Criptografia

Disciplina: Laboratório de Programação II

Professor Luciano Brum
Email: lucianobrum18@gmail.com

Assunto da aula de hoje:

Criptografia

Criptografia

- Interligação de universidades e agencias de pesquisa.
- Uso acadêmico.

Criptografia

- Interligação de universidades e agencias de pesquisa.
- Uso acadêmico.
- Pouca preocupação com segurança:

Criptografia

- Interligação de universidades e agencias de pesquisa.
- Uso acadêmico.
- Pouca preocupação com segurança:
  - Uso por especialistas.
  - Correio Eletrônico.
  - Troca de arquivos e documentos.
  - Acesso restrito.
  - Confiança mútua.
  - Poucos casos de má utilização.

Criptografia

- Inicialmente, computadores eram apenas utilizadas por pesquisadores e funcionários de empresas para envio de mensagens de correio eletrônico e compartilhamento de impressoras.

Criptografia

- Inicialmente, computadores eram apenas utilizadas por pesquisadores e funcionários de empresas para envio de mensagens de correio eletrônico e compartilhamento de impressoras.

- Segurança não era uma preocupação.

Criptografia

- Inicialmente, computadores eram apenas utilizadas por pesquisadores e funcionários de empresas para envio de mensagens de correio eletrônico e compartilhamento de impressoras.

- Segurança não era uma preocupação.

- Situação hoje: milhões de pessoas utilizando computadores.

Criptografia: Situação Atual

- **Utilização para situações não previstas:**

Criptografia: Situação Atual

- **Utilização para situações não previstas:**
- **Acesso irrestrito;**

Criptografia: Situação Atual

- **Utilização para situações não previstas:**
- **Acesso irrestrito;**
- **Mecanismos fracos de identificação e autenticação;**

Criptografia: Situação Atual

- **Utilização para situações não previstas:**
- **Acesso irrestrito;**
- **Mecanismos fracos de identificação e autenticação;**
- **Sociedade eletrônica:**

Criptografia: Situação Atual

- **Utilização para situações não previstas:**
- **Acesso irrestrito;**
- **Mecanismos fracos de identificação e autenticação;**
- **Sociedade eletrônica:**
  - Utopia x Caos.
  - Fonte de conhecimento x Validade da Informação.
  - Autoestrada da Informação x Superoferta de Informação.
  - Código de ética não escrito.
  - Existência de vândalos, malfeitores, bandidos, terroristas.
  - Necessidade de mecanismos de defesa.

Criptografia: Situação Atual

- **Transações bancárias.**
- **E-commerce.**
- **Devolução de impostos.**
- **Informações confidenciais entre funcionários.**

Criptografia: Situação Atual

- **Transações bancárias.**
- **E-commerce.**
- **Devolução de impostos.**
- **Informações confidenciais entre funcionários.**

- Segurança passa a ser uma preocupação neste momento !

Criptografia

- **A maioria dos problemas surgem devido à ação de pessoas mal-intencionadas**!

Criptografia

- **A maioria dos problemas surgem devido à ação de pessoas mal-intencionadas**!

- Que ações? Leitura/captura de informações confidenciais, modificação de mensagens, falsificação de mensagens, etc.

Criptografia

- **A maioria dos problemas surgem devido à ação de pessoas mal-intencionadas**!

- Que ações? Leitura/captura de informações confidenciais, modificação de mensagens, falsificação de mensagens, etc.

- Qual o objetivo? Chamar a atenção, obter algum benefício, prejudicar alguém ou algo, causar o caos, *hacktivistas* (*Mr. Robot*).

Criptografia

- **Tornar, por exemplo, uma rede segura, não se trata mais de lidar apenas com eventuais bugs.**

Criptografia

- **Tornar, por exemplo, uma rede segura, não se trata mais de lidar apenas com eventuais bugs.**

- **As vezes, é necessário lidar com adversários inteligentes e muito bem subsidiados ($$).**

Criptografia

- **Tornar, por exemplo, uma rede segura, não se trata mais de lidar apenas com eventuais bugs.**

- **As vezes, é necessário lidar com adversários inteligentes e muito bem subsidiados ($$).**

- **Nem sempre medidas usadas para interromper a atividade de hackers eventuais atingem os adversários ‘mais espertos’.**

Criptografia

Adversário	Objetivo
Estudante	Divertir-se bisbilhotando as mensagens de correio eletrônico de outras pessoas
Cracker	Testar o sistema de segurança de alguém; roubar dados
Representante de vendas	Tentar representar toda a Europa e não apenas Andorra
Executivo	Descobrir a estratégia de marketing do concorrente
Ex-funcionário	Vingar-se por ter sido demitido
Contador	Desviar dinheiro de uma empresa
Corretor de valores	Negar uma promessa feita a um cliente através de uma mensagem de correio eletrônico
Vigarista	Roubar números de cartão de crédito e vendê-los
Espião	Descobrir segredos militares ou industriais de um inimigo
Terrorista	Roubar segredos de armas bacteriológicas

Tabela 1: Algumas pessoas que podem causar problemas de segurança e suas razões. Fonte: TANENBAUM, 2011.

Criptografia: Conceito Básico.

- Criptografia é a arte ou ciência que trata das técnicas de tornar uma mensagem confusa, incompreensível para qualquer pessoa que não seja o destinatário da mesma

Criptografia: Conceito Básico.

- Criptografia é a arte ou ciência que trata das técnicas de tornar uma mensagem confusa, incompreensível para qualquer pessoa que não seja o destinatário da mesma

- A mensagem original é chamada texto normal, texto original, texto claro, texto aberto ou ainda texto plano.

Criptografia: Conceito Básico.

- Criptografia é a arte ou ciência que trata das técnicas de tornar uma mensagem confusa, incompreensível para qualquer pessoa que não seja o destinatário da mesma

- A mensagem original é chamada texto normal, texto original, texto claro, texto aberto ou ainda texto plano.

- O processo de usar uma técnica de criptografia é chamado encriptação ou criptografia.

Criptografia: Conceito Básico.

- Criptografia é a arte ou ciência que trata das técnicas de tornar uma mensagem confusa, incompreensível para qualquer pessoa que não seja o destinatário da mesma

- A mensagem original é chamada texto normal, texto original, texto claro, texto aberto ou ainda texto plano.

- O processo de usar uma técnica de criptografia é chamado encriptação ou criptografia.

- A mensagem resultante é chamada texto encriptado ou texto criptografado.

Criptografia: Conceito Básico.

- Decriptação é o processo de obter o texto original a partir do texto encriptado, ou seja, o contrário do processo de encriptação.

Criptografia: Conceito Básico.

- Decriptação é o processo de obter o texto original a partir do texto encriptado, ou seja, o contrário do processo de encriptação.

- Passos:
  - O remetente encripta o texto original, obtendo o texto encriptado.
  - O remente envia o texto encriptado ao destinatário.
  - O destinatário recebe o texto encriptado.
  - O destinatário decripta o texto encriptado, obtendo o texto original.

Criptografia

- O que é a Criptografia? Vem de palavras gregas: “**escrita secreta**”.

Criptografia

- O que é a Criptografia? Vem de palavras gregas: “**escrita secreta**”.

- Os profissionais da área distinguem **código** de **cifra**.

Criptografia

- O que é a Criptografia? Vem de palavras gregas: “**escrita secreta**”.

- Os profissionais da área distinguem **código** de **cifra**.

  - **Cifra**: transformação caracter por caracter ou bit a bit, sem considerar a estrutura linguística.

Criptografia

- O que é a Criptografia? Vem de palavras gregas: “**escrita secreta**”.

- Os profissionais da área distinguem **código** de **cifra**.

  - **Cifra**: transformação caracter por caracter ou bit a bit, sem considerar a estrutura linguística.
  - **Código**: substitui uma palavra por outra ou por símbolos (não utilizado).

Criptografia

- O que é a Criptografia? Vem de palavras gregas: “**escrita secreta**”.

- Os profissionais da área distinguem **código** de **cifra**.

  - **Cifra**: transformação caracter por caracter ou bit a bit, sem considerar a estrutura linguística.
  - **Código**: substitui uma palavra por outra ou por símbolos (não utilizado).
- História: Índios Navajos e a guerra EUA vs Japão.

Criptografia

- “Por três anos, onde quer que os marines aterrissassem, os japoneses recebiam uma enxurrada de estranhos ruídos gorgolejantes entremeados com outros sons que lembravam o clamor de um monge tibetano e o som de uma bolsa de água quente sendo esvaziada” (*San Diego Union*, 1945).

Criptografia

- Pessoas que contribuíram com o avanço da criptografia:
  - Militares;
  - Diplomatas;
  - Pessoas que gostam de guardar memórias;
  - Amantes.

Criptografia

- Pessoas que contribuíram com o avanço da criptografia:
  - Militares;
  - Diplomatas;
  - Pessoas que gostam de guardar memórias;
  - Amantes.
- Processo de criptografia era manual (e obviamente, oneroso).

Criptografia

- Pessoas que contribuíram com o avanço da criptografia:
  - Militares;
  - Diplomatas;
  - Pessoas que gostam de guardar memórias;
  - Amantes;
- Processo de criptografia era manual (e obviamente, oneroso).
- E se fosse necessário alterar o método criptográfico? E se o auxiliar de criptografia fosse capturado?

Criptografia

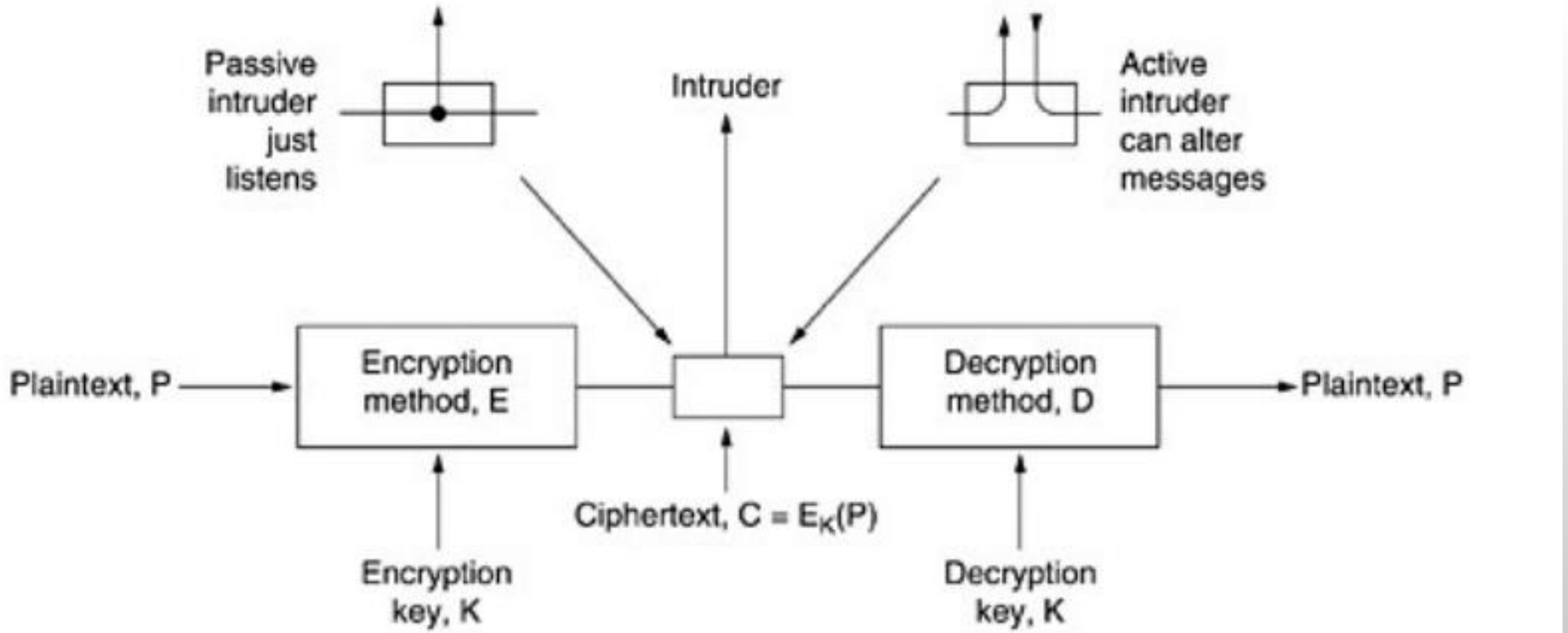


Figura 1: Modelo de criptografia. Fonte: TANENBAUM, 2011.

Criptografia: Chaves

- Exemplos de chaves:
  - Algo que o usuário sabe (senha).
  - Algo que o usuário possui (cartão).
  - Algo que o usuário é (voz, digital, íris, rosto).
- É Necessário gerenciar as chaves.
- É Necessário distribuir as chaves.

Criptografia: Atacantes

- **Atacante Passivo:**
  - Capaz de monitorar toda a transmissão;

Criptografia: Atacantes

- **Atacante Passivo:**
  - Capaz de monitorar toda a transmissão;
  - Pode obter cópia da transmissão;

Criptografia: Atacantes

- **Atacante Passivo:**
  - Capaz de monitorar toda a transmissão;
  - Pode obter cópia da transmissão;
  - Pode reproduzir dados transmitidos;

Criptografia: Atacantes

- **Atacante Passivo:**
  - Capaz de monitorar toda a transmissão;
  - Pode obter cópia da transmissão;
  - Pode reproduzir dados transmitidos;
  - Pode requerer equipamento sofisticado;

Criptografia: Atacantes

- **Atacante Passivo:**
  - Capaz de monitorar toda a transmissão;
  - Pode obter cópia da transmissão;
  - Pode reproduzir dados transmitidos;
  - Pode requerer equipamento sofisticado;
  - Fácil de ser realizado na Internet (hardware barato e software disponível);

Criptografia: Atacantes

- **Atacante Ativo:**
  - Capaz de interceptar e alterar a transmissão;

Criptografia: Atacantes

- **Atacante Ativo:**
  - Capaz de interceptar e alterar a transmissão;
  - Pode ser realizado por Engenharia Social;

Criptografia: Atacantes

- **Atacante Ativo:**
  - Capaz de interceptar e alterar a transmissão;
  - Pode ser realizado por Engenharia Social;
  - Capaz de inserir dados falsos;

Exemplo

- **Exemplo 1: você recebe uma mensagem e-mail, onde o remetente é o gerente ou alguém em nome do departamento de suporte do seu banco. Na mensagem ele diz que o serviço de internet Banking está apresentando algum problema e que tal problema pode ser corrigido se você executar o aplicativo que está anexado à mensagem. A execução deste aplicativo apresenta uma tela análoga àquela que você utiliza para ter acesso a conta bancária, aguardando que você digite sua senha. Na verdade, este aplicativo está preparado para furtar sua senha de acesso a conta bancária e enviá-la para o atacante.**

Exemplo

- **Exemplo 2: você recebe uma mensagem de e-mail, dizendo que seu computador está infectado por um vírus. A mensagem sugere que você instale uma ferramenta disponível em um site da internet, para eliminar o vírus de seu computador. A real função desta ferramenta não é eliminar um vírus, mas sim permitir que alguém tenha acesso ao seu computador e a todos os dados nele armazenados.**

- **Exemplo 3: algum desconhecido liga para a sua casa e diz ser do suporte técnico do seu provedor. Nesta ligação ele diz que sua conexão com a internet está apresentando algum problema e, então, pede sua senha para corrigi-lo. Caso você entregue sua senha, este suposto técnico poderá realizar uma infinidade de atividades maliciosas, utilizando a sua conta de acesso a internet e, portanto, relacionando tais atividades ao seu nome.**

Criptoanálise

- Atacantes fazem uso da criptoanálise, que é a arte ou ciência que trata de desvendar os segredos envolvidos no processo de criptografia.

Criptoanálise

- Atacantes fazem uso da criptoanálise, que é a arte ou ciência que trata de desvendar os segredos envolvidos no processo de criptografia.

- A criptoanálise tenta descobrir:
  - O algoritmo, comparando o texto original com o encriptado.
  - A senha, comparando o texto original com o encriptado e tendo conhecimento do algoritmo.
  - O texto original, tendo conhecimento do texto encriptado, do algoritmo e, talvez, da senha.

Criptologia e Criptoanálise

- Criptologia é a ciência que abrange a criptografia e a criptoanálise.

- Esteganografia é a arte ou ciência que trata das técnicas de ocultar a mensagem .
  - Mensagens subliminares.
  - Tinta invisível.

- A criptologia não engloba a esteganografia.

Conclusão

- Não existe sistema absolutamente seguro.
- Toda criptografia pode ser “quebrada”.
- Complexidade temporal.
- Complexidade econômica.

Criptografia

- Princípio de ***Kerckhoff***:
  - “*Todos os algoritmos devem ser públicos, apenas as chaves são secretas*.”

Criptografia

- Princípio de ***Kerckhoff***:
  - “*Todos os algoritmos devem ser públicos, apenas as chaves são secretas*.”
  - Criptografia simétrica: mesma chave usada na codificação e na decodificação.

Criptografia

- Princípio de ***Kerckhoff***:
  - "*Todos os algoritmos devem ser públicos, apenas as chaves são secretas*."
  - Criptografia simétrica: mesma chave usada na codificação e na decodificação.
  - Criptografia assimétrica: chaves diferentes.

Criptografia

- Técnicas de criptografia:
  - Cifras de substituição (monoalbabética): Cada letra é substituída por outra, criando um ‘disfarce’.

Criptografia

- Técnicas de criptografia:
  - Cifras de substituição (monoalbabética): Cada letra é substituída por outra, criando um ‘disfarce’.
    - *Cifra de César: troca a por D, b por E, c por F, ... e z se torna C*.

Criptografia

- Técnicas de criptografia:

  - Cifras de substituição (monoalbabética): Cada letra é substituída por outra, criando um ‘disfarce’.
    - *Cifra de César: troca a por D, b por E, c por F, ... e z se torna C*.
    - Genérico: o alfabeto do texto cifrado seja deslocado ‘k’ letras. ‘k’ é a chave do método.

Criptografia

- Técnicas de criptografia:
  - Cifras de substituição (monoalbabética): Cada letra é substituída por outra, criando um ‘disfarce’.
    - *Cifra de César: troca a por D, b por E, c por F, ... e z se torna C*.
    - Genérico: o alfabeto do texto cifrado seja deslocado ‘k’ letras. ‘k’ é a chave do método.
  - Cifras de transposição: Letras são reordenadas, e não disfarçadas.

Criptografia

- c = (m + k) mod n
  - c : símbolo cifrado
  - m: símbolo claro
  - k: chave (deslocamento)
  - n: quantidade de símbolos
- Cifra de César

  c = (m + 3) mod 26

```
teste de uma cifra de cesar
whvwh gh xpd fliud gh fhvdu
```

Técnica de Substituição

- Cada símbolo (letra) é substituído por outro:
  - por função matemática;
  - por tabela;

Técnica de Substituição

- Cada símbolo (letra) é substituído por outro:
  - por função matemática;
  - por tabela;

- Chaves: Considerando 26 letras, tem-se 26! possibilidades (cerca de 4.10^{26}):
- 26! = 403.291.461.126.605.635.584.000.000 possibilidades.

Técnica de Substituição

- Cada símbolo (letra) é substituído por outro:
  - por função matemática;
  - por tabela;

- Chaves: Considerando 26 letras, tem-se 26! possibilidades (cerca de 4.10^{26}):
- 26! = 403.291.461.126.605.635.584.000.000 possibilidades.

- Com 1 milisegundo por tentativa, quanto tempo seria necessário?

Técnica de Substituição

- Qual o problema da técnica de substituição direta dos símbolos?

Técnica de Substituição

- Qual o problema da técnica de substituição direta dos símbolos?

- Muito poucas tentativas (só 25)

alzal kl bth jpmyh kl klzsvjhtluav
zkyzk jk asg iolxg jk jkyruigsktzu
yjxyj ij zrf hnkwf ij ijxqthfrjsyt
xiwxi hi yqe gmjve hi hiwpsgeqirxs
whvwh gh xpd fliud gh ghvorfdphqwr
vguvg fg woc ekhtc fg fgunqecogpvq
uftuf ef vnb djgsb ef eftmpdbnfoup
teste de uma cifra de deslocamento

Criptoanálise

- Facilmente realizada analisando-se a frequência dos símbolos (letras, digramas e trigramas).

Criptoanálise

- Facilmente realizada analisando-se a frequência dos símbolos (letras, digramas e trigramas).
- Inglês:
  - E (12%)
  - T, A, O, I, N, S, H, R (de 6 a 9%)
  - D, L (4%)
  - C, U, M, W, F, G, Y, P, B (de 2,8 a 1,5%)
  - V, K, J, X, Q, Z (menos de 1%)

Criptoanálise

- Digramas

  TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA,

  NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF.

- Trigramas

  THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH.

Criptoanálise

YIF QFMZRW QFYV ECFMD ZPCVMRZW NMD

ZVEJB TXCDD UMJN DIFEFMDZ CD MQ

ZKCEYFCJMYR NCW JCSZR EXCHZ UNMXZ NZ

UCDRJ XYYSMRT M EYIFZW DYVZ VYFZ

UMRZ CRW NZ DZJJXZW GCHS MR NMD

HNCMF QCHZ JMXJZW IE JYUCFWD JNZ DIR

Criptoanálise: frequência das letras.

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

Criptoanálise: frequência das letras.

- **Inglês**

  etaoinsrhldcumfpgwybvkxjqz (e: 12 %)

- **Francês**

  etainroshdlcfumgpwbyvkqxjz (e: 13 %)

- **Alemão**

  enirsatdhulgocmbfwkzpvjyxq (e: 18 %)

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

Criptoanálise: frequência das letras.

- **Português**

  aeosirnutdclmpgfbvqhxzjkwy (a: 13 %)

- **a: 13 %**
- **e: 11%**
- **o: 10%**
- **s: 7%**
- **i: 7%**
- **r: 6%**

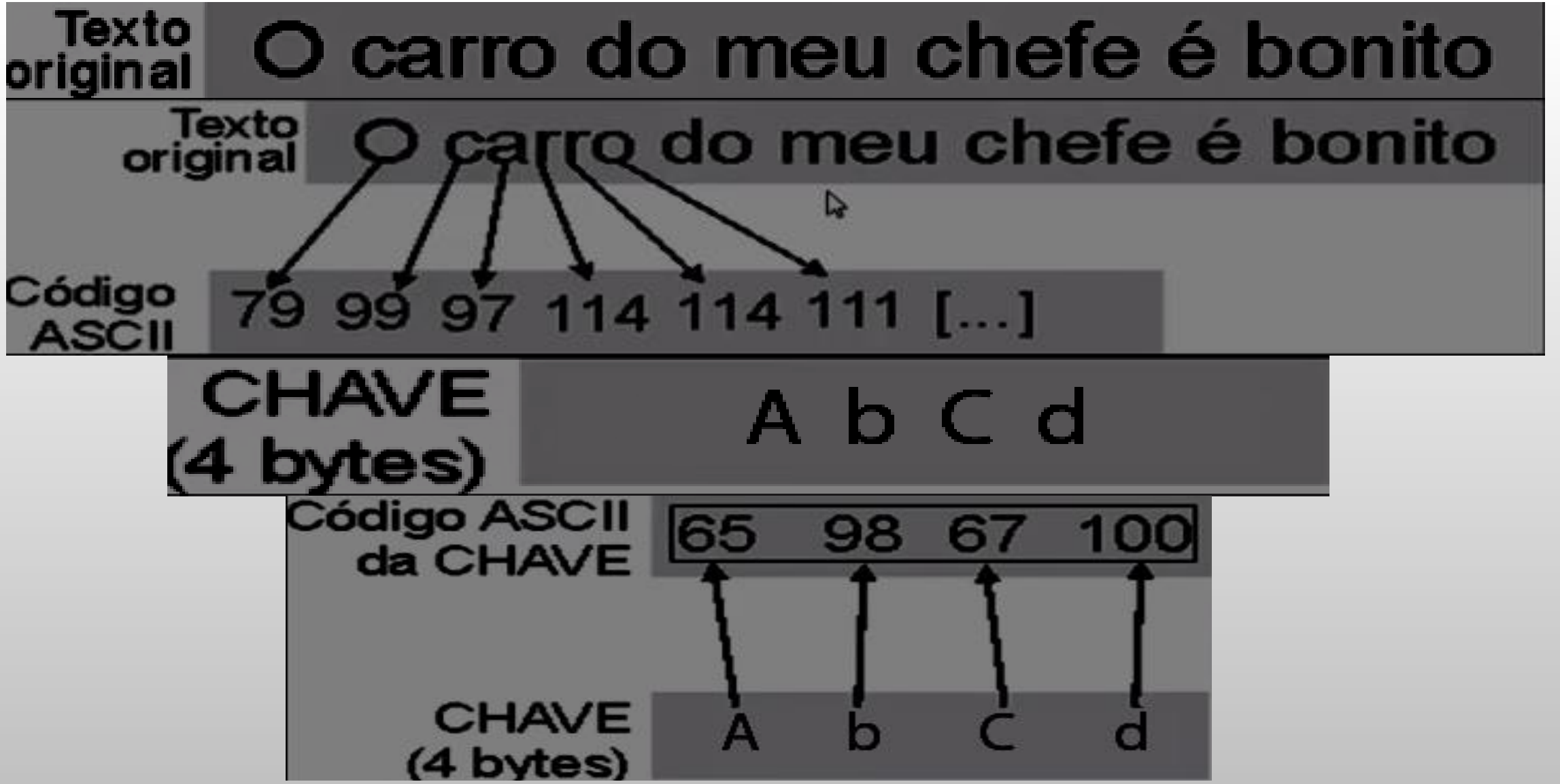
Z	20	W	8	T	2
M	16	E	7	B	1
C	15	X	6	G	1
D	13	I	5	K	1
F	11	U	5	P	1
J	11	V	5	A	0
R	10	H	4	L	0
Y	10	Q	4	O	0
N	9	S	3		

Implementação

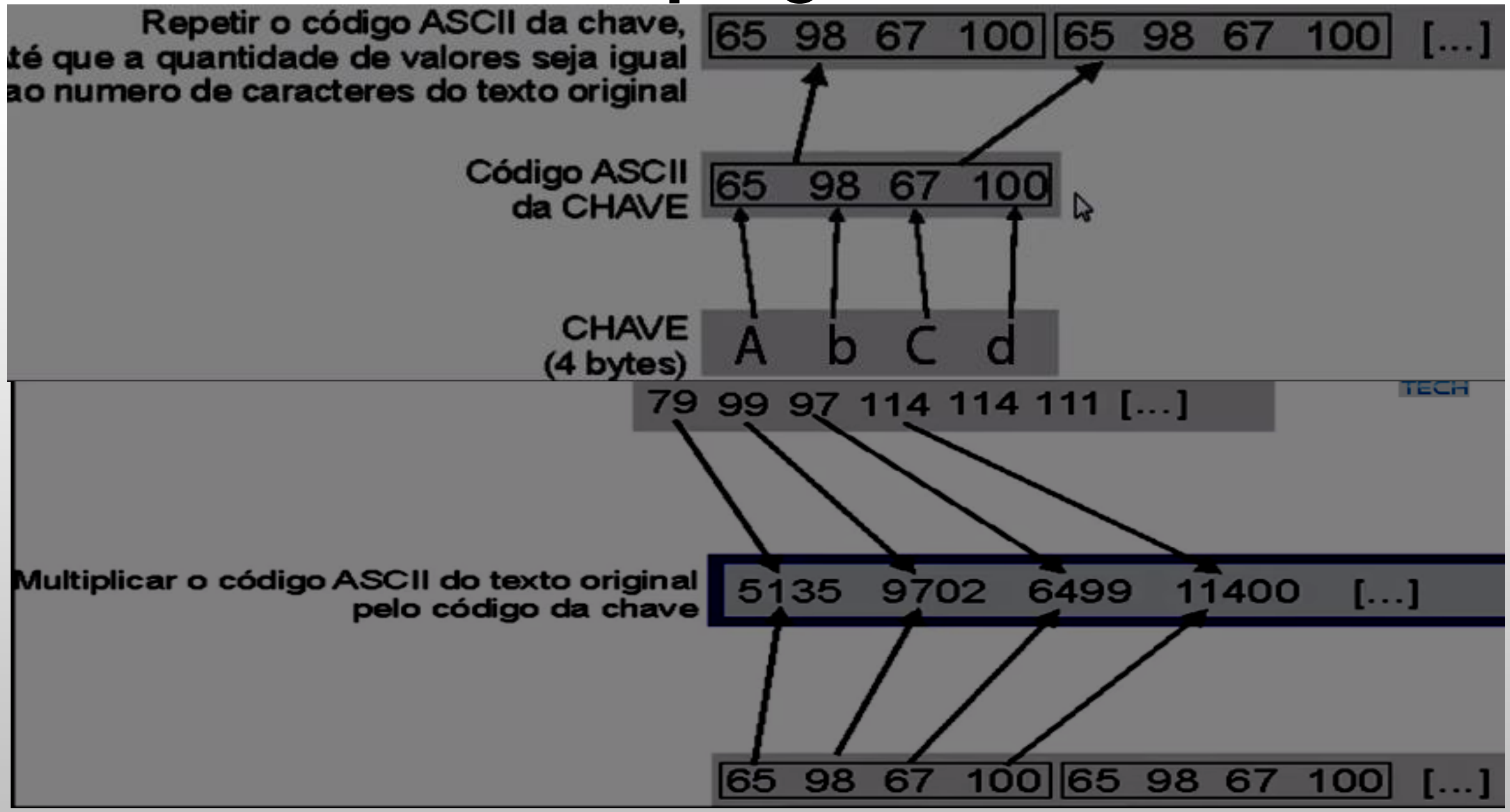
```c
//exibe a tabela ASCII em C
#include <stdio.h>
int main(void) {
    int i;
    for (i=32;i<127;i++) {
        printf("%c = %d \n",i,i);
    }
return 0;
}
```

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	00	Null	32	20	Space	64	40	@	96	60	`
1	01	Start of heading	33	21	!	65	41	A	97	61	a
2	02	Start of text	34	22	"	66	42	B	98	62	b
3	03	End of text	35	23	#	67	43	C	99	63	c
4	04	End of transmit	36	24	$	68	44	D	100	64	d
5	05	Enquiry	37	25	%	69	45	E	101	65	e
6	06	Acknowledge	38	26	&	70	46	F	102	66	f
7	07	Audible bell	39	27	'	71	47	G	103	67	g
8	08	Backspace	40	28	(	72	48	H	104	68	h
9	09	Horizontal tab	41	29	)	73	49	I	105	69	i
10	0A	Line feed	42	2A	*	74	4A	J	106	6A	j
11	0B	Vertical tab	43	2B	+	75	4B	K	107	6B	k
12	0C	Form feed	44	2C	,	76	4C	L	108	6C	l
13	0D	Carriage return	45	2D	-	77	4D	M	109	6D	m
14	0E	Shift out	46	2E	.	78	4E	N	110	6E	n
15	0F	Shift in	47	2F	/	79	4F	O	111	6F	o
16	10	Data link escape	48	30	0	80	50	P	112	70	p
17	11	Device control 1	49	31	1	81	51	Q	113	71	q
18	12	Device control 2	50	32	2	82	52	R	114	72	r
19	13	Device control 3	51	33	3	83	53	S	115	73	s
20	14	Device control 4	52	34	4	84	54	T	116	74	t
21	15	Neg. acknowledge	53	35	5	85	55	U	117	75	u
22	16	Synchronous idle	54	36	6	86	56	V	118	76	v
23	17	End trans. block	55	37	7	87	57	W	119	77	w
24	18	Cancel	56	38	8	88	58	X	120	78	x
25	19	End of medium	57	39	9	89	59	Y	121	79	y
26	1A	Substitution	58	3A	:	90	5A	Z	122	7A	z
27	1B	Escape	59	3B	;	91	5B	[	123	7B	{
28	1C	File separator	60	3C	<	92	5C	\	124	7C	|
29	1D	Group separator	61	3D	=	93	5D	]	125	7D	}
30	1E	Record separator	62	3E	>	94	5E	^	126	7E	~
31	1F	Unit separator	63	3F	?	95	5F	_	127	7F	□

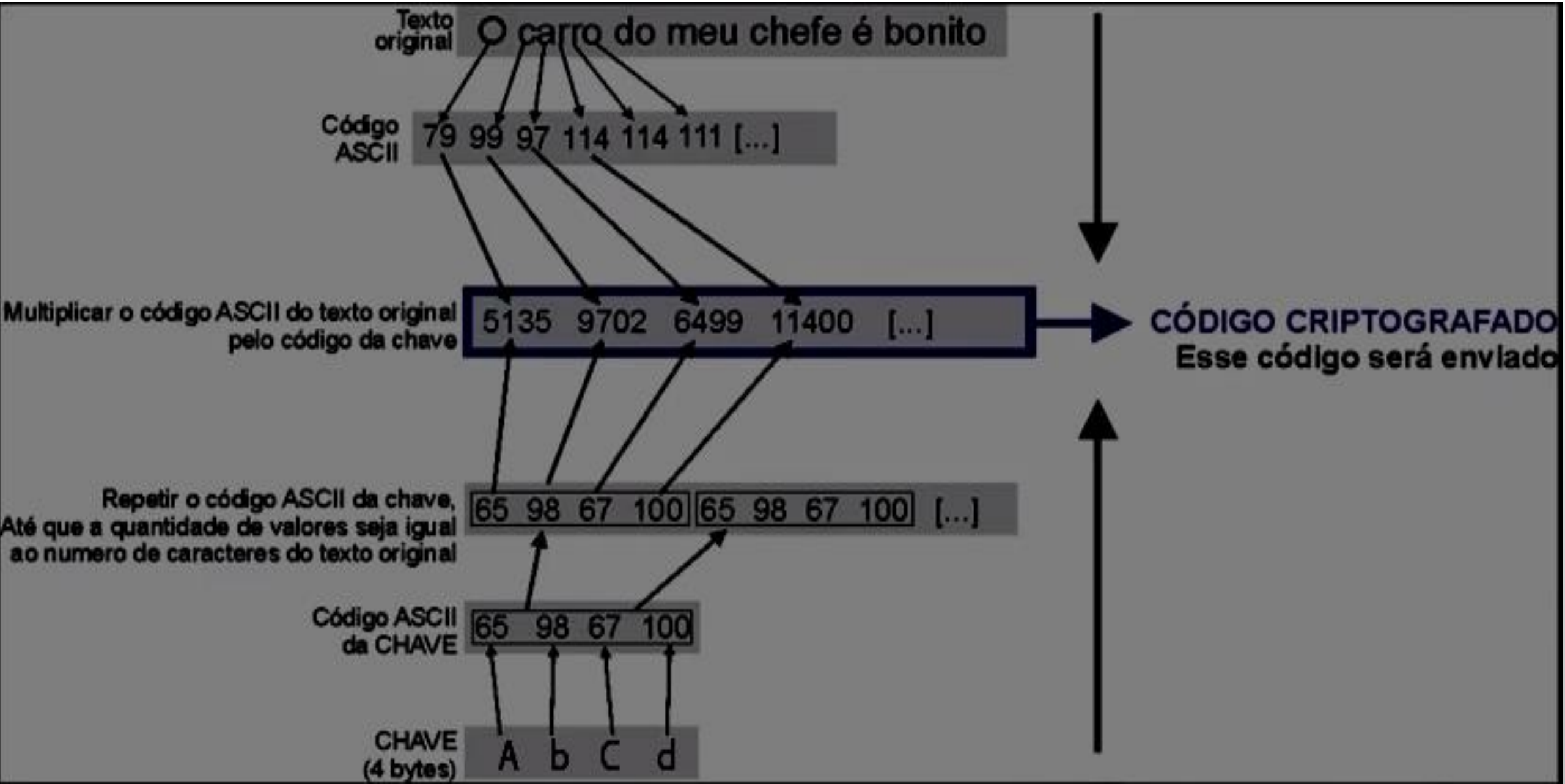
Criptografia



Criptografia



Criptografia



Criptografia

```
97  int main (void){
98      int opcao;
99     do{
100       printf("Criptografia em C\n");
101       printf("\nMenu\n");
102       printf("1 - Criptografar texto\n2 - Descriptografar texto\n3 - Fechar programa\n");
103       printf("Digite sua opcao: ");
104       scanf("%d", &opcao);
105       switch (opcao){
106         case 1:
107           Criptografar("AbCd"); // ativa a função passando como parâmetro a chave desejada
108         break;
109         case 2:
110           Descriptografar("AbCd"); // ativa a função passando como parâmetro a chave desejada
111         break;
112         case 3:
113         continue;
114         break;
115         default:
116         printf("Opcao invalida! Tente novamente.\n\n");
117       }
118    }while(opcao!=3);
119 return 0;
120 }
```

Criptografia

```
5   int Criptografar(char chave[]){
6     // Configuração da Chave para criptografia
7     int tam_chave = strlen(chave);
8     // Vetor de entrada do texto a ser criptografado
9     char texto[100000];
10    // Vetor de encriptação
11    int texto_cript[100000];
12    // Variaveis de controle de chave
13    int valor_chave, aux=0, i;
14    FILE *arquivo;
15    printf("\nDigite o texto a ser criptografado: \n");
16    scanf("\n%[^\n]s",texto);
17    printf("\n\n");
```

```
19  for(i=0; i<strlen(texto); i++){
20    texto_cript[i]=texto[i]; //atribui para TEXTO_CRIPT o ASCII dos caracteres digitados
21  }
22    //printf("\n -- %d -- \n",TEXTO_CRIPT[0]); //mostra o ASCII de TEXTO_CRIPT antes da encriptação
23    //exit(1);
24  while(aux<strlen(texto)){ //vai de 0 até o tamanho do texto incrementando dentro do for
25    for(i=0;i<tam_chave; i++){ //percorre a chave dinamicamente ex.: "aBcd" 0123
26      valor_chave = chave[i]; //pega o ASCII da chave dinamicamente ex.: "a" = 65
27      // multiplica o ASCII de TEXTO_CRIPT pelo ASCII de valor_chave e atribui para TEXTO_CRIPT.
28      //Ex: "a" 65 x 65 =  4225
29      texto_cript[aux] *= valor_chave;
30      aux++;
31    }
32  }
33    //printf("\n -- %d -- \n",TEXTO_CRIPT[0]); //mostra o ASCII de TEXTO_CRIPT depois da encriptação
34    //exit(1);
36      arquivo = fopen("criptografado.txt","w");
37      if(arquivo==NULL){
38        printf("\n\nErro ao criar o arquivo...\n\n");
39      }
40      else{
41        for(i=0; i<strlen(texto); i++){ //percorre o texto digitado pelo usuário
42          //grava em arquivo o texto já cifrado (ASCII)
43          //o espaço é necessário se decifrar depois
44          fprintf(arquivo,"%d ",texto_cript[i]);
45        }
46      }
47      fclose(arquivo);
48
49     return 1;
50  }
```

```c
int Descriptografar(char chave[]){
    // Configuração da chave para criptografia
    int tam_chave = strlen(chave);
    // Vetor de descriptação
    char texto_decript[100000];
    // Variaveis de controle de chave
    int valor, pos_chave = 0, pos_texto = 0;
    FILE *arquivo;
    arquivo = fopen("criptografado.txt","r");
    if(arquivo==NULL){
       printf("\n\nErro ao criar o arquivo...\n\n");
    }
    else{
      while(!feof(arquivo)){ // percorre o arquivo criptografado
        fscanf(arquivo,"%d ",&valor); // le os valores criptografados em ASCII
        // divide o valor pelo ASCII da pela posicao ASCII da chave
        //ex.:"AbcD" onde valor = valor (4265) / chave[0] (65)
        valor /= chave[pos_chave];
        // texto_decript recebe o typecasting de valor, ex.: 65 = "A"
        texto_decript[pos_texto] = (char)valor;
        pos_texto++; // incrementa a posição do vetor texto_decript
        //percore a chave e retorna a posição inicial, ex.: "AbCd" 0123
        if(pos_chave==tam_chave-1){
          pos_chave=0;
        }
        else{
          pos_chave++; //senão, incrementa a chave
        }
      }
      fclose(arquivo);
    }
```

Criptografia

```
85      printf("\nTexto descriptografado: \n");
86      printf("%s",texto_decript); //mostra o vetor contendo o arquivo descriptografado
87      getchar();//somente para dar um pause
88      printf("\n\n");
89      return 1;
90  }
```

Criptografia

Cifra	Autor	Comprimento da chave	Comentários
Blowfish	Bruce Schneier	1 a 448 bits	Velho e lento
DES	IBM	56 bits	Muito fraco para usar agora
IDEA	Massey e Xuejia	128 bits	Bom, mas patenteado
RC4	Ronald Rivest	1 a 2048 bits	Atenção: algumas chaves são fracas
RC5	Ronald Rivest	128 a 256 bits	Bom, mas patenteado
Rijndael	Daemen e Rijmen	128 a 256 bits	Melhor escolha
Serpent	Anderson, Biham, Knudsen	128 a 256 bits	Muito forte
DES triplo	IBM	168 bits	Segunda melhor escolha
Twofish	Bruce Schneier	128 a 256 bits	Muito forte; amplamente utilizado

Figura 2: Algoritmos de chave simétrica comuns. Fonte: TANENBAUM, 2011.

Criptografia

- Segurança Lógica
  - Privacidade
    - » Os dados somente são acessíveis para as pessoas autorizadas.

Criptografia

- Segurança Lógica
  - Privacidade
    - » Os dados somente são acessíveis para as pessoas autorizadas.
  - Autenticidade
    - » Os dados são “assinados” (gerados pelas pessoas autorizadas).

Criptografia

- Segurança Lógica
  - Privacidade
    - » Os dados somente são acessíveis para as pessoas autorizadas.
  - Autenticidade
    - » Os dados são “assinados” (gerados pelas pessoas autorizadas).
  - Integridade
    - » Modificações nos dados (intencionais ou não) são detectadas.

Criptografia

- Segurança Lógica
  - Privacidade
    - » Os dados somente são acessíveis para as pessoas autorizadas.
  - Autenticidade
    - » Os dados são “assinados” (gerados pelas pessoas autorizadas).
  - Integridade
    - » Modificações nos dados (intencionais ou não) são detectadas.
  - Irrefutabilidade
    - » O autor dos dados não pode negar a autoria.

Referências Bibliográficas

- **TANENBAUM, A. S. – Redes de Computadores – 5ª Ed., Editora Campus (Elsevier), 2003.**

Dúvidas?

Professor Luciano Brum
email: lucianobrum18@gmail.com
https://sites.google.com/view/brumluciano