Universidade Federal do Agreste de Pernambuco
Av. Bom Pastor s/n - Boa Vista
55292-270 Garanhuns/PE
☎ +55 (87) 3764-5500
http://www.ufape.edu.br

Bacharelado em Ciência da Computação
CCMP3079 Segurança de Redes de Computadores
Prof. Sérgio Mendonça

Atividade Cap. 02

Para 17/10/2023

Nome completo: Thiago Cavalcanti Silva

Questões retiradas do livro-texto da disciplina.

1. Responda (de forma objetiva) as questões a seguir:

(a) Quais são os elementos essenciais de uma cifra simétrica?

- Texto claro: mensagem original.
- Algoritmo de encriptação: realiza substituições e transformações no texto claro.
- Chave secreta: um valor independente do texto e do algoritmo, que também é entrada para o algoritmo e varia a saída do texto.
  Texto cifrado: mensagem embaralhada produzida pelo algoritmo.
- Algoritmo de decriptação: inverso da encriptação, recebe o texto cifrado e a chave e retorna o texto original.

(b) Quais são as duas funções básicas usadas nos algoritmos de encriptação?

Substituição (mapeamento de cada elemento do texto claro em outro elemento) e transposição (rearranjo dos elementos do texto claro).

(c) Qual é a diferença entre uma cifra de bloco e uma cifra de fluxo?

A de bloco processa a entrada de um bloco de elementos por vez, produzindo a saída para cada um deles. Já a cifra em fluxo, processa os elementos continuamente, retornando a saída de um elemento de cada vez.

(d) Quais são as duas técnicas gerais para atacar uma cifra?

Criptoanálise (explora o algoritmo e talvez características ou amostras de pares de texto claro-texto cifrado) e ataque por força bruta (teste de todas as chaves possíveis).

(e) Quais são os dois problemas com o one-time pad?

Criar grandes quantidades de chaves aleatórias, já que para cada encriptação será usada uma chave diferente. E também a distribuição e proteção da chave, pois a cada mensagem uma chave de mesmo tamanho do texto é necessária para o emissor e receptor.

(f) O que é uma cifra de transposição?

Algum tipo de permutação nas letras do texto claro.

(g) O que é esteganografia?

É uma técnica para esconder a existência da mensagem. Não é exatamente uma forma de encriptar, visto que a criptografia transforma o texto em vez de ocultá-lo.

2. Uma generalização da cifra de César, conhecida como cifra de César afim, tem a seguinte forma: a cada letra de texto claro p, substitua-a pela letra de texto cifrado C:

$$C = E([a, b], p) = (ap + b) \bmod 26$$

um requisito básico de qualquer algoritmo de encriptação é que ele seja um para um. Ou seja, se $p \neq q$, então $E(k, p) \neq E(k, q)$. Caso contrário, a decriptação é impossível, pois mais de um caractere de texto claro é mapeado no mesmo caractere de texto cifrado. A cifra de César afim não é um-para-um para todos os valores de a. Por exemplo, para a = 2 e b = 3, então E([a, b], 0) = E([a, b], 13) = 3.

(a) existem limitações sobre o valor de b? explique por que sim ou por que não.

Não há limitações específicas sobre o valor de 'b' em termos de tornar a cifra um-para-um. O valor de 'b' é um deslocamento e não afeta a reversibilidade da cifra. Entretanto, o valor de 'a' deve ser escolhido de forma que o processo seja inversível (possua um inverso multiplicativo módulo 26).

(b) determine quais valores de a não são permitidos.

Para garantir que a cifra seja "um-para-um" (ou injetiva), é necessário que a função de criptografia seja reversível, ou seja, que seja possível reverter o processo para decifrar a mensagem. Portanto:

'a' e 26 devem ser primos entre si (coprimos): Isso significa que 'a' não pode ter nenhum fator em comum com 26, exceto 1. Se 'a' e 26 não forem coprimos, a cifra não será injetiva porque alguns caracteres do texto claro mapearão para os mesmos caracteres no texto cifrado, tornando a decodificação impossível.

(c) ofereça uma afirmação geral sobre quais valores de a são e não são permitidos. Justifique-a.

'a' deve ser um número ímpar, pois, se 'a' for par, ele será divisível por 2, o que não seria coprimo com 26.

3. (a) Encripte a mensagem "meet me at the usual place at ten rather than eight oclock" usando a cifra de Hill com a chave $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$ **. Mostre seus cálculos e o resultado.**

Como a matriz possui duas linhas, devemos dividir a mensagem em blocos de duas letras.

Blocos: me et me at th eu su al pl ac ea tt en ra th er th an ei gh to cl oc kk

Como o 'k' estava sozinho, repete-se e ao fim da cifragem, remove-o.

Estes valores serão convertidos para números, onde:

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
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	0

Dessa forma, (matriz chave * matriz das letras convertidas em número) mod 26 nos dará o texto cifrado.

me (texto claro): $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} * \begin{bmatrix} 13 \\ 5 \end{bmatrix} = \begin{bmatrix} 9*13+4*5 \\ 5*13+7*5 \end{bmatrix} = \begin{bmatrix} 137 \\ 100 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 7 \\ 22 \end{bmatrix}$ = GV (texto cifrado)

et: $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} * \begin{bmatrix} 5 \\ 20 \end{bmatrix} = \begin{bmatrix} 9*5+4*20 \\ 5*5+7*20 \end{bmatrix} = \begin{bmatrix} 125 \\ 165 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 21 \\ 9 \end{bmatrix}$ = UI

me = GV (como visto anteriormente)

at = $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} * \begin{bmatrix} 1 \\ 20 \end{bmatrix} = \begin{bmatrix} 9*1+4*20 \\ 5*1+7*20 \end{bmatrix} = \begin{bmatrix} 89 \\ 145 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 11 \\ 15 \end{bmatrix}$ = KO

th = $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} * \begin{bmatrix} 20 \\ 8 \end{bmatrix} = \begin{bmatrix} 9*20+4*8 \\ 5*20+7*8 \end{bmatrix} = \begin{bmatrix} 212 \\ 156 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 4 \\ 0 \end{bmatrix}$ = DZ

eu = $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} * \begin{bmatrix} 5 \\ 21 \end{bmatrix} = \begin{bmatrix} 9*5+4*21 \\ 5*5+7*21 \end{bmatrix} = \begin{bmatrix} 129 \\ 172 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 25 \\ 16 \end{bmatrix}$ = YP

su = $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} * \begin{bmatrix} 19 \\ 21 \end{bmatrix} = \begin{bmatrix} 9*19+4*21 \\ 5*19+7*21 \end{bmatrix} = \begin{bmatrix} 255 \\ 242 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 21 \\ 12 \end{bmatrix}$ = UH

al = $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} * \begin{bmatrix} 1 \\ 12 \end{bmatrix} = \begin{bmatrix} 9*1+4*12 \\ 5*1+7*12 \end{bmatrix} = \begin{bmatrix} 57 \\ 89 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 5 \\ 11 \end{bmatrix}$ = EK

pl = $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} * \begin{bmatrix} 16 \\ 12 \end{bmatrix} = \begin{bmatrix} 9*16+4*12 \\ 5*16+7*12 \end{bmatrix} = \begin{bmatrix} 192 \\ 164 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 10 \\ 8 \end{bmatrix}$ = JH

ac = $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} * \begin{bmatrix} 1 \\ 3 \end{bmatrix} = \begin{bmatrix} 9*1+4*3 \\ 5*1+7*3 \end{bmatrix} = \begin{bmatrix} 21 \\ 26 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 21 \\ 0 \end{bmatrix}$ = UZ

ea = $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} * \begin{bmatrix} 5 \\ 1 \end{bmatrix} = \begin{bmatrix} 9*5+4*1 \\ 5*5+7*1 \end{bmatrix} = \begin{bmatrix} 49 \\ 32 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 23 \\ 6 \end{bmatrix}$ = WF

tt = $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} * \begin{bmatrix} 20 \\ 20 \end{bmatrix} = \begin{bmatrix} 9*20+4*20 \\ 5*20+7*20 \end{bmatrix} = \begin{bmatrix} 260 \\ 240 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 0 \\ 6 \end{bmatrix}$ = ZF

en = $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} * \begin{bmatrix} 5 \\ 14 \end{bmatrix} = \begin{bmatrix} 9*5+4*14 \\ 5*5+7*14 \end{bmatrix} = \begin{bmatrix} 101 \\ 123 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 23 \\ 19 \end{bmatrix}$ = WS

ra = $\begin{bmatrix}9 & 4\\5 & 7\end{bmatrix}*\begin{bmatrix}18\\1\end{bmatrix} = \begin{bmatrix}9*18+4*1\\5*18+7*1\end{bmatrix} = \begin{bmatrix}166\\97\end{bmatrix}$ mod 26 = $\begin{bmatrix}10\\19\end{bmatrix}$ = JS

th = DZ (como visto anteriormente)

er = $\begin{bmatrix}9 & 4\\5 & 7\end{bmatrix}*\begin{bmatrix}5\\18\end{bmatrix} = \begin{bmatrix}9*5+4*18\\5*5+7*18\end{bmatrix} = \begin{bmatrix}117\\151\end{bmatrix}$ mod 26 = $\begin{bmatrix}13\\21\end{bmatrix}$ = MU

th = DZ (como visto anteriormente)

an = $\begin{bmatrix}9 & 4\\5 & 7\end{bmatrix}*\begin{bmatrix}1\\14\end{bmatrix} = \begin{bmatrix}9*1+4*14\\5*1+7*14\end{bmatrix} = \begin{bmatrix}65\\103\end{bmatrix}$ mod 26 = $\begin{bmatrix}13\\25\end{bmatrix}$ = MY

ei = $\begin{bmatrix}9 & 4\\5 & 7\end{bmatrix}*\begin{bmatrix}5\\9\end{bmatrix} = \begin{bmatrix}9*5+4*9\\5*5+7*9\end{bmatrix} = \begin{bmatrix}81\\88\end{bmatrix}$ mod 26 = $\begin{bmatrix}3\\10\end{bmatrix}$ = CJ

gh = $\begin{bmatrix}9 & 4\\5 & 7\end{bmatrix}*\begin{bmatrix}7\\8\end{bmatrix} = \begin{bmatrix}9*7+4*8\\5*7+7*8\end{bmatrix} = \begin{bmatrix}95\\91\end{bmatrix}$ mod 26 = $\begin{bmatrix}17\\13\end{bmatrix}$ = QM

to = $\begin{bmatrix}9 & 4\\5 & 7\end{bmatrix}*\begin{bmatrix}20\\15\end{bmatrix} = \begin{bmatrix}9*20+4*15\\5*20+7*15\end{bmatrix} = \begin{bmatrix}240\\205\end{bmatrix}$ mod 26 = $\begin{bmatrix}6\\23\end{bmatrix}$ = FW

cl = $\begin{bmatrix}9 & 4\\5 & 7\end{bmatrix}*\begin{bmatrix}3\\12\end{bmatrix} = \begin{bmatrix}9*3+4*12\\5*3+7*12\end{bmatrix} = \begin{bmatrix}75\\99\end{bmatrix}$ mod 26 = $\begin{bmatrix}23\\21\end{bmatrix}$ = WU

oc = $\begin{bmatrix}9 & 4\\5 & 7\end{bmatrix}*\begin{bmatrix}15\\3\end{bmatrix} = \begin{bmatrix}9*15+4*3\\5*15+7*3\end{bmatrix} = \begin{bmatrix}147\\96\end{bmatrix}$ mod 26 = $\begin{bmatrix}17\\18\end{bmatrix}$ = QR

kk = $\begin{bmatrix}9 & 4\\5 & 7\end{bmatrix}*\begin{bmatrix}11\\11\end{bmatrix} = \begin{bmatrix}9*11+4*11\\5*11+7*11\end{bmatrix} = \begin{bmatrix}143\\132\end{bmatrix}$ mod 26 = $\begin{bmatrix}13\\2\end{bmatrix}$ = MB

Portanto, a mensagem cifrada é:

GVUIGVKODZYPUHEKJHUZWFZFWSJSDZMUDZMYCJQMFWWUQRMB

(b) Mostre os cálculos para a decriptação correspondente do texto cifrado a fim de recuperar o texto claro original.

Para decriptar, precisamos do inverso multiplicativo modular do determinante (obtido pelo determinante da chave) e da matriz inversa da chave.

Determinante da chave = detChave = (7 * 9) – (-4 * -5) = 63 – 20 = 43

Inverso modular = (detChave * i) mod 26 = 1

(43 * i) mod 26 = 1

i = 23, pois (43 * 23) mod 26 = 989 mod 26 = 1

Chave = $\begin{bmatrix}9 & 4\\5 & 7\end{bmatrix}$, logo, Chave^{-1} = $\begin{bmatrix}7 & -4\\-5 & 9\end{bmatrix}$.

Com essas informações podemos gerar a chave decodificadora através do seguinte cálculo:

Chave decodificadora = i * Chave^{-1} mod 26 = 23 * $\begin{bmatrix}7 & -4\\-5 & 9\end{bmatrix}$ mod 26 = $\begin{bmatrix}161 & -92\\-115 & 207\end{bmatrix}$ mod 26 = $\begin{bmatrix}5 & 12\\15 & 25\end{bmatrix}$.

Agora, basta multiplicar a chave decodificadora pela representação numérica das letras, calculando o módulo de 26, para obter a mensagem original.

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
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	0

GV (texto cifrado): $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} * \begin{bmatrix} 7 \\ 22 \end{bmatrix} = \begin{bmatrix} 5*7+12*22 \\ 15*7+25*22 \end{bmatrix} = \begin{bmatrix} 299 \\ 655 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 13 \\ 5 \end{bmatrix}$ = me (texto claro)

UI = $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} * \begin{bmatrix} 21 \\ 9 \end{bmatrix} = \begin{bmatrix} 5*21+12*9 \\ 15*21+25*9 \end{bmatrix} = \begin{bmatrix} 213 \\ 540 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 5 \\ 20 \end{bmatrix}$ = et

GV = me (como visto anteriormente)

KO = $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} * \begin{bmatrix} 11 \\ 15 \end{bmatrix} = \begin{bmatrix} 5*11+12*15 \\ 15*11+25*15 \end{bmatrix} = \begin{bmatrix} 235 \\ 540 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 1 \\ 20 \end{bmatrix}$ = at

DZ = $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} * \begin{bmatrix} 4 \\ 0 \end{bmatrix} = \begin{bmatrix} 5*4+12*0 \\ 15*4+25*0 \end{bmatrix} = \begin{bmatrix} 20 \\ 60 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 20 \\ 8 \end{bmatrix}$ = th

YP = $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} * \begin{bmatrix} 25 \\ 16 \end{bmatrix} = \begin{bmatrix} 5*25+12*16 \\ 15*25+25*16 \end{bmatrix} = \begin{bmatrix} 317 \\ 775 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 5 \\ 21 \end{bmatrix}$ = eu

UH = $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} * \begin{bmatrix} 21 \\ 8 \end{bmatrix} = \begin{bmatrix} 5*21+12*8 \\ 15*21+25*8 \end{bmatrix} = \begin{bmatrix} 201 \\ 515 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 19 \\ 21 \end{bmatrix}$ = su

EK = $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} * \begin{bmatrix} 5 \\ 11 \end{bmatrix} = \begin{bmatrix} 5*5+12*11 \\ 15*5+25*11 \end{bmatrix} = \begin{bmatrix} 157 \\ 350 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 1 \\ 12 \end{bmatrix}$ = al

JH = $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} * \begin{bmatrix} 10 \\ 8 \end{bmatrix} = \begin{bmatrix} 5*10+12*8 \\ 15*10+25*8 \end{bmatrix} = \begin{bmatrix} 146 \\ 350 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 116 \\ 12 \end{bmatrix}$ = pl

UZ = $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} * \begin{bmatrix} 21 \\ 0 \end{bmatrix} = \begin{bmatrix} 5*21+12*0 \\ 15*21+25*0 \end{bmatrix} = \begin{bmatrix} 105 \\ 315 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 1 \\ 3 \end{bmatrix}$ = ac

WF = $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} * \begin{bmatrix} 23 \\ 6 \end{bmatrix} = \begin{bmatrix} 5*23+12*6 \\ 15*23+25*6 \end{bmatrix} = \begin{bmatrix} 187 \\ 495 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 5 \\ 1 \end{bmatrix}$ = ea

ZF = $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} * \begin{bmatrix} 0 \\ 6 \end{bmatrix} = \begin{bmatrix} 5*0+12*6 \\ 15*0+25*6 \end{bmatrix} = \begin{bmatrix} 72 \\ 150 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 20 \\ 20 \end{bmatrix}$ = tt

WS = $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} * \begin{bmatrix} 23 \\ 19 \end{bmatrix} = \begin{bmatrix} 5*23+12*19 \\ 15*23+25*19 \end{bmatrix} = \begin{bmatrix} 343 \\ 820 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 5 \\ 14 \end{bmatrix}$ = em

JS = $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} * \begin{bmatrix} 10 \\ 19 \end{bmatrix} = \begin{bmatrix} 5*10+12*19 \\ 15*10+25*19 \end{bmatrix} = \begin{bmatrix} 278 \\ 625 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 18 \\ 1 \end{bmatrix}$ = ra

DZ = th (como visto anteriormente)

MU = $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} * \begin{bmatrix} 13 \\ 21 \end{bmatrix} = \begin{bmatrix} 5*13+12*21 \\ 15*13+25*21 \end{bmatrix} = \begin{bmatrix} 317 \\ 720 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 5 \\ 18 \end{bmatrix}$ = er

DZ = th (como visto anteriormente)

MY = $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} * \begin{bmatrix} 13 \\ 25 \end{bmatrix} = \begin{bmatrix} 5*13+12*25 \\ 15*13+25*25 \end{bmatrix} = \begin{bmatrix} 365 \\ 820 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 1 \\ 14 \end{bmatrix}$ = na

CJ = $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} * \begin{bmatrix} 3 \\ 10 \end{bmatrix} = \begin{bmatrix} 5*3+12*10 \\ 15*3+25*10 \end{bmatrix} = \begin{bmatrix} 135 \\ 295 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 5 \\ 9 \end{bmatrix}$ = ei

QM = $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} * \begin{bmatrix} 17 \\ 13 \end{bmatrix} = \begin{bmatrix} 5*17+12*13 \\ 15*17+25*13 \end{bmatrix} = \begin{bmatrix} 241 \\ 580 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 7 \\ 8 \end{bmatrix}$ = gh

FW = $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} * \begin{bmatrix} 6 \\ 23 \end{bmatrix} = \begin{bmatrix} 5*6+12*23 \\ 15*6+25*23 \end{bmatrix} = \begin{bmatrix} 306 \\ 665 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 20 \\ 15 \end{bmatrix}$ = to

WU = $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} * \begin{bmatrix} 23 \\ 21 \end{bmatrix} = \begin{bmatrix} 5*23+12*21 \\ 15*23+25*21 \end{bmatrix} = \begin{bmatrix} 367 \\ 395 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 3 \\ 12 \end{bmatrix}$ = cl

QR = $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} * \begin{bmatrix} 17 \\ 18 \end{bmatrix} = \begin{bmatrix} 5*17+12*18 \\ 15*17+25*18 \end{bmatrix} = \begin{bmatrix} 301 \\ 705 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 15 \\ 3 \end{bmatrix}$ = oc

MB = $\begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} * \begin{bmatrix} 13 \\ 2 \end{bmatrix} = \begin{bmatrix} 5*13+12*2 \\ 15*13+25*2 \end{bmatrix} = \begin{bmatrix} 89 \\ 245 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 11 \\ 11 \end{bmatrix}$ = kk

Agora basta remover o último k, pois foi duplicado já que a mensagem era de tamanho ímpar.

4. Elabore um programa que possa encriptar e decriptar usando a cifra de César geral, também conhecida como cifra aditiva.

Notebook do SageMath disponibilizado no arquivo “Exercícios do capítulo 2.ipynb”.

5. Elabore um programa que possa realizar um ataque de frequência de letra em uma cifra aditiva sem intervenção humana. Seu software deverá produzir textos claros possíveis em ordem aproximada de probabilidade. Seria bom se a sua interface com o usuário permitisse que ele especificasse “mostre os 10 textos claros mais prováveis”.

Notebook do SageMath disponibilizado no arquivo “Exercícios do capítulo 2.ipynb”.

6. Crie um software que possa encriptar e decriptar usando uma cifra de Hill 2 × 2.

Notebook do SageMath disponibilizado no arquivo “Exercícios do capítulo 2.ipynb”.

Livro-texto da disciplina:

STALLINGS, William. Criptografia e segurança de redes. Princípios e práticas, Ed. 6. 2014.