Assignment 4

Exercise 9

The first entry of the table get popped in ervery step.

Basestruct	Pre-Terminal	Probability	Pivot Value
$D_1L_3S_2D_1$	$4L_3\$\$4$	0.188	0
$L_3D_1S_1$	$L_34!$	0.097	0

Basestruct	Pre-Terminal	Probability	Pivot Value
$L_3D_1S_1$	$L_34!$	0.097	0
$D_1L_3S_2D_1$	$4L_3**4$	0.081	2
$D_1L_3S_2D_1$	$4L_3\$\$5$	0.063	3
$D_1L_3S_2D_1$	$5L_3\$\$4$	0.063	0

Basestruct	Pre-Terminal	Probability	Pivot Value
$D_1L_3S_2D_1$	$4L_3**4$	0.081	2
$D_1L_3S_2D_1$	$4L_3\$\$5$	0.063	3
$D_1L_3S_2D_1$	$5L\$\$4$	0.063	0
$L_3D_1S_1$	$L_34\%$	0.045	2
$L_3D_1S_1$	$L_35!$	0.033	1

Basestruct	Pre-Terminal	Probability	Pivot Value
$D_1L_3S_2D_1$	$4L_3\$\$5$	0.063	3
$D_1L_3S_2D_1$	$5L\$\$4$	0.063	0
$L_3D_1S_1$	$L_34\%$	0.045	2
$L_3D_1S_1$	$L_35!$	0.033	1
$D_1L_3S_2D_1$	$4L_3**5$	0.027	3

Basestruct	Pre-Terminal	Probability	Pivot Value
$D_1L_3S_2D_1$	$5L_3\$\$4$	0.063	0
$D_1L_3S_2D_1$	$4L_3\$\$6$	0.063	3
$L_3D_1S_1$	$L_34\%$	0.045	2
$L_3D_1S_1$	$L_35!$	0.033	1
$D_1L_3S_2D_1$	$4L_3**5$	0.025	3

Exercise 11

11.1

Userinformations are stored in the following form in a master.passwd file in 'OpenBSD':

$$name : password : uid : gid : class : change : expire : gecos : homedir : shell$$

The password is hashed via Bcrypt. The format of the bcrypt is the following :

$$\${brcypt\,version}\${costparamter}\${salt : 22\,chars, base64}\{hash : 31\,chars, base64\}$$

11.2

For cracking the passwords we wrote a small python script.

It basically generated all possible combination of 4 numbers between 0-9 and hashed them. Then we compared it with the hashed passwords from the given file. For finding the english word we download a big dictionary (354984 word). For this word we generated hashes and compared the hashes again. For the sake of saving time we parrelised everything so the running time was acceptable(~30 minutes). For more details see the source code.

For finding the password for the user rand we made a background check of Randall Munroe and found an interessting comic ;)

The found password were as follow:

[('alice', '2053'), ('bob', '2184'), ('carol', '7251'), ('dave', '9559'), ('charlie', 'demisemiquaver'), ('rand', 'correct horse battery staple')]