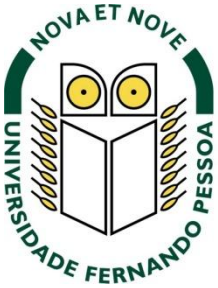

Universidade Fernando Pessoa
www.ufp.pt

Segurança em Aplicações Web

Criptoanálise

Ana Beatriz Gomes, 2014

Criptoanálise – Exercício

Considere a seguinte mensagem cifrada, resultado da aplicação de um algoritmo de cifragem de deslocamento simples num determinado texto:

VZ KPNYHTHZ L AYPNYHTHZ ZHV JVUQBUAVZ KL KBHZ VB AYLZ SLAYHZ ZLNBPKHZ L XBL JVUZAPABLT ZBI WHSHCYHZ L XBL MHGLT WHYAL KL BTH WHSHCYH L JVT YLJBYZV H VIALUJHV KVZ KPNYHTHZ L AYPNYHTHZ JVUZLNBPTVZ ALY BTH PKLPH KHZ CPGPUOHUJHZ XBL ZL LUJVUAYHT UBT KLALYTPUHKV PKPVTH VB ZLQH XBHPZ HZ SLAYHZ XBL HWHYLJLT THPZ CLGLZ HJVZZPHKHZ H VBAYHZ SLAYHZ KLUAYV KL BTH KLALYTPUHKH WHSHCYH VB ALEAV

Criptoanálise – Exercício

Letras mais frequentes no texto cifrado

Letras mais frequentes na Língua Portuguesa

	A	E	O	S
H				
L				
Z				
Y				

Criptoanálise – Exercício

Digramas mais frequentes na Língua Portuguesa

Digramas mais frequentes no texto cifrado

	DE	RA	OS	ES	AS	DO
HZ						
YH						
AY						
TH						
ZL						
LA						
KL						

Criptoanálise – Exercício

Chave:

Texto original: