Seth Lunders

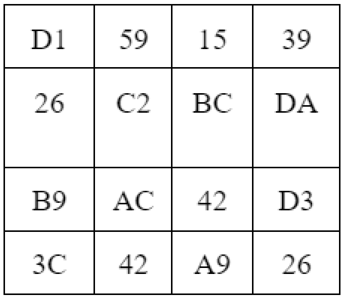
Professor Song

CS336 HW#3

24 September 2021

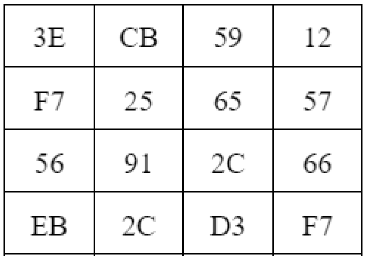
1.
    a. 26*26*26*26 = 456,976 seconds, or 5.29 days
    b. 26+26+26+26 = 104 seconds max, if it's always the last letter checked. I believe on average it should take half that time, so I would expect the average time to be 52 seconds.
2. Per-subject access control list is used. Deleting is inconvenient 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



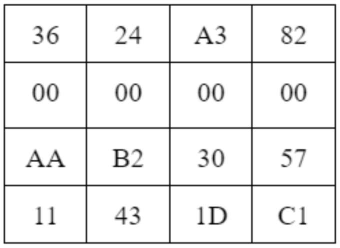
D1	59	15	39
26	C2	BC	DA
B9	AC	42	D3
3C	42	A9	26

a. Use the S-Box to begin the AES encryption process



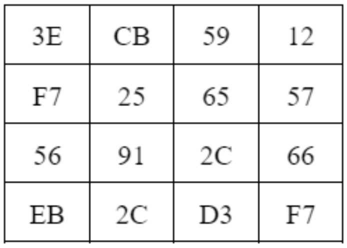
3E	CB	59	12
F7	25	65	57
56	91	2C	66
EB	2C	D3	F7

b. XOR the round key:



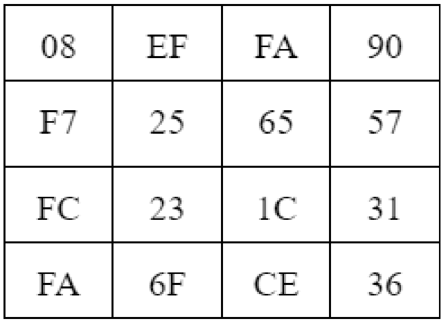
36	24	A3	82
00	00	00	00
AA	B2	30	57
11	43	1D	C1

⊕



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:

Seth Landis

Diffie-Hellman key exchange

5. Common prime $n=11$ User A: pub $Y_a = 9$

Primitive root $g = 2$ User B: pub $Y_b = 3$

a) What is A's private key?

$Y_a = g^{X_a} \bmod n$

$9 = 2^{X_a} \bmod 11$

1	2	3	4	5	6	7	8
2	4	8	16	32	64	128	256
2	4	8	5	10	9	7	3

$X_a = 6$

b) B's private key $3 = 2^{X_b} \bmod 11$ $X_b = 8$

$X = 2^6 \bmod 11$ $Y = 2^8 \bmod 11$

$9 = 64 \bmod 11$ $3 = 256 \bmod 11$

$3^6 \bmod 11$ $9^8 \bmod 11$

$3 = 3$

$\boxed{K=3}$

RSA

Seth Luders

$p^e \bmod n = \text{encrypt} \qquad (p^e)^d \bmod n = p$

6)

Ciphertext $C = 10$

User's public key is $e = 5$, $n = 35$

$\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$

$\varphi(n) = (5-1)(7-1)$

$= 4 \cdot 6$

$= 24$

$e = 2 \Rightarrow \gcd(e, 24) = 2$

$e = 3 \Rightarrow \gcd(e, 24) = 3$

$e = 4 \qquad = 4$

$e = 5 \Rightarrow \gcd(e, 24) = 1$ ✓

$d^* e \bmod \varphi(n) = 1$

$d = (1 + k^* \varphi(n))/e$

$d = (1 + k \cdot 24)/5$

$K = 0 = 1/5$

$K = 1 = 5$ ✓

$d = 5.$

```
 4
 35     35
  8      7
---    ---
 40     35
240    210
280    245
```

Reminder: $C = 10$, $e = 5$, $n = 35$

$P = C^d \bmod n$

$P = 10^5 \bmod 35$

$P = 100000 \bmod 35$

$\boxed{P = 5}$

```
     2857 r5
35 | 100000
      70
     -------
      300
      280
     -------
       200
       175
        250
```