

Avaliação 1 – Ciber Segurança

Professor: Fábio Oliveira Guimarães

Questão 1 - O texto em português a seguir foi cifrado usando o cifrador de César. Encontre o texto original e a chave usada para cifrá-lo; explique seu procedimento.

Kjqne fvzjqj vzt ywfsxkjjw t vzt

xfgj j fuwjsij t vzt jsxnsf.

Htwf Htwfqnsf.

Para facilitar seu trabalho, a tabela a seguir traz a frequência de caracteres típica de textos na língua portuguesa:

letra	freq%	letra	freq%	letra	freq%	letra	freq%	letra	freq%
A	14,6	B	1,04	C	3,88	D	4,99	E	12,6
F	1,02	G	1,30	H	1,28	I	6,18	J	0,40
K	0,02	L	2,78	M	4,74	N	5,05	O	10,7
P	2,52	Q	1,20	R	6,53	S	7,81	T	4,34
U	4,63	V	1,67	W	0,01	X	0,21	Y	0,01
Z	0,47								

Questão 2 - Cifre o texto 01101100 utilizando uma Cifra de Feistel. Como função de encriptação F, utilize a operação AND. Para gerar as subchaves K_i , realize um deslocamento circular a esquerda no texto original. No total, realize duas rodadas do algoritmo para gerar o texto cifrado.

Questão 3 - Realize uma substituição de caixa-S utilizando como entrada a palavra 011010 e a caixa S1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13