



Algoritmos de criptografia

Prof. Dieisson Martinelli

dieisson.martinelli@udesc.br

Programa

- Introdução à criptografia
- Cifras de substituição e de transposição
- Classificação das cifras
- Técnicas clássicas de criptografia
 - Cifra de César
 - Cifra Monoalfabética
 - Cerca de Ferrovia
 - Cifra de Playfair
- Atividades

Criptografia

- A palavra “**criptografia**” vem do grego **Kriptos** que significa “escrita secreta”

▶ **Kriptos** (em grego) = Secreto + **Grafia** (de escrever)

▶ **Criptografia** = Escrita secreta

- Criar **mensagens cifradas**

- História de centenas de anos
 - Ex.: Cifras hebraicas – Atbash, Albam e Atbah – de 600-500 aC, utilizadas em textos religiosos (ex.: Jeremias, Bíblia)

Criptografia

- Dois processos básicos estão envolvidos na **Criptografia**:

▶ **Cifrar**
(encriptar, codificar, criptografar)

▶ **Decifrar**
(decriptar, decodificar, descriptografar)

Criptografia

► Para se **criptografar** e/ou **descriptografar** uma informação é necessário utilizar-se, no mínimo de:

- Um **algoritmo criptográfico** (que atua como uma função); e
- Uma ou mais **chaves de encriptação**



Criptografia

- ▶ Para categorizar sistemas baseados em criptografia pode-se utilizar três abordagens:
 - ▶ Número de **chaves utilizadas**: que também determina se a criptografia é **Simétrica** (chave compartilhada) ou **Assimétrica** (chave pública)
 - ▶ Modo como o **texto claro** é **processado** no algoritmo de encriptação: **cifras de blocos**, onde os blocos são processados a cada vez; **cifras de fluxo**, elementos individuais são processados para obter encriptação / deciptação
 - ▶ Tipo de **operação** para ocasionar **encriptação**

Criptografia

- Todos os **algoritmos de criptografia** se baseiam em dois princípios gerais:

▶ Substituição

- Cada elemento é mapeado em outro

▶ Transposição

- Alteração da posição dos elementos

**Todas as operações
DEVEM ser reversíveis**

Cifras de substituição



Cifras de substituição podem ser:



Simples, apenas um símbolo é substituído de cada vez

- Cifras de **substituição simples** subdividem-se:
 - **Única** – cada símbolo é deslocado um **número fixo de posições**, módulo dimensão do alfabeto (ex: cifra de César)
 - **Polifônica** – a substituição é dirigida por uma **tabela de permutação**, determinada por uma **frase**
 - **Polialfabética** – usa uma entre várias **substituições monoalfabéticas**, dependendo da posição (ex: cifra Vigenère, rotor Enigma)

Cifras de substituição

- ▶ **Poligráfica**, a substituição envolve **vários símbolos** de cada vez (ex: Playfair)
- ▶ **Homofônica**, cada símbolo é substituído por **um entre vários símbolos** de um subconjunto (um-para-muitos)
 - Ex.: a letra ‘a’ pode ser codificada nos valores ‘29’, ‘35’, ‘82’ ou ‘87’; e na decodificação qualquer um desses valores será traduzido na letra ‘a’

Cifras de transposição

► **Trocam a ordem** das letras da mensagem utilizando um determinado critério e gerando um **anagrama**

- Exemplo: uma **palavra** de três letras pode gerar apenas **seis combinações** diferentes:

Transposições:

PAI → PIA → AIP → API → IAP → IPA

- A transposição **eleva a segurança**, entretanto, aumenta as dificuldades de **recuperação da mensagem**
 - Outros exemplos: CARRO → ORARC;
ARGENTINO → IGNORANTE (mas não seja indelicado)

Classificação das cifras

 As **técnicas anteriores** ainda podem ser classificadas em:

Cifras de bloco

- Blocos são processados a cada vez

Cifras de fluxo

- Elementos individuais são processados para obter a encriptação/decriptação

Técnicas clássicas de criptografia

Cifra de César

- Uso mais antigo baseado em uma **cifra de substituição**
- Consiste em substituir **cada letra** do alfabeto pela letra que fica **K posições** adiante
- Por exemplo, se $K = 3$

Texto normal:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Texto cifrado:

DEFGHIJKLMNOPQRSTUVWXYZABC

Técnicas clássicas de criptografia

► Cifra de César – Algoritmo

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

Encriptação

$$C = (k + n) \bmod 26$$

Onde:

C = Texto Cifrado

K = Deslocamento

N = Texto Puro

Por exemplo, para encriptar S com K = 3

$$C = (3+18) \bmod 26$$

$$C = 21 \bmod 26$$

$$C = 21$$

Portanto **S = V**

Decriptação

$$C = (k - n) \bmod 26$$

Por exemplo, para decriptar V com K = 3

$$C = (3-21) \bmod 26$$

$$C = 18 \bmod 26$$

$$C = 18$$

Portanto **V = S**

Técnicas clássicas de criptografia

Cifra Monoalfabética

- A Cifra de César tem um **universo de chaves** muito restrito = **26 possibilidades** de K (em geral)
- Na **Cifra Monoalfabética**, cada substituição pode ser, portanto, uma possibilidade de 26 permutações
 - Qualquer letra pode ser substituída por qualquer outra, contanto que cada letra tenha uma substituta exclusiva

Alfabeto Normal:

a b c d e f g h i j k l m n o p q r s t u v w x y z

Monoalfabeto:

m n b v c x z a s d f g h j k l p o i u y t r w e q

Técnicas clássicas de criptografia

► Cifra Monoalfabética – **Exemplo**

- A mensagem em **texto aberto**:

"Bob, i love you. Alice."


- **Mensagem cifrada**:

"Nkn, s gktc wky. Mgsbc."

- Como as substituições se baseiam em **valores aleatórios**, o processo é **mais seguro** que a substituição com um padrão regular (k posições)
 - Usar força bruta para experimentar 10^{26} permutações demandaria muito esforço; A análise estatística da mensagem seria mais fácil de quebrar o código (ex. Identificar letras e grupos de letras mais frequentes)

Técnicas clássicas de criptografia

Cerca de Ferrovia:

- Consiste em alternar as **letras** em **duas linhas** (ou mais) para gerar a mensagem cifrada.
- A **chave** do algoritmo é um número inteiro N que corresponderá ao número de linhas alternadas (em zigue-zague) 
- Exemplo para $N = 2$

Texto plano:

SEGURANÇA EM COMPUTAÇÃO

Texto alternado:

S G R N A M O P T C O
E U A C E C M U A A

Texto cifrado:

SGRNAMOPTCOEUACECMUAA

Técnicas clássicas de criptografia

- **Cerca de Ferrovia – Codificação:**

- Texto = “ESTRUTURA DE DADOS”

- **N = 2**

E	.	T	.	U	.	U	.	A	.	E	.	A	.	0	.
.	S	.	R	.	T	.	R	.	D	.	D	.	D	.	S

 → ETUUAEAO SRTRDDDS

- **N = 3**

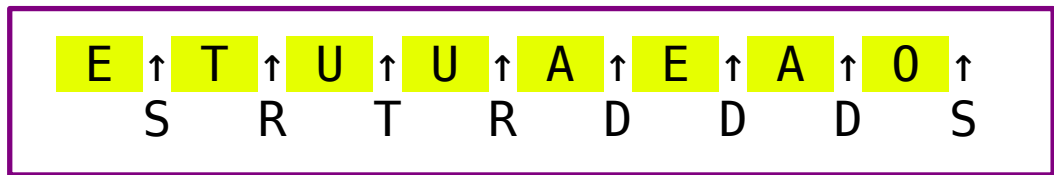
E	.	.	.	U	.	.	.	A	.	.	.	A	.	.	.
.	S	.	R	.	T	.	R	.	D	.	D	.	D	.	S
.	.	T	.	.	.	U	.	.	.	E	.	.	.	0	.

 → EUAASRTRDDDS TUEO

Técnicas clássicas de criptografia

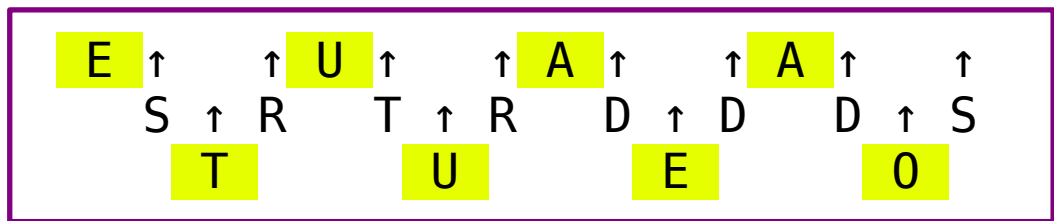
- **Cerca de Ferrovia – Decodificação:**

- Texto = “ETUUAEAOSRTRDDDS”, **N = 2**



→ ESTRUTURADEDADOS

- Texto = “EUAASRTRDDDDSTUEO”, **N = 3**



→ ESTRUTURADEDADOS

Técnicas clássicas de criptografia

Cifra Playfair

- Técnica estabelecida em 1854
- Tem como princípio usar uma **tabela (matriz) de 5x5** contendo as **letras do alfabeto**
- Essa matriz é preenchida de acordo com os seguintes **critérios**:
 - ▶ Para facilitar a memorização, o preenchimento da matriz inicia com uma **palavra-chave**
 - ▶ O restante das **células** é preenchido com as letras em ordem alfabética, **sem repetição** da palavra-chave
 - ★ **Letras iguais** na própria **palavra-chave** também não devem se **repetir**

Técnicas clássicas de criptografia

- Cifra Playfair – **Tabela**

F	I	R	S	T
A	M	E	N	D
B	C	G	H	K
L	O	P	Q	U
V	W	X	Y	Z

Tabela 5 x 5 (25 letras)



Chave escolhida:
= **FIRST AMEND**



Restante da tabela:
Letras em **ordem alfabética**,
e **não repetir** letras da chave

- **Observações:**

- **1** das 26 letras do alfabeto pode ser desconsiderada para compatibilidade da tabela (normalmente “**Q**”)
- “**I**” pode se igual a “**J**” para compatibilidade da tabela

Técnicas clássicas de criptografia

Cifra Playfair – **Exemplo**

- **Passo 1:** processo de decomposição
 - O texto plano a ser encriptado deve ser decomposto em grupos de 2 letras

Texto plano:
ATACAR AMANHÃ

Texto decomposto:
AT AC AR AM AN HA

Técnicas clássicas de criptografia

- Se a **2ª. letra** de um grupo é idêntica à **1ª.**, substitua por **X**, e transfira a **2ª. letra** para o **próximo bloco**

Texto plano:

HIDE THE GOLD IN THE TR**EE** STUMP

Texto decomposto:

HI DE TH EG OL DI NT HE TR **EX ES** TU MP

- Se necessário, inclua **Z** para **completar o grupo**

Texto plano:

MENSAGEM SECRETA

Texto decomposto:

ME NS AG EM SE CR ET **AZ**

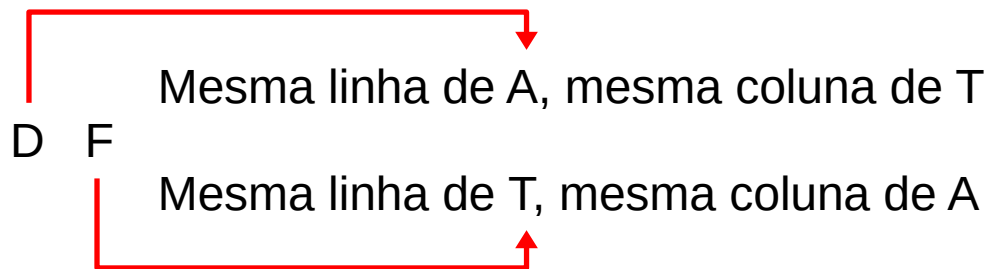
Técnicas clássicas de criptografia

● Passo 2: processo de **encriptação Playfair**

- **Regra 1:** se o par de caracteres está em linhas e colunas diferentes na tabela, **cada caractere** é substituído pelo **caractere oposto** de mesma linha e coluna (formando um **retângulo na tabela**)
- Por exemplo, em: **AT** AC AR AM AN HA

AT torna-se **DF**

F	I	R	S	T
A	M	E	N	D
B	C	G	H	K
L	O	P	Q	U
V	W	X	Y	Z

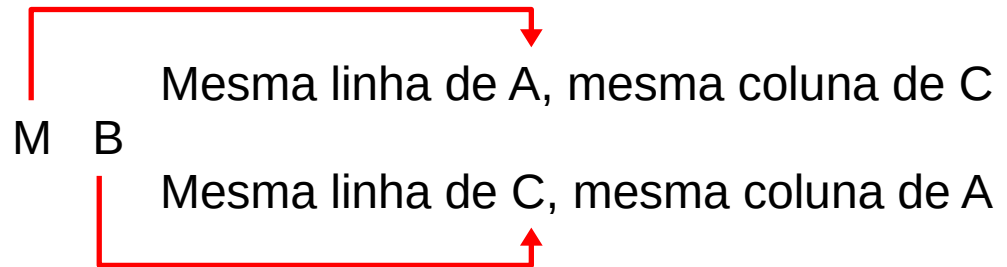


Técnicas clássicas de criptografia

- Neste próximo grupo também aplicar a **Regra 1**:
- Em: **AT** **AC** AR AM AN HA

AC torna-se **MB**

F	I	R	S	T
A	M	E	N	D
B	C	G	H	K
L	O	P	Q	U
V	W	X	Y	Z



Substituição formando um retângulo

Técnicas clássicas de criptografia

- Neste próximo grupo também aplicar a **Regra 1**:
- Em: AT AC **AR** AM AN HA

AR torna-se **EF**

F	I	R	S	T
A	M	E	N	D
B	C	G	H	K
L	O	P	Q	U
V	W	X	Y	Z

E F

Mesma linha de A, mesma coluna de R

Mesma linha de R, mesma coluna de A

Técnicas clássicas de criptografia

- **Regra 2:** Se um **par de caracteres** está na mesma linha, cada letra do par é substituída pela **próxima letra à direita** de onde a respectiva letra do par se encontra na tabela (rotacionando se necessário)
 - **1º. exemplo:** PQ torna-se **QU**
 - **2º. exemplo:** CH torna-se **GK**
 - **3º. exemplo:** IT torna-se **RF**

F	I	R	S	T
A	M	E	N	D
B	C	G	H	K
L	O	P	Q	U
V	W	X	Y	Z

Substituição de mesma linha
Exemplo 1.

F	I	R	S	T
A	M	E	N	D
B	C	G	H	K
L	O	P	Q	U
V	W	X	Y	Z

Substituição de mesma linha
Exemplo 2.

F	I	R	S	T
A	M	E	N	D
B	C	G	H	K
L	O	P	Q	U
V	W	X	Y	Z

Substituição de mesma linha
Exemplo 3.

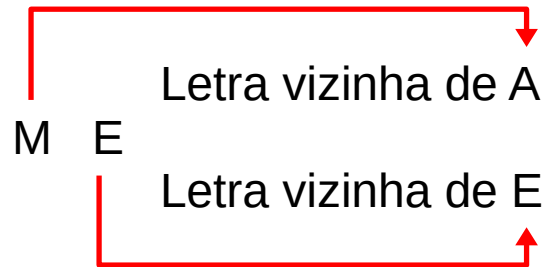
Técnicas clássicas de criptografia

- Aplicando a **Regra 2** no exemplo:
- Em: AT AC AR **AM** AN HA

AM torna-se **ME**

F	I	R	S	T
A	M	E	N	D
B	C	G	H	K
L	O	P	Q	U
V	W	X	Y	Z

Substituição de mesma linha



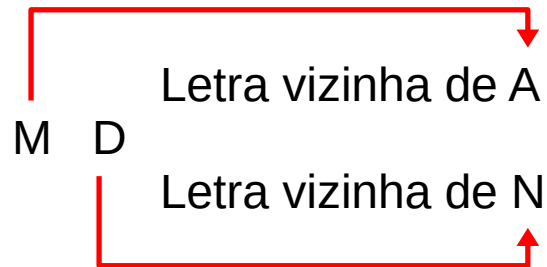
Técnicas clássicas de criptografia

- Neste próximo grupo também aplicar a **Regra 2**:
- Em: AT AC AR AM **AN** HA

AN torna-se **MD**

F	I	R	S	T
A	M	E	N	D
B	C	G	H	K
L	O	P	Q	U
V	W	X	Y	Z

Substituição de mesma linha

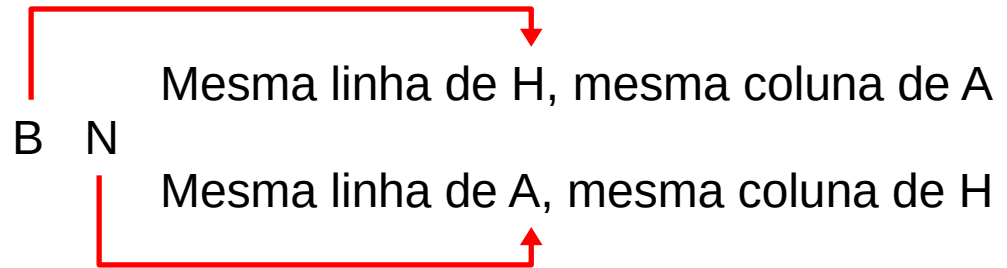


Técnicas clássicas de criptografia

- Neste último grupo também aplicar a **Regra 1**:
- Em: AT AC AR AM AN **HA**

HA torna-se **BN**

F	I	R	S	T
A	M	E	N	D
B	C	G	H	K
L	O	P	Q	U
V	W	X	Y	Z



Substituição formando um retângulo

Técnicas clássicas de criptografia

- **Regra 3:** Se um **par de caracteres** está na mesma coluna, cada letra do par é substituída pela **próxima letra abaixo** de onde a respectiva letra do par se encontra na tabela (rotacionando se necessário)
 - **1º. exemplo:** TK torna-se **DU**
 - **2º. exemplo:** GX torna-se **PR**

F	I	R	S	T
A	M	E	N	D
B	C	G	H	K
L	O	P	Q	U
V	W	X	Y	Z

Substituição de mesma coluna
Exemplo 1.

F	I	R	S	T
A	M	E	N	D
B	C	G	H	K
L	O	P	Q	U
V	W	X	Y	Z

Substituição de mesma coluna
Exemplo 2.

Técnicas clássicas de criptografia

- **Passo 3:** mensagem cifrada

Texto plano:
ATACAR AMANHÃ

Texto decomposto:
AT AC AR AM AN HA

Texto cifrado:
DF MB EF ME MD BN

Técnicas clássicas de criptografia

- **Passo 4: processo de deciptação Playfair**
 - Aplicar a **Regra 1** para as letras do grupo cifrado quando estiverem em linhas e colunas diferentes
 - Aplicar o procedimento oposto para as **Regras 2 e 3**, ou seja, pegar a próxima letra à esquerda (para a **Regra 2**) e próxima letra acima (para a **Regra 3**)
 - Assim que estiver pronto retirar os **Xs**, acertar os **Qs** ou incluir os respectivos **Js**, conforme o algoritmo

Atividades

- Utilizando como chave a palavra “SEGURANCA”, qual é o texto original da seguinte cifra de Playfair?

FDUSFPFACNMENMDSUROS DOME
VFNINATNSNGVGRV