Exercise 1:

A:

De ciphertekst:

yyrroxilpveckdmpwvtvpeebtwtuoxiejuenn

Samen met de sleutel:

Franklin

De sleutel “Franklin” wordt onder de ciphertekst geplaatst:

Franklinfranklinfranklinfranklinfrank

Na het uitlezen van de Vigenère tabel ontstaat deze zin:

Three may keep a secret if two of them are dead.

B:

De plaintekst wordt:

warispeacefreedomisslaveryignoranceisstrength

De key wordt (evenveel letters als de plaintekst):

therewasnowayofshuttingitoffcompletelyhemove

Hierdoor onstaat de ciphertekst:

phvzwlespsbrcsigtclltnbmkmnlpcdpygxmdqavqbbxk

C:

Als eenmaal bekend is met welke paar woorden de key start is het gemakkelijk te achterhalen hoe de rest van de key verloopt omdat de key uit een boek komt.

Exercise 2:

ASCII	u	s	e	_	j	u	s	t
plain	1110101	1110011	1100101	0100000	1101010	1110101	1110011	1110100
pad	1010011	0011000	0111101	0011000	0100000	0000001	1001011	0110010
XOR	0100110	1101011	1011000	1001010	1001010	1110100	0111000	1000110
ASCII	&	k	X	8	J	t	8	F
_	o	n	e	_	t	i	m	e
0100000	1101111	1101110	1100101	0100000	1110100	1101001	1101001	1100101
0001010	0001000	0000000	0110010	1101100	1000010	1000010	1000010	0001100
0101010	1100111	1101110	1010111	1001100	0110110	0101011	1101101	1101001
*	g	n	W	L	6	+	m	i

Exercise 3:

A:

State	x0	x1	x2	x3	x4	x5	x6	x7	output

-1	0	1	1	1	1	0	1	1	0
0	1	1	1	1	0	1	1	0	1
1	1	1	1	0	1	1	0	0	1
2	1	1	0	1	1	0	0	0	1
3	1	0	1	1	0	0	0	1	1
4	0	1	1	0	0	0	1	0	0
5	1	1	0	0	0	1	0	0	1

B:

State	x0	x1	x2	x3	x4	x5	x6	x7	
-1	0	1	1	1	1	0	1	1	
-2	1	0	1	1	1	1	0	1	
-3	1	1	0	1	1	1	1	0	
-4	1	1	1	0	1	1	1	1	
-5	0	1	1	1	0	1	1	1	

C:

Ciphertekst:

0100

Output van vier shifts (zie opdracht 3A):

0111

Plaintekst:

0011