Benjamín Aage B. Birgisson

Exercise 10.1.1:

(a)

1. Information disclosure.
   Enables an attacker to gain valuable information about a system.
   For example: Intruder could gain valuable information about user A or user B when the user is writing on the terminal line and thereby intercept data communication.

2. Information modification or destruction.
   An unauthorized modification of data or programs, which may be performed by a legitimate user or by an intruder, or a deliberate / accidental deletion of information or damage to hardware.
   For example: Intruder could insert arbitrary messages into the communication stream of user B.

3. Unauthorized use of services.
   A circumvention of the system's user authentication services to make unauthorized use of a service.
   For example: As the intruder has access to intercept all communication of both user A and user B, the intruder could therefore try and guess A's or B's password and thereby access all unauthorized use of services.

4. Denial of service.
   Preventing a legitimate user from employing a service in a timely manner.
   For example: None, as I do not see how it would be possible with the information and access that the intruder has in these particular cases.

Exercise 10.2.2:

(a)

- without salt
  m encryptions are needed, followed by m*n comparisons.
  → Encryption = h us
  → Looking up and comparing a value = c us
  Time : h * m + c * n

- with salt

  m*n encryptions are necessary, followed by m*n*n comparisons.
  → Encryption = 10*h us
  → Looking up and comparing a value = c us
  Time : 10 * h * m + c * n * n

(b)

- without salt

  Time : h * m + c * n
  Time = 1 * 100,000 + 0.01 * 1000
  = 100,000 + 10
  = 100,010 us

- with salt

  Time : 10 * h * m + c * n * n
  Time = 10 * 1 * 100,000 + 0.01 * 1000 * 1000
  = 1,000,000 + 10,000
  = 1,010,000 us

Exercise 10.2.3:

(a)

"Cat" in ASCII = 67 97 116

H("Cat")	=	67^3 mod 100, 97^3 mod 100, 116^3 mod 100
	=	63 73 96
H(H("Cat"))	=	63^3 mod 100, 73^3 mod 100, 96^3 mod 100
	=	47 17 36
H(H(H("Cat")))	=	47^3 mod 100, 17^3 mod 100, 36^3 mod 100
	=	23 13 56
H(H(H(H("Cat"))))	=	23^3 mod 100, 13^3 mod 100, 56^3 mod 100
	=	67 97 16
H(H(H(H(H("Cat")))))	=	67^3 mod 100, 97^3 mod 100, 16^3 mod 100
	=	63 73 96 (same as the first)

Exercise 10.2.5:

(a)

9 / 1000 = 0.009 = 0.9% < 1%
So 9 out of 1000 imposter fingerprints.
Therefore, the threshold value of n must be at 0.3.

(b)

If less than 1% of genuine attempts are rejected, then 99% (or more) attempts are accepted.
So, only 9 out of the 1000 genuine attempts are rejected, so the threshold value of n would be at 0.2.

(c)

With no genuine attempts rejected, the threshold value of n would be at 0.0 and it would lead to all imposter attempts would be accepted as well.

Exercise 10.3.1:

(a)

With a set of access lists (D, rights), the number of entries necessary would be three – that is one for the single domain covering 95% of objects, one for the three domains (on average) accessing the 4% of objects, and one for all of the rest of domains covering accessibility of the last 1% of objects.

(b)

You would need 200 entries if the matrix is implemented as a set of capability lists (O, rights), as there are 200 domains in the access matrix.

Exercise 10.3.2:

(a)

Access lists

O1	O2	O3
(D1,orwx)	(D2,orwx)	(D1,rx)
(D2,rw)	(D3,x)	(D4,owrx)
(D4,r)	(D4,r)	

(b)

	Capability lists
D1	(O1,orwx), (O3,rx)
D2	(O1,rw), (O2,orwx)
D3	(O2,x)
D4	(O1,r), (O2,r), (O3,owrx)

(c)

- read O_2 → D_2
- execute O_2 → D_2 and D_3

Exercise 10.4.1:

(a)

(b)

Key consists of 3 ASCII characters, and there are 128 characters in ASCII code.
The time for one encryption is 0.01 us.
So, to try all possible keys on a ciphertext of 30 characters would take:

30^{3*2*1} * 0.01us = 7290000us (* 128 characters = 933120000 us?)

(c)

1 day = 24 hours = 1440 minutes = 86400 seconds
86,400 seconds * 30 days = 2,592,000 seconds per month

30^x * 0.01 us = 2,592,000 seconds
x = 7 (?)

Exercise 10.4.2:

(a)

The decryption applies the function $P = C^5 \bmod 35$ to every digit in the stream and then interprets each pair of numbers as the hexadecimal ASCII code:
Decrypting the first pair, (9,4), results is $9^5 \bmod 35 = 4$ and $4^5 \bmod 35 = 9$, respectively.

49 is the hexadecimal code for the ASCII character "I".

$P = C^5 \bmod 35$

(9,4)	→	(9^5 mod 35) (4^5 mod 35)	→	(4) (9)	→	49
(32,0)	→	(32^5 mod 35) (0^5 mod 35)	→	(2) (0)	→	20
(6,15)	→	(6^5 mod 35) (15^5 mod 35)	→	(6) (15)	→	6F
(7,7)	→	(7^5 mod 35) (7^5 mod 35)	→	(7) (7)	→	77
(6,10)	→	(6^5 mod 35) (10^5 mod 35)	→	(6) (5)	→	65
(32,0)	→	(32^5 mod 35) (0^5 mod 35)	→	(2) (0)	→	20
(7,4)	→	(7^5 mod 35) (4^5 mod 35)	→	(7) (9)	→	79
(6,15)	→	(6^5 mod 35) (15^5 mod 35)	→	(6) (15)	→	6F
(7,10)	→	(7^5 mod 35) (10^5 mod 35)	→	(7) (5)	→	75

(32,0)	→	(32^5 mod 35) (0^5 mod 35)	→	(2) (0)	→	20
(32,9)	→	(32^5 mod 35) (9^5 mod 35)	→	(2) (4)	→	24
(33,1)	→	(33^5 mod 35) (1^5 mod 35)	→	(3) (1)	→	31
(32,17)	→	(32^5 mod 35) (17^5 mod 35)	→	(2) (12)	→	2C
(33,0)	→	(33^5 mod 35) (0^5 mod 35)	→	(3) (0)	→	30
(33,0)	→	(33^5 mod 35) (0^5 mod 35)	→	(3) (0)	→	30
(33,0)	→	(33^5 mod 35) (0^5 mod 35)	→	(3) (0)	→	30
(32,17)	→	(32^5 mod 35) (17^5 mod 35)	→	(2) (12)	→	2C
(33,0)	→	(33^5 mod 35) (0^5 mod 35)	→	(3) (0)	→	30
(33,0)	→	(33^5 mod 35) (0^5 mod 35)	→	(3) (0)	→	30
(33,0)	→	(33^5 mod 35) (0^5 mod 35)	→	(3) (0)	→	30
(32,1)	→	(32^5 mod 5) (1^5 mod 35)	→	(2) (1)	→	21

Decryption: 49206F776520796F752024312C3030302C30303021

(b)

Exercise 10.4.3:

(a)

Yes, the message received is genuine and could only be repudiated by the sender if he/she holds the digital signature to undeniably link the string to the producer and guarantees that the document has not been altered in any way.