Criptografia

Introdução

FURB
UNIVERSIDADE DE BLUMENAU

Bibliografia

AUMASSON, J.-P. **Serious Cryptography - A pratical introduction to modern encryption**. San Francisco, CA: Starch Press, Inc., 2018.

BURNETT, S.; PAINE, S. **Criptografia e segurança - O guia oficial RSA**. Rio de Janeiro: Elsevier, 2002.

CIFRA DE CÉSAR. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2019. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Cifra_de_C%C3%A9sar&oldid=54032443>. Acesso em: 12 jan. 2019.

https://web.archive.org/web/20160305112110/http://www.emc.com/emc-plus/rsa-labs/historical/the-rsa-laboratories-secret-key-challenge.htm

Criptografia

- O objetivo da criptografia é transformar dados legíveis em ilegíveis.
- Por exemplo, supor que o material sigiloso seja este:

```
Não acreditamos que a concorrência possa se igualar ao novo
conjunto de recursos, ainda que suas ofertas de suporte,
serviços e consultoria representem uma séria ameaça à nossa
capacidade de venda. Temos que investir mais dinheiro em nossa
```

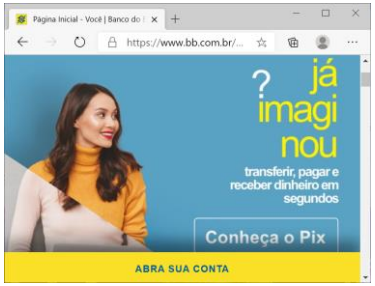
- Ao criptografá-lo, poderiam parecer com:

```
*╢+J%&=06&=X]\G8BG/4-3Q[]QVBF┤%)/%U6. 7+F?.S(#
3%67J*#F*<#&R&8[YM[M_3P198!/>49. HR4>$-
$F:&!U5LQK5VRUA?+7K(6D93?&31#@K266</┣*&R,O)+%54?0%4
3F]EKUG][MU^4@UQD8╣>/.I >+A╱2A┸U(86^7J[':-(-7+",A77U?6*.-
ES2/))7F<&$L";OQ@D">D''&:U":"#//"_9H]9C]A@S
```

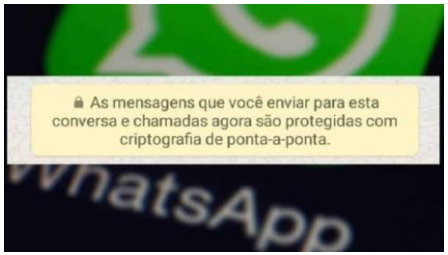
- Se o agente tiver acesso aos dados, a informação continua confidencial

Onde a criptografia é utilizada nos dias de hoje?

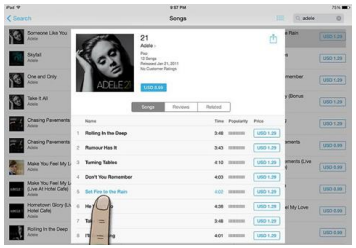
Em transações comerciais e financeiras na internet



Para trocar informações sigilosas entre pessoas



Para armazenar dados sigilosos

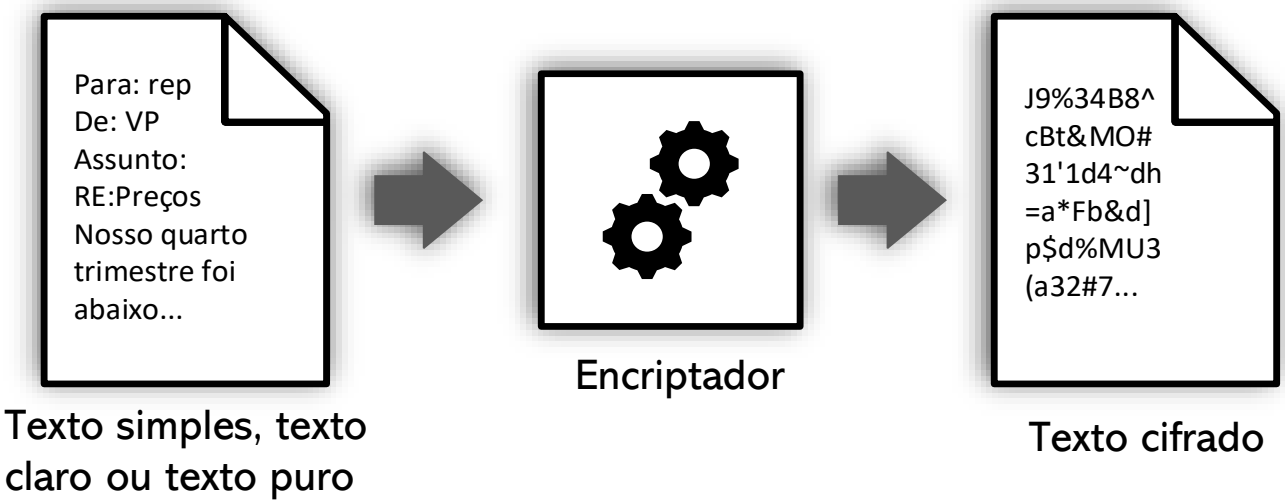


Criptografia

- Normalmente está associada à confidencialidade
  - Mas também é utilizada para tratar integridade, autenticidade e não-repúdio
- A criptografia não garante segurança dos dados
  - A criptografia é um instrumento entre vários
- A criptografia não é a prova de falhas
  - Pode ser quebrada
  - Se for implementada de forma incorreta, não agrega nenhuma segurança real

Conceitos

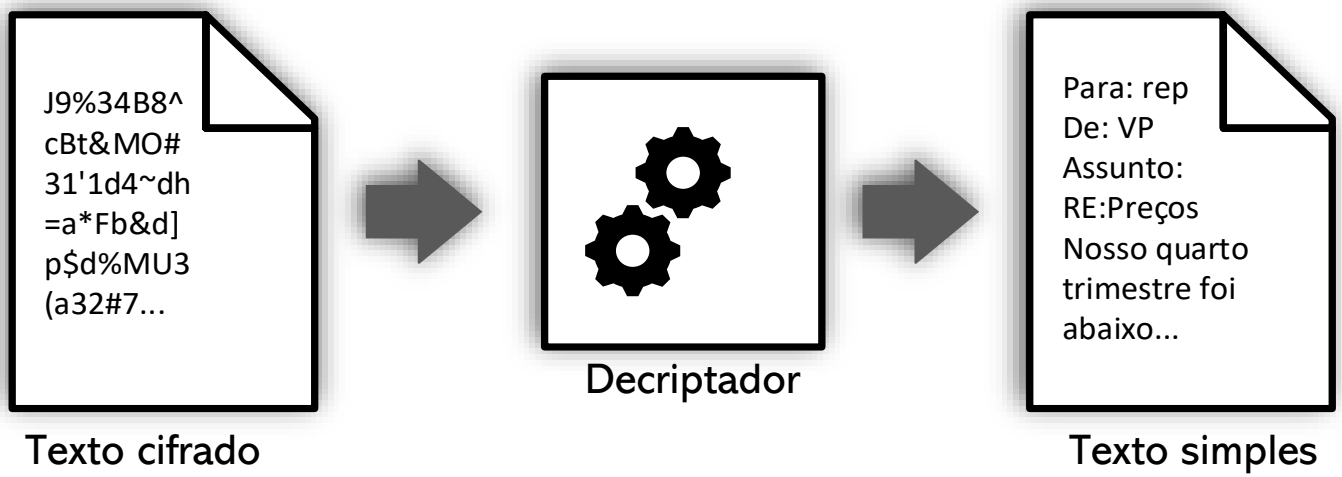
- Quando queremos converter informações sigilosas em algo ilegível, nós **criptografamos** os dados.



- São sinônimos de criptografia: codificar, encriptar ou cifrar.
- **Texto simples** - São dados que se quer manter em segredo. Pode ser texto legível para o ser humano ou um arquivo binário.

Conceitos

- Quando queremos converter o texto crifrado em texto simples (legível), nós **decriptografamos** os dados



- São sinônimos de decriptar: decodificar, decriptografar ou decifrar

Criptografia clássica e moderna

- A criptografia clássica refere-se aos algoritmos que foram utilizados antes da década de 1970.
- São algoritmos que requerem apenas caneta e papel para cifrar e decifrar
- O oposto da criptografia clássica é a criptografia moderna
  - Inviável sem o uso do computador
- Podem ser classificadas:
  - Cifras de substituição
  - Cifras de transposição

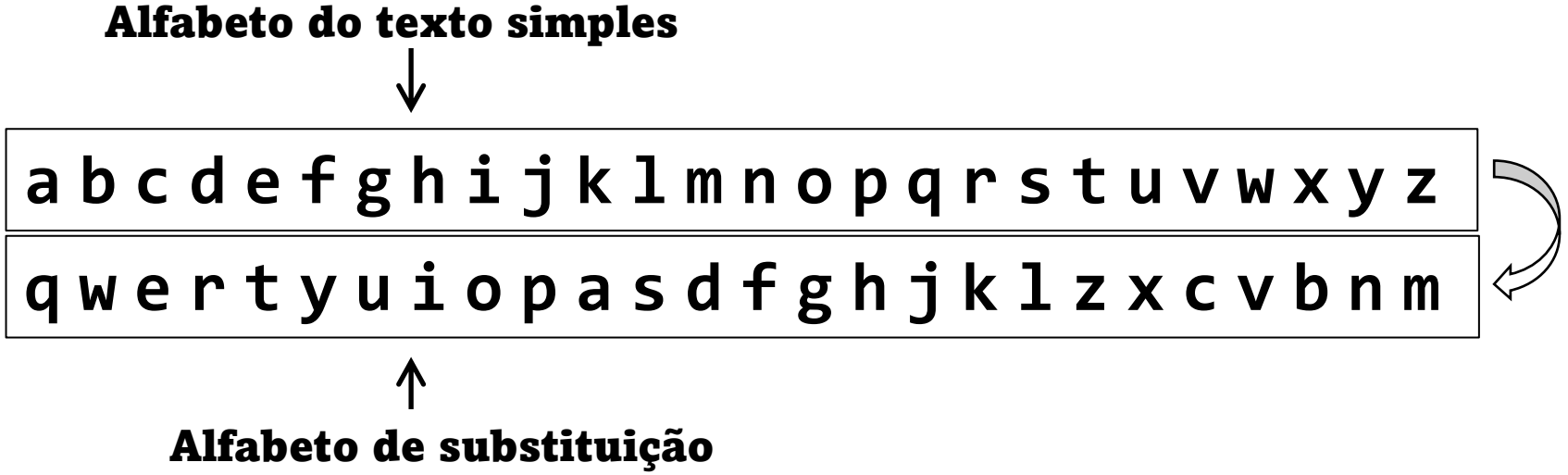
Cifras de substituição

FURB
UNIVERSIDADE DE BLUMENAU

Cifras de substituição

Criptografia clássica

- Cada caractere do texto simples é mapeado num novo caractere de um alfabeto de substituição



- Exemplo: a frase “Vamos invadir no domingo” seria cifrada:

```
vamos invadir no domingo
cqdgk ofcqrok fg rgdofug
```

Cifras de substituição

Criptografia clássica

- Em várias ocasiões, o texto cifrado era escrito sem espaços e sem pontuação

```
vamos invadir no domingo
cqdgk ofcqrok fg rgdofug

cqdgkofcqrokfgrgdofug
```

- Frequentemente, o texto era escrito em blocos de comprimento fixo

```
cqdgk ofcqr okfgr gdofu g
```

Cifras de substituição

Criptografia clássica

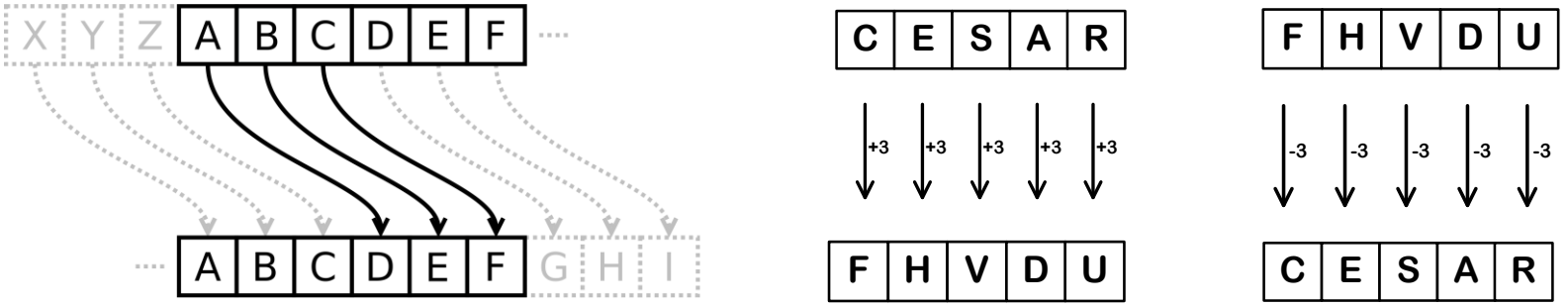
- A decifragem consiste em fazer o mapeamento do caractere cifrado para o alfabeto do texto simples

- As cifras de substituição foram amplamente utilizadas até a 2ª guerra mundial.

A cifra de César

Cifras de substituição

- A cifra de César foi utilizada aproximadamente em 50 a.C. para proteger mensagens de significado militar.
- O algoritmo de César encripta uma mensagem trocando os caracteres 3 posições à sua frente.



Fonte: CIFRA DE CÉSAR, 2018

Cifras de transposição

FURB
UNIVERSIDADE DE BLUMENAU

Cifras de transposição

- As cifras de transposição não utilizam substituição. Ao invés disso, alteram a disposição lógica dos caracteres

- Podem ser:
  - Transposição geométrica
    - São cifras que efetuam um rearranjo do texto usando uma figura geométrica (quadrado ou retângulo). Pode ser colunar ou linear
  - Transposição em grades ou grelha

Cifra de transposição geométrica colunar

- Nesta cifra o texto simples é escrito numa matriz, em linhas. O texto cifrado é obtido a partir das **colunas**.
- A quantidade de colunas da matriz é um parâmetro de cifragem
  - Valor fixado
- Espaços não preenchidos são completados com algum outro caractere (X, _, ou espaço em branco eram típicos)
- Também conhecido simplesmente como “transposição colunar”

Cifra de transposição geométrica colunar

Exemplo de cifragem

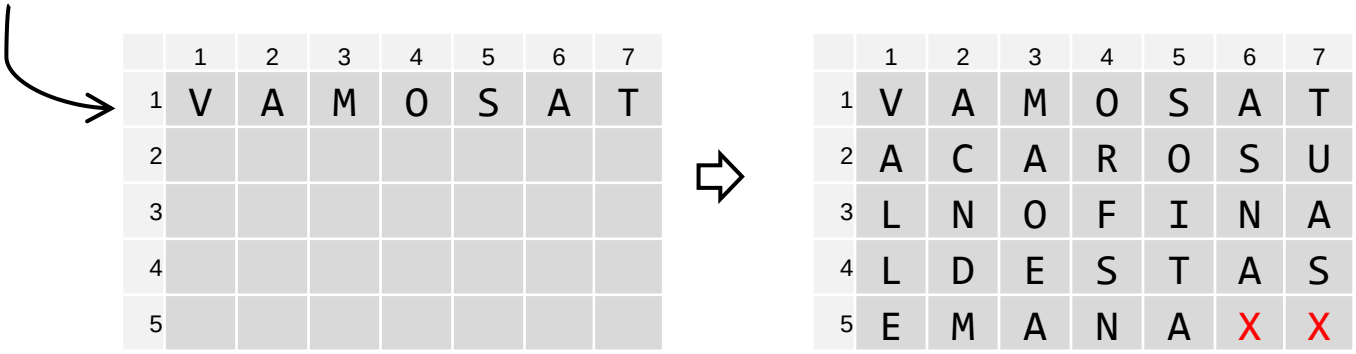
- Cifrar VAMOS ATACAR O SUL NO FINAL DESTA SEMANA

  Usando 7 colunas

- Remover os espaços em branco

  VAMOSATACAROSULNOFINALDESTASEMANA

O texto tem 33 caracteres, logo, usar uma matriz com 5 linhas



	1	2	3	4	5	6	7
1	V	A	M	O	S	A	T
2							
3							
4							
5							

	1	2	3	4	5	6	7
1	V	A	M	O	S	A	T
2	A	C	A	R	O	S	U
3	L	N	O	F	I	N	A
4	L	D	E	S	T	A	S
5	E	M	A	N	A	X	X

- Saída (texto cifrado):

  VALLEACNDMMAOEAORFSNSOITAASNAXTUASX

Cifra de transposição geométrica colunar

Exemplo de decifragem

- Para decifrar, o texto cifrado deve preencher uma matriz em colunas. O texto simples é extraído a partir das linhas

- Usando 7 colunas, decifrar:

  VALLEACNDMMAOEAORFSNSOITAASNAXTUASX

Como o texto tem 35 caracteres, uma matriz de 7 colunas terá 5 linhas

	1	2	3	4	5	6	7
1	V						
2	A						
3	L						
4	L						
5	E						

	1	2	3	4	5	6	7
1	V	A	M	O	S	A	T
2	A	C	A	R	O	S	U
3	L	N	O	F	I	N	A
4	L	D	E	S	T	A	S
5	E	M	A	N	A	X	X

- Saída (texto decifrado):
  VAMOSATACAROSULNOFINALDESTASEMANAXX

Cifra de transposição geométrica linear

- Semelhante à cifra de transposição geométrica colunar, porém o texto simples é escrito em coluna e o texto cifrado é obtido a partir das linhas

- A quantidade de linhas da matriz é um parâmetro de cifragem
  - Valor fixado

Cifra de transposição geométrica linear

Exemplo de cifragem

- Usando 4 linhas, cifrar

  VAMOS ATACAR O SUL NO FINAL DESTA SEMANA

  VAMOSATACAROSULNOFINALDESTASEMANA

33 caracteres

	1	2	3	4	5	6	7	8	9
1	V	S	C	S	O	A	S	E	A
2	A	A	A	U	F	L	T	M	X
3	M	T	R	L	I	D	A	A	X
4	O	A	O	N	N	E	S	N	X

- Texto cifrado:

  VSCSOASEAAAAUFLTMXMTRLIDAAXOAONNESNX

Cifra de transposição geométrica linear

Exemplo de decifragem

- Para decifrar, o texto cifrado deve preencher uma matriz em linhas. O texto simples é extraído a partir das colunas

- Exemplo: Usando 4 linhas decifrar:

  VSCSOASEAAAAUFLTMXMTRLIDAAXOAONNESNX

36 caracteres

	1	2	3	4	5	6	7	8	9
1	V	S	C	S	O	A	S	E	A
2	A	A	A	U	F	L	T	M	X
3	M	T	R	L	I	D	A	A	X
4	O	A	O	N	N	E	S	N	X

- Obtendo o texto a partir das colunas:

  VAMOSATACAROSULNOFINALDESTASEMANAXXX

Cifra de cerca ferroviária

FURB
UNIVERSIDADE DE BLUMENAU

Cifra de cerca ferroviária (rail fence)

Cifra de transposição - exemplo

- O texto é escrito em diagonal nos trilhos de uma cerca imaginária.
  - Começa do trilho superior indo em direção para o inferior.
  - Ao atingir o inferior, prossegue até o trilho superior novamente.
  - Permanece neste ciclo até terminar a mensagem
- Exemplo para cifrar “VAMOS INVADIR O SUL AMANHA”

```
V · · · S · · · A · · · O · · · A · · · H ·
· A · O · I · V · D · R · S · L · M · N · A
· · M · · · N · · · I · · · U · · · A · · ·
```

- A mensagem criptografada é constituída dos caracteres registrados em cada trilha (da superior para inferior)

V S A O A H A O I V D R S L M N A M N I U A

Cifra de cerca ferroviária (rail fence)

Exemplo de decifragem

- Parar decifrar, é preciso conhecer a quantidade de trilhas que foi utilizada.

. . . .
. . . .
. . . .

- A técnica sugere cifrar uma string com mesma extensão, mas constituído de um caractere arbitrário.

@ @

22 caracteres

@ . . . @ . . . @ . . . @ . . . @ . . . @ . . . @ .
. @ . @ . @ . @ . @ . @ . @ . @ . @ . @ . @ . @
. . @ . . . @ . . . @ . . . @ . . . @ . . . @ . . .

Cifra de cerca ferroviária (rail fence)

Exemplo de decifragem

- Em seguida, percorre-se a matriz linha a linha. A cada ocorrência do caractere arbitrário, substitui-se por um caractere do texto cifrado

V S A O A H A O I V D R S L M N A M N I U A

V · · · S · · · A · · · O · · · A · · · H ·
· A · O · I · V · D · R · S · L · M · N · A
· · M · · · N · · · I · · · U · · · A · · ·

- Para extrair o texto decifrado, fazer o caminho em zigue-zague, para obter um caractere e compor o texto