Session 3: 11:50
Room URS 2s21

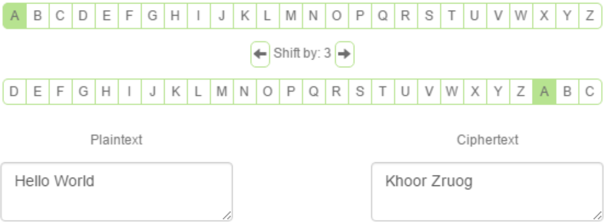
Public Key Cryptography Learning Resource

Matthew Palmer

BSc in Computer Science with Industrial Year

ABSTRACT

Cryptography is a complex subject that is increasingly relied upon by the modern world. Meaning that those involved in the creation of secure digital environments require more knowledge than ever before. Novel ways to bypass cryptography systems can be missed entirely due to these complexities, requiring a simple way to learn and understand the concepts and protocols behind it. By analyzing the e-learning sites that provide cryptography modules and looking to improve upon these modules through the use of the latest technology, a host of new interactive tools were created to explore how cryptography works. Surveying a range of individuals showed that the improved tools provided an enhanced method of learning whilst also highlighting other areas in which the tools could be improved further, helping fulfil the aim of the project to create an affective learning resource for Public Key Cryptography.

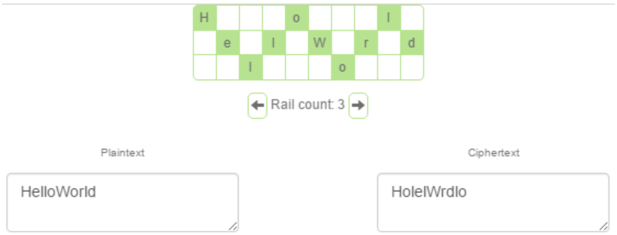


A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Plaintext: Hello World

Ciphertext: Khoor Zruog

Figure 1. Caesar Cipher interactive cipher created for the learning website



H				o				l	
	e		l		W		r		d
		l				o			

Plaintext: HelloWorld

Ciphertext: HolelWrdlo

Figure 2. Rail Fence interactive cipher created for the learning website

M Palmer, Public Key Cryptography Learning Resource, *Proc. 15th School Conf. for Annual Research Projects*, V F Ruiz (Ed), pp. xx–yy, University of Reading, 24th May 2016.

Proc. School Conf. for Annual Research Projects
School of Systems Engineering
University of Reading
©2016 SCARP