é caracterizada pela preservação da confidencialidade, integridade e disponibilidade.

PRINCÍPIOS BÁSICOS DA SEGURANÇA DA INFORMAÇÃO

- CONFIDENCIALIDADE (privacidade) - assegurar que a informação só será acessada pelas pessoas que têm autorização (garantida pela **CRIPTOGRAFIA**).
- INTEGRIDADE - assegurar que a informação não foi alterada durante o processo de armazenamento ou de transporte do emissor para o receptor (garantida pelo **HASH**).
- DISPONIBILIDADE - assegurar que os usuários autorizados tenham acesso a informações e a recursos associados quando requeridos. Ou seja, assegurar que as informações estarão disponíveis quando solicitadas pelos usuários autorizados (garantida pelo **QoS** - Quality of Service-Qualidade de Serviço).

CRIPTOGRAFIA - é um conjunto de técnicas que possibilita tornar incompreensível uma mensagem originalmente escrita com clareza, de forma a permitir que apenas o destinatário a decifre e compreenda.

ESSA ATIVIDADE SUPERVISIONADA ABORDA O TEMA CRIPTOGRAFIA UTILIZANDO TÉCNICAS DE ÁLGEBRA LINEAR!

Só é possível gerir, o que se pode medir !

APLICAÇÃO DE ÁLGEBRA LINEAR A CRIPTOGRAFIA

Para **criptografar** uma palavra de **6 letras** e enviar uma mensagem confidencial deve-se proceder da seguinte forma:

a) **Escolher** a palavra que deseja enviar como uma mensagem, por exemplo: **BRASIL**.

b) **Colocar** as letras como elementos de uma matriz 3 x 2 na ordem ilustrada abaixo.

$$M = \begin{bmatrix} B & S \\ R & I \\ A & L \end{bmatrix}_{3x2}$$

c) **Substituir** cada letra pelo número da tabela de conversão abaixo, na qual o símbolo (*) representa um espaço em branco.

A=1	H=8	O=15	V=22
B=2	I=9	P=16	W=23
C=3	J=10	Q=17	X=24
D=4	K=11	R=18	Y=25
E=5	L=12	S=19	Z=26
F=6	M=13	T=20	*=0
G=7	N=14	U=21	

A mensagem ficará armazenada na matriz M como abaixo:

$$M = \begin{bmatrix} B & S \\ R & I \\ A & L \end{bmatrix}_{3x2} = \begin{bmatrix} 2 & 19 \\ 18 & 9 \\ 1 & 12 \end{bmatrix}_{3x2}$$

TABELA DE CONVERSÃO CHAR/NUMÉRICO DO ALGORITMO

d) **Codificar** a mensagem ⇒ ALGORITMO DE CRIPTOGRAFIA

MULTIPLICAR a matriz **M** pela **MATRIZ DE CRIPTOGRAFIA C_{3x3}** dada abaixo:

$$C = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 2 & -1 \end{bmatrix}_{3x3}$$ **MATRIZ DE CRIPTOGRAFIA** ⇒ 3x3

A MENSAGEM CRIPTOGRAFADA (MC) SERÁ ⇒ MC = C x M

$$MC = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 2 & -1 \end{bmatrix}_{3x3} \times \begin{bmatrix} 2 & 19 \\ 18 & 9 \\ 1 & 12 \end{bmatrix}_{3x2} \qquad MC = \begin{bmatrix} 3 & 31 \\ 21 & 40 \\ 35 & 6 \end{bmatrix}_{3x2}$$

$$C \quad \times \quad M$$

Suponha agora que a mensagem criptografada **MC** recebida foi a matriz abaixo.

$$MC = \begin{bmatrix} 27 & 20 \\ 28 & 41 \\ -12 & 23 \end{bmatrix}_{3x2}$$

PERGUNTA: Qual a mensagem original enviada (palavra)?

ATIVIDADE SUPERVISIONADA

Desenvolver um ALGORITMO em DOIS MÓDULOS descritos a seguir:

MÓDULO-01 - CRIPTOGRAFIA

OBJETIVO - ler uma mensagem de **6 caracteres** (**M**) e gerar a matriz com a mensagem criptografada (**MC**) correspondente.

ETAPAS

- LER uma palavra de 6 caracteres
- CODIFICAR e armazenar a palavra lida em uma matriz **M** (3x2) numérica usando a **TABELA DE CONVERSÃO** da página anterior.
- MULTIPLICAR **a MATRIZ DE CRIPTOGRAFIA - C (3x3)** pela matriz da mensagem **M (3x2) e** gerar **a MATRIZ COM A MENSAGEM CRIPTOGRAFADA** **MC (3x2)** $\Rightarrow$ $\mathbf{MC_{3x2} = C_{3x3} \times M_{3x2}}$
- **IMPRIMIR**
  - A palavra (mensagem) original lida
  - A matriz **M**(3x2) codificada de acordo com a **TABELA DE CONVERSÃO**
  - A matriz da mensagem criptografada **MC** (3x2)

MÓDULO-02 - DESCRIPTOGRAFIA

OBJETIVO - ler uma mensagem criptografada (**MC**) no MÓDULO-01, descriptografar e imprimir.

ETAPAS

- LER uma matriz de mensagem criptografada **MC** (3x2)
- MULTIPLICAR a matriz inversa de **C** ($\mathbf{C^{-1}}_{3x3}$) pela matriz criptografada $\mathbf{MC}_{3x2}$ e gerar a matriz da mensagem original $\mathbf{M}_{3x2} \Rightarrow \mathbf{M}_{3x2} = \mathbf{C^{-1}}_{3x3} \times \mathbf{MC_{3x2}}$
- GERAR mensagem original enviada (palavra) utilizando a matriz da mensagem $\mathbf{M_{3x2}}$ e a TABELA DE CONVERSÃO.
- IMPRIMIR
  - A matriz da mensagem criptografada $\mathbf{MC_{3x2}}$
  - A matriz M_{3x2} descriptografada com a inversa de **C** (C^{-1}).
  - A mensagem original enviada (palavra).

TECNOLOGIAS

Linguagens - C (Dev C++) ou PYTHON

C (DEV C++) - diretivas de compilação usadas em Introdução a Programação e Programação Estruturada.
ou
PYTHON
https://colab.research.google.com/

O QUE DEVE SER ENTREGUE

EM DEV C(++)
CÓDIGO FONTE E EXECUTÁVEL DE CADA MÓDULO (4 arquivos)

EM PYTHON – NOTEBOOK.YPNB (APS_ALG2.YPNB) (1 ou 2 arquivos…)

OBS - COLOCAR OS NOMES DOS COMPONENTES NO INÍCIO PROGRAMA QUE SERÁ DESENVOLVIDO.

COMPONENTES POR GRUPO - máximo 4

VALOR DA APS - 4,0 PONTOS NA AV2

DATA DA ENTREGA - 01 DE JUNHO (SÁBADO)

OBSERVAÇÕES

01- Para achar a inversa pode ser usado uma função de inversão de matriz (DEV C++) já pronta (liks abaixo) e o NumPy se usar PYTHON.

LINKS COM CÓDIGO DE INVERSA EM C

https://coisasdapaloma.blogspot.com/2013/01/achar-matriz-inversa-em-c.html

https://github.com/marymeendes/ALC/blob/master/inversa.c

…….

INVERSA EM PYTHON

NumPy….

02- Tanto a TABELA DE CONVERSÃO como a MATRIZ DE CRIPTOGRAFIA (C) são constantes.

PERGUNTA – VALE PONTO!

- Como podemos melhorar a segurança do ALGORITMO DE CRIPTOGRAFIA? Coloque a sugestão como comentário no programa.

A grandeza não consiste em receber honras, mas em merecê-las.

Aristóteles

(Estagira/Macedônia 384 a.C. - 322 a.C. Cálcis/Grécia)