IFSULDEMINAS, *campus* Muzambinho
**Curso de Ciência da Computação**


# Criptografia

**Prof. Ricardo José Martins**
**ricardo.martins@muz.ifsuldeminas.edu.br**

Curso de Bacharelado em Ciência da Computação
AED III – Algoritmo e Estruturas de Dados III

# Introdução

- ***Criptografia*** : é caracterizada como a ciência (ou arte) de escrever em códigos ou em cifras, ou seja, é um conjunto de métodos que permite tornar incompreensível uma mensagem (ou informação), de forma a permitir que apenas as pessoas autorizadas consigam decifrá-la e compreendê-la.

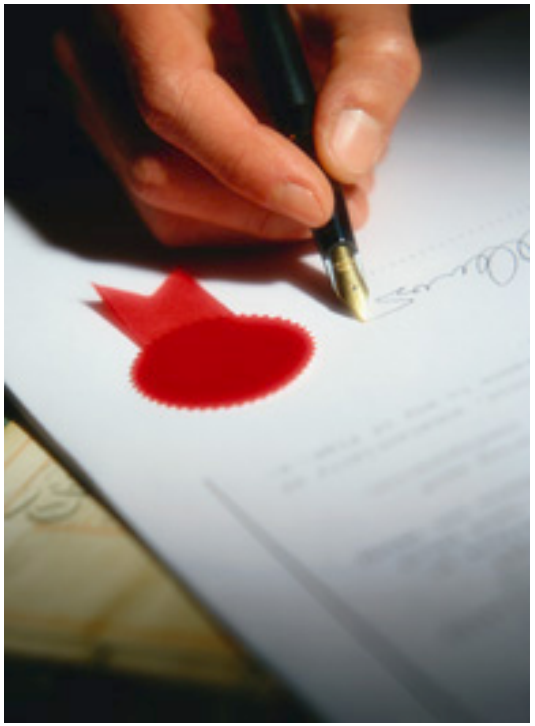
# Introdução

- ***Criptoanálise*** : a arte ou ciência de recuperar uma determinada informação criptografada sem possuir a autorização (a chave, a senha ou até mesmo o conhecimento do algoritmo utilizado).
- Uma tentativa de criptoanálise é comumente chamada de ***ataque***.

# Motivação

- A necessidade de sigilo, integridade e autenticação
  - Mensagens e dados precisam ser protegidos de sorte que somente pessoas ou processos autorizados consigam utilizá-los
  - Deve-se evitar alteração fraudulenta da informação, e mesmo criação de informação falsa ou destruição de informação correta.
  - Origem da Informação

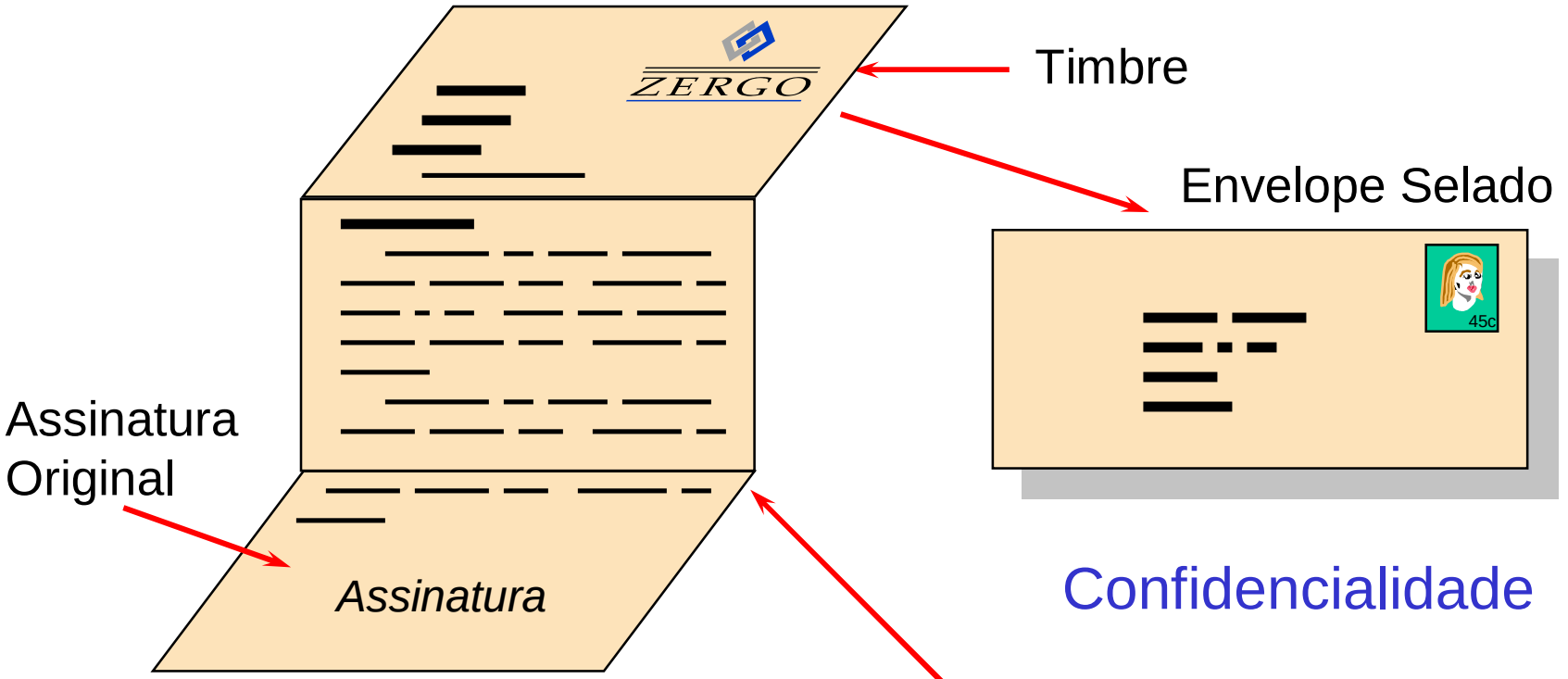
# Exemplo de Aplicação



Técnicas e Algoritmos de Criptografia:

Transferir a credibilidade baseada em conhecimento e papel para o ambiente do comércio eletrônico

# Mecanismos de Segurança baseada em Papel



# Serviços de Segurança Eletrônica

## Autenticação

Quem é a origem?

## Integridade

O conteúdo foi alterado?

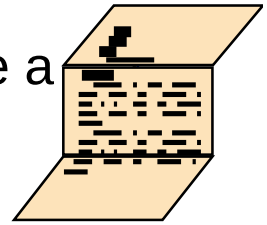
## Não Repúdio

O remetente pode negar ter sido a origem da informação?

## Confidencialidade

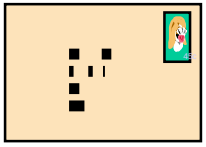
## Assinatura Digital

Substitui o timbre e a assinatura do documento original



## Criptografia

Substitui o envelope

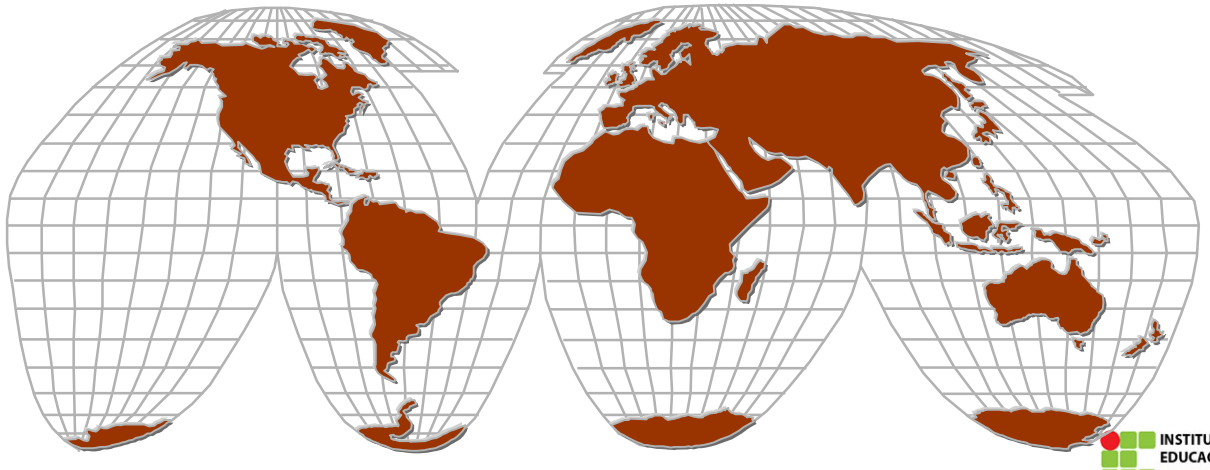


INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
SUL DE MINAS GERAIS
Campus Muzambinho

# Internet & Segurança

- Mais de 70% das fraudes eletrônicas tem origem em público interno
- As oportunidades de acesso a redes corporativas estão aumentando com o crescimento da Internet
- 75% das empresas contabilizam perdas por falhas de segurança por fraudes financeiras, roubo de informações proprietárias ou furto de lap-tops

Fonte: Forester Research



# Fundamentos da Credibilidade

## Autenticação

- Identificação de uma pessoa ou entidade

## Confidencialidade

- A informação é mantida privada

## Integridade

- A informação não pode ser modificada

## Não Repúdio

- A origem da informação não pode ser negada

# Aplicações

- Basicamente, a criptografia é utilizada para garantir:
  - Sigilo de informações
  - Integridade de informações
  - Autenticação de usuário
  - Autenticação de remetentes
  - Autenticação de destinatários
  - Autenticação de tempestividade

# Criptografia Tradicional

- Até o advento dos computadores um dos fatores determinantes do sucesso ou fracasso de um dado método de criptografia era a habilidade que os seus usuários tinham para realizar as transformações necessárias.

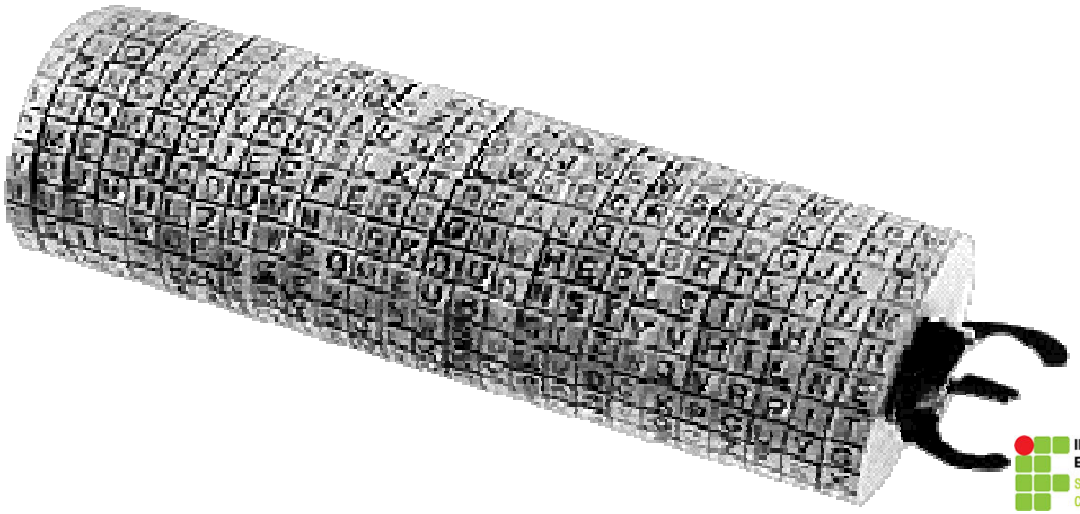
# História: A Roma Antiga

A palavra criptografia tem sua origem no grego e significa “Palavra Oculta”. Júlio César escrevia textos criptografados para Cícero e para seus generais a mais de 2.000 anos atrás. A Cifra de César - substituia cada letra do texto por outra que está três letras adiante na ordem alfabética.

A palavra CESAR é escrita como FHVDU

# A Roda Criptográfica - Século 18

Thomas Jefferson utilizou este recurso para manter comunicações privadas quando foi representante junto ao governo Francês (1784-1789) porque na época, os serviços de correio abriam toda a correspondência enviada ou recebida



# A Máquina Enigma - Século 20

A máquina Enigma foi um dos segredos mais bem guardados na Segunda Grande Guerra, usada pelos Alemães para proteger as comunicações entre o comando e as embarcações navais

# Criptografia Contemporânea

- A criptografia contemporânea não é mais baseada em obscuridade, ou seja, não se utiliza mais a suposição de que qualquer sistema pode ser seguro na medida em que ninguém, exceto seus criadores, tem acesso à metodologia ou aos algoritmo utilizados internamente ao sistema.

# Criptografia Contemporânea

- Para uso moderno, um criptosistema deve ter sua segurança baseada não nos algoritmos de cifragem e decifragem, mas sim em um valor secreto – uma **chave**.

# Segurança

- O mecanismo deve ser tão seguro que nem mesmo o autor de um algoritmo deve ser capaz de decifrar um texto cifrado sem dispor da chave apropriada. Assim, assume-se que um criptoanalista conhece *todo* o criptosistema, *exceto* as chaves utilizadas.

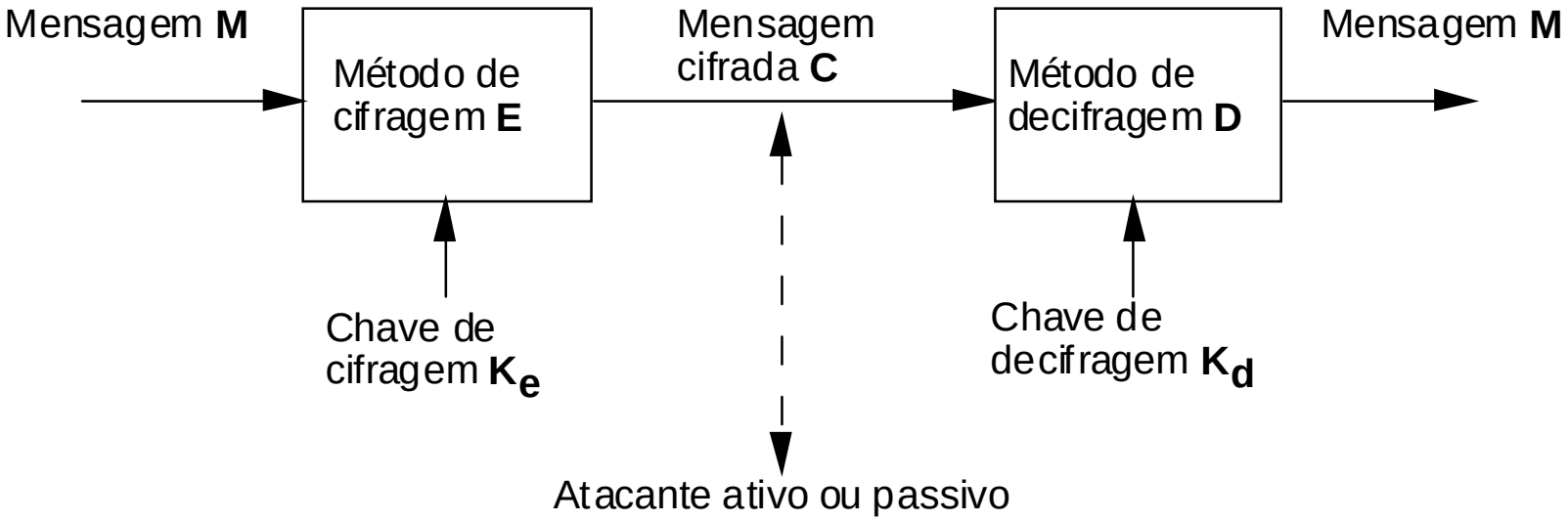
# Premissas de segurança

- Para um algoritmo ser analisado do ponto de vista de sua robustez a ataques são assumidas as seguintes premissas :
  - O criptoanalista tem acesso à descrição completa do algoritmo.
  - O criptoanalista tem acesso a grandes volumes de mensagens originais e suas mensagens cifradas correspondentes.
  - É capaz de escolher quais mensagens serão cifradas e receber as mensagens cifradas.

# Modelo de criptosistema

- Finalidade básica:
  - cifrar uma mensagem através de um **método de cifragem**, que recebe como entrada a própria **mensagem** e uma **chave de cifragem**, produzindo como resultado uma **mensagem cifrada**. Esta mensagem cifrada é então armazenada em um meio qualquer ou transmitida até um receptor.
  - Para **decifrar** a mensagem utiliza-se um **método de decifragem**, que recebe como entradas a **mensagem cifrada** e uma **chave de decifragem** e fornece como saída a mensagem original.

# Modelo de Criptossistema



# Modelo de Criptossistema

- Matematicamente, tem-se:
  - $C = E ( M, K_e )$
  - $M = D ( C, K_d ) = D ( E ( M, K_e ), K_d )$
- Ataques
  - Existem basicamente 5 tipos de ataques, todos eles supõe que o criptoanalista conhece os métodos de cifragem e decifragem.

# Ataque do texto cifrado

- O criptoanalista tem a sua disposição uma grande quantidade de mensagens cifradas, mas desconhece as mensagens originais e as chaves utilizadas.
- Dado: $C_1 = E(M_1,K_e)$, $C_2 = E(M_2,K_e)$, . . . $C_n = E(M_n,K_e)$.
- Deduzir: $M_1$, $M_2$, . . . $M_n$; ou $K_e$ ($K_d$); ou um método para inferir $M_{n+1}$ a partir de $C_{n+1}$.

# Ataque do texto conhecido

- O criptoanalista não somente tem a sua disposição uma grande quantidade de mensagens cifradas, mas conhece também as mensagens originais equivalentes.
- Dado: $M_1$, $C_1 = E(M_1,K_e)$, $M_2$, $C_2 = E(M_2,K_e)$, . . . $M_n$, $C_n = E(M_n,K_e)$.
- Deduzir: $K_e$ ($K_d$); ou um método para inferir $M_{n+1}$ a partir de $C_{n+1}$

# Ataque adaptativo do texto escolhido

- Pode existir uma realimentação entre uma mensagem escolhida para cifragem e a próxima mensagem.
  - Dado: $M_1$, $C_1 = E(M_1,K_e)$, $M_2$, $C_2 = E(M_2,K_e)$, . . . $M_n$, $C_n = E(M_n,K_e)$, onde o criptoanalista escolhe $M_1$, $M_2$, . . . $M_n$ em diferentes instantes no tempo, após analisar $C_1$, $C_2$, . . . $C_n$.
  - Deduzir: $K_e$ ($K_d$); ou um método para inferir $M_{n+1}$ a partir de $C_{n+1}$.

# Ataque do texto cifrado escolhido

- Pode produzir uma mensagem cifrada específica para ser decifrada e obter o resultado produzido. Este ataque é utilizado quando se tem uma "caixa-preta" que faz decifragem automática. Sua tarefa é deduzir as chaves utilizadas.
  - Dado: $C_1$, $M_1 = E(C_1,K_d)$, $C_2$, $M_2 = E(C_2,K_d)$, . . . $C_n$, $M_n = E(C_n,K_d)$, onde o criptoanalista escolhe $C_1$, $C_2$, . . . $C_n$.
  - Deduzir: $K_d$ ($K_e$).

# Ataque da chave escolhida

- Embora não considerado por muitos especialistas como sendo um ataque (não é um ataque quando a chave é conhecida), um criptoanalista pode testar o sistema com diversas chaves diferentes, ou pode convencer diversos usuários legítimos do sistema a utilizarem determinadas chaves. Neste último caso, a finalidade imediata seria poder decifrar as mensagens cifradas com estas chaves.

# Criptografia tradicional

- Criptografia orientada a caracteres.
  - substituindo um caracter por outro ou trocando caracteres de posição.
  - Atualmente a complexidade aumentou e em vez de caracteres se trabalham com bits, mas os métodos básicos continuam a ser utilizados.
  - Note-se que todos os métodos da criptografia tradicional são sistemas simétricos, ou seja, utiliza-se para a decifragem a mesma chave da cifragem.

# Cifras de substituição

- Cifragem : cada caracter (ou grupo de caracteres) na mensagem é substituído por outro na mensagem cifrada. Esta substituição é realizada para tornar o texto cifrado mais obscuro e incompreensível.
- Decifragem : é feita realizando-se a substituição inversa, de forma a restaurar os caracteres do texto original.

# Substituição monoalfabética

- Cada caracter é substituído por outro, de acordo com uma tabela ou uma regra simples.
  - Cifra de César : cada caracter é substituído por três caracteres adiante do alfabeto. Assim, A é substituído por D, B por E, etc.
    - Generalização : o alfabeto é deslocado de *k* posições, onde *k* é a chave a ser utilizada.
  - ROT13 : os caracteres avançam 13 posições (A se torna N, B é O, . . ., N é A, O é B, etc).

# Substituição polialfabética

- É uma combinação do uso de várias substituições monoalfabéticas, usadas em rotação de acordo com algum critério ou chave.
  - Assim, por exemplo, poderiam ser usadas 4 tabelas, em alternância a cada quatro caracteres : a primeira para os caracteres localizados nas posições 1, 5, 9, 13, etc; a segunda nas posições 2, 6, 10, 14, etc;

# Substituição por polígramos

- Utiliza grupos de caracteres em vez de trabalhar com caracteres individuais. Assim, por exemplo, se forem considerados trigramas, “ABA” poderia ser substituído por ”RTQ”, “ABB” por “KXS”, etc. Note-se que as tabelas de substituição aumentam rapidamente ($26^2$ para digramas, $26^3$ para trigramas, e assim por diante).

# Cifras de transposição

- Cada caracter permanece inalterado, mas sua posição na mensagem é alterada de acordo com alguma regra ou função (que também podem estar baseadas em alguma chave).
- A diferenciação entre os métodos é bem fácil. Se a frequência for a mesma da língua, trata-se de uma transposição. Se não, tem-se uma substituição.

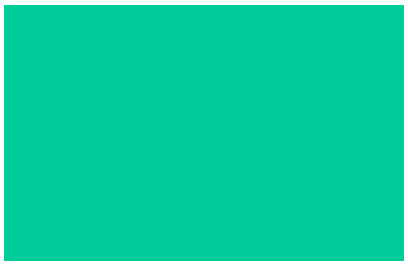
# Técnicas de Cifragem

- Cifragem por blocos
  - A entrada para o algoritmo consiste de um bloco de bits de texto, e de tamanho fixo; a saída também é um bloco de bits, de tamanho fixo.
- Cifragem bit a bit
  - Utiliza-se um gerador de bits que gera uma cadeia criptografica de bits. Cada bit do texto original é combinado com um bit da cadeia criptográfica, formando um bit de saída. Tipicamente esta operação é um ou exclusivo.

# Cifragem por bloco

Chave

Bloco de entrada
(*l bits)*



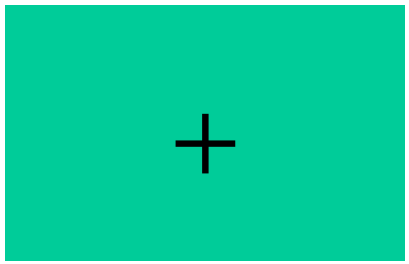
Bloco de saída
(*m bits)*

Cifrador por blocos

# Cifragem bit-a-bit

Gerador de Bits

Bit de entrada



Bit de saída

Cifrador bit-a-bit

# Encadeamento por blocos

- Realimentação de texto original
  - cifragem: $Y_i = C(X_i + U_i) \qquad (i = 1, 2, ...)$
    - onde Xi é o i-ésimo bloco de texto original
    - Ui é dado por :
      - $U_1 = Z$
      - $U_i = X_{i-1} \qquad (i = 2, 3, ...)$
  - decifragem: $X_i = D(Y_i) + U_i \qquad (i = 1, 2, ...)$

# Encadeamento por blocos

- Realimentação de texto cifrado
  - cifragem: $Y_i = C(X_i + U_i)$ $(i = 1, 2, ...)$
    - onde Xi é o i-ésimo bloco de texto original
    - Ui é dado por :
      - $U_1 = Z$
      - $U_i = X_{i-1}$ $(i = 2, 3, ...)$
  - decifragem: $X_i = D(Y_i) + U_i$ $(i = 1, 2, ...)$

Exercícios:

1 – Implemente a Cifragem e a Decifragem da Cifra de César.

2 – Implemente a Cifragem e a Decifragem ROT13

3 – Implemente uma Cifragem e Decifragem Alfabética utilizando digramas.