

INF140-Introduction to Cybersecurity, Mandatory Assignment 1

Overview of Cybersecurity (20 pts)

Question 1:

Explain the meanings of the following security attributes in computer systems: confidentiality, integrity, authenticity, accountability, availability.

For each attribute, describe an example in which the attribute of an asset in an information system can be potentially violated and the security techniques/controls that can be used to protect the attribute of the asset.

Confidentiality: Confidentiality deals with the private and confidential information such as unauthorized entities cannot access the system.

- Violation:

It's common to use password protection to keep your unwanted individuals away, however there is a lot of different approaches an attacker can take to gain access anyways. E.g. the use of software to guess the password, and unfortunately it's common to use weak passwords and use it to multiple accounts, which makes it way easier for the unauthorized individual.

- Protection:

To protect against these attacks you can choose a much stronger password, or even better, the use of two factor authentication. Some examples on this is biometrical confirmations or the use of your phone for confirmation.

Integrity: Integrity assures that information isn't tampered by the program it's using or along the destination of the information.

- Violation:

Even if most of the information traveling through the internet is encrypted, there exists exploits that can give an unauthorized person the ability to modify information between sender and receiver.

- Protection

To protect yourself from integrity attacks the sender and receiver must be assure that

their software doesn't contain any form for malware and be connected to a secure network.

Authenticity: Authenticity is about being able to confirm and verify the user is who they say they are, and that they are being trustworthy.

- Violation:

A party within a transaction may have left behind by an unauthorized entity.

- Protection:

Have a second form for authentication to confirm the authenticity.

Accountability: Accountability is the term involving the tracing and identification of every entity connected to the internet. The reason why, is in the instance of a security breach, the breach needs to be traced back to the origin of the attacker.

- Violation:

The use of shared user IDs and passwords render accountability useless.

- Protection:

Ensure that every user has its own identity on the network.

Availability: Ensuring minimal delay and reliable access to and use of information, such as authorized users aren't denied.

- Violation:

Overwhelming security can cause antivirus and firewalls to interfere with the availability of the system

- Protection:

Making sure only necessary protection software are installed and wont interfere with the main system that's trying to run.

Question 2:

Consider a company whose operations are housed in two buildings on the same property:

- *one building is headquarters*
- *the other building contains network and computer services.*

The property is physically protected by a fence around the perimeter. The only entrance to the property is through a guarded front gate. The local networks are split between the Headquarters' LAN and the Network Services' LAN. Internet users connect to the Web server through a firewall. Dial-up users get access to a particular server on the Network Services' LAN.

Read Section 1.5 in Chapter 1 and develop an attack tree in which

- *the root node represents disclosure of proprietary secrets;*
- *there are at least 10 nodes;*
- *attacks include physical, social engineering, and technical attacks;*
- *both AND and OR nodes may be contained.*

Disclosure of proprietary secrets:

- Snaking into the property
 - Using tools to get past the fence
 - Scouting the area and gathering guard information
 - Help from man on the inside
 - Smuggling
 - Patrol routes, and potential cameras
 - Parachuting onto the roof
 - Entering through the sewers
- Identity theft
 - Copying/Stealing RFID from authorized worker
 - Taking the place of a look alike
 - Surgery to change biometrics
- Social engineering
 - Vishing
 - Phishing

- Tailgating
- Software attack
 - Exploiting weakness in the firewall
 - Trojan horse

Cryptographic Tools (60 pts)

Question 3:

Encrypt the following sentence

Cybersecurity is an evolving process and is determined by the weakest link

by

- *the Vigenère cipher with key $k = \text{human}$; and*
- *the column transposition cipher 34681752*

The Vigenère Cipher:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

- Plain text: cybersecurity is an evolving process and is determined by the weakest link
- Key: human

- Cipher: jsneezyouepnk if hh qvbspunt wlacrmz mnq pm pegllyialx ny goy ienryet yphw

The Column transposition cipher:

- Plain text: cybersecurity is an evolving process and is determined by the weakest link
- Key: 34681752

Using the column transposition cipher method:

3	4	6	8	1	7	5	2
c	y	b	e	r	s	e	c
u	r	i	t	y	i	s	a
n	e	v	o	l	v	i	n
g	p	r	o	c	e	s	s
a	n	d	i	s	d	e	t
e	r	m	i	n	e	d	b
y	t	h	e	w	e	a	k
e	s	t	l	i	n	k	

- Line 1: rylcsnwi
 - Line 2: canstbk
 - Line 3: cungaeye
 - Line 4: yrepnrts
 - Line 5: esisedak
 - Line 6: bivrdmht
 - Line 7: sivedeen
 - Line 8: etooiiel
- Cipher: rylcsnwicanstbkcungaeyeyrepnrtsesisedakbivrdmhtsivedeenetooiiel

Question 4:

This problem introduces a hash function similar in spirit to SHA-1 that operates on letters instead of binary data. It is called the toy tetragraph hash (TTH). Given a message consisting of a sequence of letters, TTH produces a hash value consisting of four letters. First, TTH divides the message into blocks of 16 letters, ignoring spaces, punctuation, and capitalization. If the message length is not divisible by 16, it is padded out with nulls. A four-number running total is maintained that starts out with the value (0, 0, 0, 0); this is input to a function, known

as a compression function, for processing the first block. The compression function consists of two rounds:

Round 1. Get the next block of text and arrange it as a row-wise 4×4 block of text and convert it to numbers ($A = 0, B = 1 \dots$), for example, for the block *ABCDEFGH IJKLMNOP*, we have

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

Then, add each column mod 26 and add the result to the running total, mod 26. In this example, the running total is (24,2,6,10).

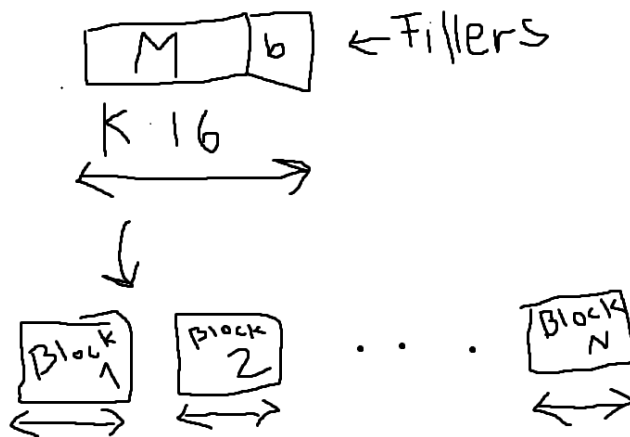
Round 2. Using the matrix from round 1, rotate the first row left by 1, second row left by 2, third row left by 3, and reverse the order of the fourth row. In our example

B	C	D	A
G	H	E	F
L	I	J	K
P	O	N	M

1	2	3	0
6	7	4	5
11	8	9	10
15	14	13	12

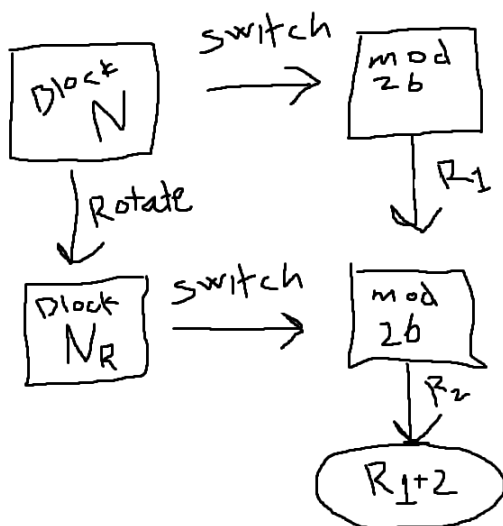
Now, add each column modulo 26 and add the result to the running total. The new running total is (5,7,9,11). This running total is now the input into the first round of the compression function for the next block of text. After the final block is processed, convert the final running total to letters. For example, if the message is *ABCDEFGH IJKLMNOP*, then the hash is *FHJL*.

1. Draw figures of the overall TTH logic and the compression function logic (5 pts)



$M + b$ must be divisible by 16.

Each block is 16 letters long. For each block we have:



We switch the letters out with number in block N and mod them by 26. We get the running number R_1 . Then we rotate the block N and then switch out the new letter in block N_R with number to get R_2 . $R_1 + R_2$ will give us the new running number for block N. This procedure is repeated by every block and added together to a final hash value.

2. Calculate the hash function for the 48-letter message "I leave twenty million dollars to my friendly cousin Bill." (7 pts)

We split up the 48-letter message into 3 blocks:

Block 1

i	l	e	a
v	e	t	w
e	n	t	y
m	i	l	l

->

8	11	4	0
21	4	19	22
4	13	19	24
12	8	11	11

->

11	4	0	8
19	22	21	4
24	4	13	19
11	11	8	12

mod 26:

v

mod 26:

v

A = [19 10 1 5] + [13 15 16 17]

Block 2

i	o	n	d
o	l	l	a
r	s	t	o
m	y	f	r

->

8	14	13	3
14	11	11	0
17	18	19	14
12	24	5	17

->

14	13	3	8
11	0	14	11
14	17	18	19
17	5	24	12

mod 26:

v

mod 26:

v

B = [25 15 22 8] + [4 9 7 24]

Block 3

i	e	n	d
l	y	c	o
u	s	i	n
b	i	l	l

->

8	4	13	3
11	24	2	14
20	18	8	13
1	8	11	11

->

4	13	3	8
2	14	11	24
13	20	18	8
11	11	8	1

mod 26:

v

mod 26:

v

C = [14 2 8 15] + [4 6 14 15]

We add all the sums of the blocks together and get our final running number

$$A + B + C = [1, 5, 16, 6]$$

Which gives us hash: **B, F, Q, G**

3. To demonstrate the weakness of TTH, find a 48-letter block that produces the same hash as that just derived. (8 pts)

With the 48-letter message ayhgdaaaaaaaaaa aaaaaaaaaaaaaaaaaa aaaaaaaaaaaaaaaaaa.

Block 1

a	y	h	g
d	a	a	a
a	a	a	a
a	a	a	a

->

0	24	7	6
3	0	0	0
0	0	0	0
0	0	0	0

->

24	7	6	0
0	0	3	0
0	0	0	0
0	0	0	0

mod 26:

v

mod 26:

v

A = [3 24 7 6] + [24 7 9 0]

Block 2

a	a	a	a
a	a	a	a
a	a	a	a
a	a	a	a

->

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

->

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

mod 26:

v

mod 26:

v

B = [0 0 0 0] + [0 0 0 0]

Block 3

a	a	a	a
a	a	a	a
a	a	a	a
a	a	a	a

->

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

->

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

mod 26:

v

mod 26:

v

C = [0 0 0 0] + [0 0 0 0]

$$A + B + C = [1, 5, 16, 6] \Rightarrow \mathbf{B, F, Q, G}$$

As you can see, we still get the same hash as the message in question 4.2

Question 5:

(1) Perform encryption and decryption using the RSA algorithm, as in the slides, for the following examples (10 pts: 2 pts for each):

1. $p = 13; q = 31, e = 19; M = 2$
2. $p = 11; q = 31, e = 7; M = 4$
3. $p = 3; q = 17, e = 5; M = 5$

$$4. \quad p = 5; q = 17, e = 7; M = 6$$

$$5. \quad p = 7; q = 17, e = 29; M = 3$$

1. **Encryption:**

$$C = M^e \bmod n = 2^{19} \bmod 403 = 388$$

$$n = p * q = 13 * 31 = 403$$

Decryption:

$$M = C^d \bmod n = 388^{19} \bmod 403 = 2$$

$$\varphi(n) = (p-1) * (q-1) = 12 * 30 = 360$$

$$d = e^{-1} \bmod \varphi(n) = 1/19 \bmod 360 = 19$$

2. **Encryption:**

$$C = M^e \bmod n = 4^7 \bmod 341 = 16$$

$$n = p * q = 11 * 31 = 341$$

Decryption:

$$M = C^d \bmod n = 16^{43} \bmod 341 = 4$$

$$\varphi(n) = (p-1) * (q-1) = 10 * 30 = 300$$

$$d = e^{-1} \bmod \varphi(n) = 1/7 \bmod 300 = 43$$

3. **Encryption:**

$$C = M^e \bmod n = 5^5 \bmod 51 = 14$$

$$n = p * q = 3 * 17 = 51$$

Decryption:

$$M = C^d \bmod n = 14^{13} \bmod 51 = 5$$

$$\varphi(n) = (p-1) * (q-1) = 2 * 16 = 32$$

$$d = e^{-1} \bmod \varphi(n) = 1/5 \bmod 32 = 13$$

4. **Encryption:**

$$C = M^e \bmod n = 6^7 \bmod 85 = 31$$

$$n = p * q = 5 * 17 = 85$$

Decryption:

$$M = C^d \bmod n = 31^{23} \bmod 85 = 6$$

$$\varphi(n) = (p-1) * (q-1) = 4 * 16 = 64$$

$$d = e^{-1} \bmod \varphi(n) = 1/7 \bmod 64 = 55$$

5. Encryption:

$$C = M^e \bmod n = 3^{53} \bmod 119 = 12$$

$$n = p * q = 7 * 17 = 119$$

Decryption:

$$M = C^d \bmod n = 12^{19} \bmod 119 = 3$$

$$\phi(n) = (p-1) * (q-1) = 6 * 16 = 96$$

$$d = e^{-1} \bmod \phi(n) = 1/29 \bmod 96 = 53$$

(2) In a public-key system using RSA, suppose you intercepted a cipher text $C=61$ sent to a user whose public key is $e=11$, $n=91$. What is the plaintext M ? Explain the steps that you find the plaintext. (5 pts)

We use the formula:

$$M = C^d \bmod n$$

$$d = e^{-1} \bmod \phi(n)$$

$$\phi(n) = (p-1) * (q-1)$$

We must find d , and therefore we need to find p and q

Test every prime (p) starting from the bottom: $n/p = 91/p \Rightarrow p = 7$

Finding q : $91/7 = 13$

$$\phi(n) = (p-1) * (q-1) = 6 * 12 = 72$$

$$d = e^{-1} \bmod \phi(n) = 1/11 \bmod 72 = 59$$

$$M = C^d \bmod n = 61^{59} \bmod 91 = 3$$

Question 6:

Consider a Diffie-Hellman scheme with a common prime $q=23$ and a generator $g=5$.

1. Alice has public key $PUBA=10$, what is Alice's private key $PRIA$? (2 pts)

Function:

$$g^{PRIA} \bmod q = PUBA$$

$$5^{PRIA} \bmod 23 = 10$$

Testing every number of $PRIA$ starting with 1:

$$PRIA = 3$$

2. Bob has public key $PUBB=8$, what is the shared secret key K ? (3 pts)

$$K = \text{PUBB}^{\text{PRIA}} \bmod q = 8^3 \bmod 23 = 6$$

Question 7:

After taking some courses on cryptography, Alice and Bob decide to try it out in their communication. They agree that they will use Vigenere cipher for data encryption/decryption, and RSA for sharing secret key, where the key of Vigenere cipher only uses letters A,B,...,J and letters in a key are encoded as digits 0,1,...,9 for RSA. For instance, the key BAJ is 109.

Alice chooses a RSA public key $(n, e) = (341, 7)$. Bob uses the Vigenere cipher to encrypt a sentence and encrypt the Vigenere key by Alice's RSA public key. Then Bob sends the following message to Alice:

61, Tfsghgs zq tadnov zuws gutoiosgoz dflqsk vik fffgmopf. Ov jy uuxkdz. Answer the following questions:

- What is the Vigenere key used by Bob? (6 pts)

Using decryption of RSA to find their shared Vigenere key:

$$M = C^d \bmod n$$

$$n = p * q$$

Finding p and q

$$341 = 11 * 31$$

$$\varphi(n) = (p-1) * (q-1) = 10 * 30 = 300$$

$$d = e^{-1} \pmod{\varphi(n)} = (1/7) \pmod{300} = 43$$

$$M = C^d \bmod n = 61^{43} \bmod 341 = 216$$

- What is the original message from Bob? (4 pts)

Converting the letters to number and subtracting the key from the numbers and converting them back to letters:

[illegible]

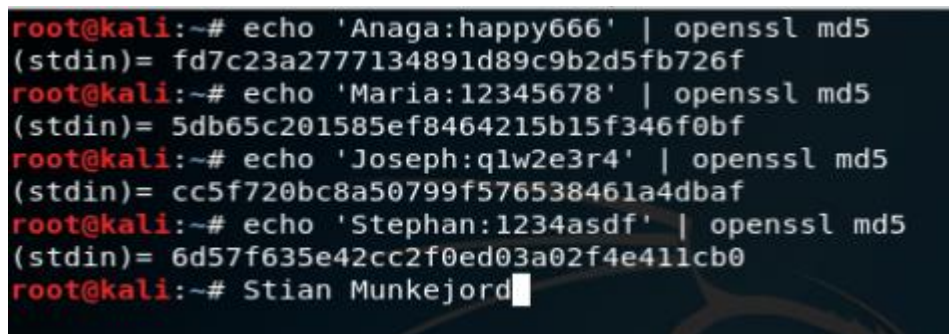
Question 8:

Suppose a computer system stores users' password by simply calculating the MD5 of "user name:password" and restricts password to chosen from lower case letters and digits with max. length 8.

1. Use OpenSSL to calculate the following user names and passwords (4 pts):

- Anaga:happy666*
- Maria:12345678*
- Joseph: q1w2e3r4*
- Stephan:1234asdf*

and take a screenshot of your commands and results. (NB: Pay attention the option of echo in your commands)



```
root@kali:~# echo 'Anaga:happy666' | openssl md5
(stdin)= fd7c23a2777134891d89c9b2d5fb726f
root@kali:~# echo 'Maria:12345678' | openssl md5
(stdin)= 5db65c201585ef8464215b15f346f0bf
root@kali:~# echo 'Joseph:q1w2e3r4' | openssl md5
(stdin)= cc5f720bc8a50799f576538461a4dbaf
root@kali:~# echo 'Stephan:1234asdf' | openssl md5
(stdin)= 6d57f635e42cc2f0ed03a02f4e411cb0
root@kali:~# Stian Munkejord
```

2. Use OpenSSL command to test the speed of MD5 in your computer. Suppose Nikolay is a user in the system, use the speed information to estimate how long do you need to crack Nikolay's password in the following cases (8 pts):

- Nikolay chooses a password of length 4 with all digits*
- Nikolay chooses a password of length 8 with all digits*
- Nikolay chooses a password of length 8 with all lower-case letters*
- Nikolay chooses a password of length 8 with each position either a digit or a lower-case letter*

In your answer, you should clearly give your estimation of the MD5 speed in your computer. For each case, you should show the steps how your estimation is obtained.

```

root@kali:~# time echo '1234' | openssl md5
(stdin)= e7df7cd2ca07f4f1ab415d457a6e1c13

real    0m0.009s
user    0m0.008s
sys     0m0.000s
root@kali:~# time echo '12345678' | openssl md5
(stdin)= 23cdc18507b52418db7740cbb5543e54

real    0m0.009s
user    0m0.009s
sys     0m0.000s
root@kali:~# time echo 'asdfghjk' | openssl md5
(stdin)= 2fd72c203f74e90c987247ded3b9f417

real    0m0.007s
user    0m0.008s
sys     0m0.000s
root@kali:~# time echo 'e3e3e3e3' | openssl md5
(stdin)= 3ab362825e151531cdf92847a101b47d

real    0m0.007s
user    0m0.004s
sys     0m0.004s
root@kali:~# stian munkejord

```

Function (Brute force) = Real time * max. possible combinations

- 4-digit password: $F(b) = 0.009 \text{ sec} * 10^4 = 90 \text{ sec}$
- 8-digit password: $F(b) = 0.009 \text{ sec} * 10^8 = 250 \text{ hours}$
- 8 lc-letter password: $F(b) = 0.007 \text{ sec} * 26^8 \approx 46 \text{ years}$
- 8-character password with lc-letters or numbers: $F(b) = 0.009 \text{ sec} * 36^8 \approx 805 \text{ years}$

Question 9:

The inclusion of the salt in the UNIX password scheme increases the difficulty of guessing by a factor of 4096. But the salt is stored in plaintext in the same entry as the corresponding hashed password. Therefore, those two characters are known to the attacker and need not be guessed. Why is it asserted that the salt increases security? (4 pts)

Whit salt two users can have the same password without sharing the same hash value. Salt will also increase the difficulty of dictionary attacks.

Question 10:

The following is an entry in the password file in a Linux system, which a root user can access (4 pts):

```

root:$6$Q8uKtWWm/dptau2a$E184j/HJuiuw2lsUT7yuBvTh3FioWj5KKUvPQT
/1OJT4rtBACAm4NlEFV4n4x6ndTN3wD9A5uHOjEQQ/JJqN./:18142:0:99999:7:::

```

Search on the Internet and explain each segment in the above password.

1. In the beginning root: Is the username of the account

2. \$6\$ is the algorithm which is SHA-512
3. *Q8uKtWWm/dptau2a\$E184j/HJuiuw2lsUT7yuBvTh3FioWj5KKUvPQT*
/1OJT4rtBACAm4NlEFV4n4x6ndTN3wD9A5uHOjEQQ/JJqN./: is the password itself
on the encrypted method.
4. *18142*: number of days which the password was changed.
5. *0*: This specifies the days in which the password change is allowed.
6. *99999*: specify the duration of the password's validity.
7. *7*: The number of days before password change warning displays.
8. *:::* The three last fields is
 - Days before the account is closed
 - Days before the password expires
 - Last one is usually unused