Seth Lunders

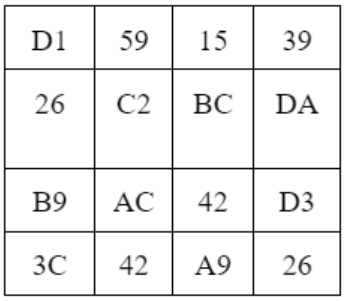
Professor Song

CS336 HW#3

24 September 2021

1.
    a. 26*26*26*26 = 456,976 seconds, or 5.29 days
    b. 26+26+26+26 = 104 seconds max, if it's always the last letter checked. I believe on average it should take half that time, so I would expect the average time to be 52 seconds.
2. Per-subject access control list is used. Deleting is inconvenient because changes must be made to control lists of all subjects who had access to the object. A less costly alternative would be to leave the object permissions intact and the pointers to the object, but to delete all its content. So even though people could still 'access' it, there isn't anything useful to access.
3. I dual boot Windows and Linux on my laptop, so I decided to check Linux. The password is stored as a hash in the /etc/shadow file. Opening this file and viewing the hash also shows you the hash used. In my case, it is 6 which means SHA-512 encryption. When I try to login, the system hashes my attempted password and compares it to the hash in the /etc/shadow file.

4. AES Algorithm

a. 

D1	59	15	39
26	C2	BC	DA
B9	AC	42	D3
3C	42	A9	26

Use the S-Box to begin the AES encryption process

3E	CB	59	12
F7	25	65	57
56	91	2C	66
EB	2C	D3	F7

b. XOR the round key:

36	24	A3	82
00	00	00	00
AA	B2	30	57
11	43	1D	C1

$\oplus$

3E	CB	59	12
F7	25	65	57
56	91	2C	66
EB	2C	D3	F7

Result:

08	EF	FA	90
F7	25	65	57
FC	23	1C	31
FA	6F	CE	36

5 and 6: Answers and work shown on next pages: