UNIVERSITETET I BERGEN

KANDIDAT

227

PRØVE

INF140 0 Introduksjon til datasikkerhet

Emnekode	INF140
Vurderingsform	Skriftlig eksamen
Starttid	25.11.2020 08:00
Sluttid	25.11.2020 11:00
Sensurfrist	--
PDF opprettet	02.10.2022 11:17

Section 1

Oppgave	Oppgavetype
i	Informasjon eller ressurser
i	Informasjon eller ressurser
i	Informasjon eller ressurser

Section 2 - Multiple-choice Questions (single correct alternative)

Oppgave	Oppgavetype
1	Flervalg
2	Flervalg
3	Flervalg
4	Flervalg
5	Flervalg
6	Flervalg
7	Flervalg
8	Flervalg
9	Flervalg
10	Flervalg
11	Flervalg
12	Flervalg
13	Flervalg
14	Flervalg
15	Flervalg
16	Flervalg
17	Flervalg
18	Flervalg
19	Flervalg
20	Flervalg

Section 3 - Multiple-Response Questions (multiple correct alternatives)

Oppgave	Oppgavetype
21	Flervalg (flere svar)
22	Flervalg (flere svar)
23	Flervalg (flere svar)

24	Flervalg (flere svar)
25	Flervalg (flere svar)
26	Flervalg (flere svar)
27	Flervalg (flere svar)
28	Flervalg (flere svar)
29	Flervalg (flere svar)
30	Flervalg (flere svar)

Section 4

Oppgave	Oppgavetype
31	Fyll inn tekst
32	Fyll inn tekst
33	Fyll inn tekst

Section 5

Oppgave	Oppgavetype
34	Langsvar
35	Langsvar

Section 6

Oppgave	Oppgavetype
36	Tekstfelt

1 What kind of cybersecurity risks can be minimized by using a Virtual Private Network (VPN)?

Select one alternative:

- De-anonymization by network operators
- Key-logging
- Use of insecure Wi-Fi networks
- Phishing attacks

Maks poeng: 0.5

2 WannaCry is a type of _____

Select one alternative:

- Spyware
- Ransomware
- Riskware
- Adware

Maks poeng: 0.5

3 A/An _____ in a system is a potential danger that a vulnerability will be exploited

Select one alternative:

- attack
- vulnerability
- exploit
- threat

Maks poeng: 0.5

4 The operating system access controls comprise which type of control in the following?

Select one alternative:

- Physical controls
- Administrative controls
- Logical controls
- Compensating controls

Maks poeng: 0.5

5 A _____ provides malicious users remote control over the targeted computer

Select one alternative:

- Backdoor Trojan
- DDoS-Trojan
- Trojan-Downloader
- Trojan-Banker

Maks poeng: 0.5

6 Which of the following is a type of transport layer DoS?

Select one alternative:

- HTTP flooding
- DNS query flooding
- SYN flooding
- Ping flooding

Maks poeng: 0.5

7 Which of the following attacks uses DNS-based vulnerabilities to divert the traffic of the Internet ?

Select one alternative:

- DNS cracking
- Domain link poisoning
- DNS poisoning
- DNS re-routing

Maks poeng: 0.5

8 Which of the following attacks pretends to associate a certain IP address to its MAC address in a LAN?

Select one alternative:

- DNS spoofing
- DHCP spoofing
- SYN spoofing
- ARP spoofing

Maks poeng: 0.5

9 Which of the following is an example of physical hacking?

Select one alternative:

- DDoS (Distributed Denial of Service) attack
- Inserting malware loaded USB to a system
- Remote Unauthorised access
- SQL Injection on SQL vulnerable site

Maks poeng: 0.5

10 Hackers who help in finding bugs and vulnerabilities in a system & do not intend to crack a system are known as

Select one alternative:

- Black Hat Hackers
- White Hat Hackers
- Red Hat Hackers
- Grey Hat Hackers

Maks poeng: 0.5

11 _____ is a naming system given to different computers which adapt to human-readable domain names.

Select one alternative:

- DNS
- ISP
- HTTP
- WWW

Maks poeng: 0.5

12 Which of the following heavily bases its security on certain hard mathematical problems?

Select one alternative:

- DES
- SHA256
- AES
- RSA

Maks poeng: 0.5

13 Which of the following is not used to provide data integrity?

Select one alternative:

- MAC
- Asymmetric Encryption
- Hash function
- Symmetric Encryption

Maks poeng: 0.5

14 You have just got an unexpected email

****

Dear Customer,

You are receiving this email because you've previously registered in our customer mail list.
As you have bought a gas grill from us recently, we'd like to make you a special offer with 40% discount for your future purchases. Please click the following coupon to activate it no longer than 1 day after your receive this email

If you don't want to receive our offers in future, you can cancel your registration it by clicking the unsubscribe link: **UNSUBSCRIBE**

****

What is the best course of action to take?

Select one alternative:

- It's good to receive a coupon. I should activate the coupon immediately in case I forget it later
- It's a spam email. I would ignore it and block the sender's email address
- It's wired since I haven't registered there. I need to click the link to unsubscribe it
- It's a spam email. I need to unsubscribe it

Maks poeng: 0.5

15 Which of the following statements best describes modern hackers?

Select one alternative:

- Bored and lonely anti-social teenagers who hack as a challenge and sometimes for profit
- Highly-organised crime gangs run like businesses who deploy highly automated and sometimes highly targeted attacks against individuals and businesses for profit
- Computer savvy people who hack individuals and businesses as a form of competition
- All of the above

Maks poeng: 0.5

16 One common way to maintain data availability is _____

Select one alternative:

- data altering
- data clustering
- data recovery
- data mirroring and backup

Maks poeng: 0.5

17 Suicide Hackers are those

Select one alternative:

- who break a system for some specific purpose with or without keeping in mind that they may suffer long term imprisonment due to their malicious activity
- who know the consequences of their hacking activities and hence try to prevent them by erasing their digital footprints
- who are employed in an organisation to do malicious activities on other firms
- individuals with no knowledge of codes but an expert in using hacking tools

Maks poeng: 0.5

18 Which method of hacking will record all your keystrokes?

Select one alternative:

- Keyboard monitoring
- Keyjacking
- Keyhijacking
- Keylogging

Maks poeng: 0.5

19 _____ is an internet scam done by cyber-criminals where the user is convinced digitally to provide confidential information.

Select one alternative:

- MiTM attack
- Website attack
- DoS attack
- Phishing attack

Maks poeng: 0.5

20 The intent of a _____ is to overkill the targeted server's bandwidth and other resources of the target website.

Select one alternative:

- Website attack
- DoS attack
- Phishing attack
- MiTM attack

Maks poeng: 0.5

21 Which of the following are security requirements of a cryptographic Hash function?

Select one or more alternatives:

- [x] it has variable input length
- [x] it should be collision resistant
- [x] it should have distinct outputs for any two different inputs
- [x] it has fixed output length
- [ ] it should be pre-image resistant
- [x] it should be distinguishable from randomly generated string

Maks poeng: 1

22 Suppose a user's password is hashed with SHA256 and the hash is then stored in a system. In practice, which of the following will significantly reduce the strength of hashed password and may lead to a successful password cracking?

Select one or more alternatives:

- [x] upper-case letters in the user's password are converted to lower-case letters before the password is hashed
- [x] SHA256 is replaced with a fast hash function with 64-bit digest
- [ ] the user's password consists of only 20 lower-case letters
- [ ] a dynamically varying salt is added the the calculation of the password hash

Maks poeng: 1

23 Which of the following are in the category of social engineering attacks?

Select one or more alternatives:

- [x] an attacker sends an e-mail that appears to come from a legitimate business requesting "verification" of information
- [ ] an attacker sends an advertisement to a large number of recipients
- [x] an attacker sends highly customized emails to few end users to obtain their private information
- [ ] an attacker inserts a virus-infected USB stick to a file system
- [x] an attacker pretends to be another person with the goal of gaining access physically to a system or building

Maks poeng: 1

24 Which of the following are entity authentication practices in network access controls?

Select one or more alternatives:

- [x] Password-based Authentication Protocol
- [ ] Virtual Private Network
- [ ] Firewalls
- [ ] IEEE 802.11
- [x] WPA2 with IEEE 802.X
- [x] RADIUS

Maks poeng: 1

25 Which of the following security controls are elements of access control?

Select one or more alternatives:

- [x] accountability
- [x] authentication
- [x] authorization
- [ ] availability

Maks poeng: 1

26 Which of the following access control methods are used in a computer system?

Select one or more alternatives:

- [ ] manpower-based access control
- [x] role-based access control
- [x] discretionary access control
- [ ] rule-based access control
- [x] attribute-based access control

Maks poeng: 1

27 In a Linux system, suppose a user's password is stored in **/etc/shadow** as:

Password:6lM97wGbU5S.Funda$8HxX3gD5UjdwnXD7mHu7Foh9s6w.NCn5cxifoki7pr0m01Re5VG/yad86LjKmpJuXB/66ks1Y7T5y6cjV6.351:18313:0:9999

Which of the following statements about the above file are not correct?

Select one or more alternatives:

- [x] '6' indicates the hash type used in the calculation
- [ ] there is no login name in the file
- [ ] '6' indicates the number of bytes in the salt
- [ ] '18313' indicates the number of hash iterations in the file
- [x] 'Password' is the user name

Maks poeng: 1

28 Which of the following can be used for protecting data integrity in an insecure communication channel?

Select one or more alternatives:

- [x] hash function
- [ ] symmetric encryption
- [ ] user authentication
- [x] message authentication code
- [x] digital signature

Maks poeng: 1

29 Which of the following are user authentications?

Select one or more alternatives:

- [x] a person opens his/her mobile phone with fingerprint
- [ ] a user receives "Permission Denied" when he/she opens a file in a system
- [x] a person provides user name and password when login to a website
- [ ] a person enters the letters from the image of "I am not a robot" in a login page
- [x] an employee uses his/her employee card to enter an office

Maks poeng: 1

30 Which of the following characteristics are provided by the RADIUS?

Select one or more alternatives:

- [x] accountability
- [ ] availability
- [ ] anti-malware
- [x] authentication
- [x] authorization

Maks poeng: 1

31 **Marks for answers:**

- no/wrong alternative gets 0 pt
- each correct alternative gets 0.5 pt
- all correct alternatives get 5 pt

Consider the following paragraphs about security and cryptography.

There are missing words/phrases, to be filled in the bank, in the sentences. Select the correct word/phrase from the list, and give your answers below the paragraphs. 0.5 marks for each correct answer.

List of words/phrases to select from:
access control; active; AES; agency; assets; security attributes; asymmetric; attack; authentication; availability; central; ciphertext; confidentiality; countermeasure; integrity; intelligence; key; masquerade; modification; non-repudiation; passive; plaintext; security policy; private key; public key; receiver; release message contents; replay; RSA; sender; symmetric; threat; traffic analysis; vulnerabilities;

The three key security objectives of computer security are *confidentiality*, *integrity* and *availability*. To provide computer security we can consider a number of related concepts.

Owners or users want to protect integrety of their assets and they specify the rules to protect them. Weaknesses in a system implementation are called vulnerabilities. If they are exploited then there is a potential violation of integrety. A/An attack is a threat that is carried out, and a countermeasure is a way to deal with it.

In communication security, if an active attack occurs it results in changes to the system resources or operation. The names of two such attacks are: traffic analysis attack and reply attack. Another attack on communication lines, called release message contents, can occur even if communications are encrypted and signed, and involves an attacker observing the time and frequency of communications. To prevent/detect attacks, security mechanisms are used to provide security services. One security service, called non-repudiation, makes it difficult for an attacker to deny that communications have taken place. Another security service, called masquerade, makes it difficult for an attacker to claim to be someone else.

Cryptography is an important part of many security mechanisms. To encrypt with a cipher a plaintext and key are used as input, and ciphertext is output. To provide confidentiality, with public key ciphers (an example algorithm is called RSA), the public key of the receiver is used as input, whereas for symetric ciphers (an example algorithm is called AES) a shared secret key is used. Comparing the two types of ciphers, an advantage of public key ciphers is that they are useful for secret key distribution, while an advantage of symmetric) ciphers is that they are fast.

Maks poeng: 5

32 Marks for answers:

- no/wrong alternative gets 0 pt
- each correct alternative gets 0.5 pt
- all correct alternatives get 5 pt

This question tests your knowledge and skills regarding OpenSSL. It's advisable to upgrade OpenSSL in case earlier versions encounter unexpected issues. (Refer to https://www.openssl.org/docs/man1.1.1 for help)

Below are some OpenSSL commands and results, you can use them as a guide to answer the questions. Some commands have selected parts hidden with XXX.

- echo -n XXX | openssl dgst -XXX
- openssl dgst -XXX
- openssl dgst -XXX -sign XXX -out XXX message.txt
- openssl dgst -XXX -verify XXX -XXX sig.bin message.txt
- openssl pkey -in XXX -out pubRSA.out -XXX
- openssl pkey -in XXX -
- openssl pkey -in XXX -pubin -text
- openssl genpkey -algorithm XXX -out XXX.pem

OpenSSL results

- 967fd5b5188289d0b28f7780013e93f481bdc196cdc50349627d7b89f3b74cb1
- 3abaeabe9bc26f534480dbdf406eccabe765941d4a179b94650301825fda3074
- 79f2b05296d391e129b54babbc303c05adc3fca819326cbf1832ef567053a1e4
- 5b9d87cc255d7b1adb3aed75214050dae04c76618becc8c20c8c2bda5bbd26c3
- 0c102ab608afc2ffe2965d509f4f58b5b115080ab40b89b495bb8e8b20387f25
- a8d942b73fc88043fc62b3f5db7c6fae15be151f40b5238fa7b60b65cc644aad
- a8cd456fa12ea6e550cd9a81e740b3b2e3bb5fb8aba3c0f47eaa561fe72ded0b

1. Calculate the SHA256 hash of the following phrase in hex-decimal form

Cybersecurity is an ever-evolving process instead of a technology

Given your answer below.

2. I generate a RSA key pair with Openssl and get the following RSA private key

-----BEGIN RSA PRIVATE KEY-----
MIIJKgIBAAKCAgEAoyXJJwHW53v35k5VKkHlFFfQNCGO/rnjtpgVqZuyx5wre7J/
7qXK2P/d+8TEEBbUTrd05pnCijQFKnV3a/4tsY1NPWygVbMIBgF/eZxJFEN5+5ZJ
lpuppfqic9DMDkhAf4/v91bmRHoVf2OHfk4CxV8u679KPor6vEgwkBFw8TJPJjTz
cM0OAWaS4SiEBlxmvQsAn5qGywD1+e93cwsvaB9pYissM3fVuelPnVgyMrnjR+Lb
kXUeZ9b2YHptuHNIPeHY6SjdsVh5ETNeYDNHp1iXQy9EPaCiq99n/FjwPwm8CUwg
DJZY20cBfSdhR2pk1E5OMzNX+OOLMyOuBApwB4SP1aQf3lYg6hyXWS5aOvz9lisc
4BIL5UGyndJjG3XxglDtTmYN+yNdwq17rJh3wMF7zUtSG9uIKHS5ZV7bR7nKSQc1
VctyKF/hDLtXkyy391wgpp60i93f9/0nsqFfvVQMzh+JX1Dm4MWMYaXk8NrhQrT5
Vk0H7jkDMH0ZqGNIPG4Bq1pB+bnBFhT2LVpwCrGedPHafSQ23w4AstLkVFy5Gwnt
AM7rTRM579PoZPh+0lKUlN/OPLtKw+0wgvk6c8tWXLBUHpFVlHioo6+MXgjQa0/+
Q6JV9BcSWzjwCsIhmNOd+Md13SPRr8LbgDdqN5InDnjfo/usktCyDQQ79CUCAwEA
AQKCAgEAlc1MNhTqTwL1TPMAIB0BSvyWoEdwFVR6Ul6zBVmBfudWxe3QqkBxUW8f
VN4HaP6NUvoAzPzCNEQvuhzB2tc4/Z7RHWVwk0AgTeNyOSfXsIOC3g/Q4glsbIsG
P3Go7DRLhNWVcXbJWHcA5kdtUfwvbytG2hB7C5JxSBDBBof9PHsFUf+syBaAlaip
lTSuhWiyrUI9AE/TFPN86FGJTlkormKpUQpzO479IAECdWdWMF2e45LaKWVw1cf7
0fqYZJT18Fw/31c2uHCUOccBETQExxQBUB9GeY/VzhsEUCEZ98focGEFzIkAbdd0
9oYCPKDkIEySYVDzpgTI+9v3HJ643bbW6lidJMQEMOOy9UFhuOOCUclWfp7dvG5t
4+T7zTT1TRNDDz3cBPO7zdKzN9XBK229jcivFzpT1Rdv2P0UIPcqqSg46dwI19dS
N7ERcwDcOQeKgo1IvOyq3UA4tmyjzH3DaZH6uAV12sMIp+RL4DAkyBISgVeS97wR
Zw9pMQOvyKNeT/nSwr/S0P3Xkk9rwXqVi86O0JKDUROjQBM/KDXYNI0ZG4meoJiL
nOtfc7zbrgP15QNXD9lhv627/sLOI8mVoRcdgWCp9rDk16tZWeD7kApTt7hi1nqo
RJIGQPTV4EKmnNx9ECq7f3QOlsFo654bMJ53n+SKBMkzh+hzWMECggEBANItZkjb
hOyqHpvs5lF1pPeFfsZvrVyclkm4VSDo0JKeR10KkxL9X5fdVRbhxjwgzIWlnSsV
YapnPDgv6De4J871xhEIS1/CTH2RA3TvRViBtCB9pqPpGC11uhOWTFbd4A8Q+ENX
n2hwcCzOMFncZ8F19f3QkcNm2Xq+6ehzADmitX/To0DuIeEO74BPXYd5+eoKkeq1
rIA41eFKpq137DOQBtB1D04apOxhrLMttRIx1nfE1al8vRGlxThOjmFWi1gNncLa
bNjF6nFrUa79H+cbh4YsZGz7WiVhl/tVq4PrXYe2RfCaEY6jOvos3mbo+OGvlME7
9ghWo1R/QA9fzJsCggEBAMa3hXr2R82QtSSfc6lEuJO/bSmPJYyLNm02lNkYEAG9
itOwfNXGD/DIO23khketU3btA0+xdmzYKWF598EvYpMtrY8uh4G6qkMyf9VyBTEP
A5MFCqIOLqVsT0pVeOsrhDsut+NBS2Bn3182N14w8sGXcLGZz/+AwIxnHNoldsJi
s27MADyTF4vTF3eM8hmfewFWMOEMljvD5C9HfaeAtc3QEjpdBSm20OSzJHfNaMkI
zW8/vz2vsJnYnoe0XY7H0b/NblmjyqQpMSnEvLr9oAk/VW9pLRf43KkR8TlWOWss
0RNhVh5sP2ZNP0j/LWt+q8VVlWEowekVXkjXLX4abj8CggEBAJFr6ialBl6/klgu
jJl2PcMpcbMZGCIluoypZvVTQOUBcL0WkPaFqzunX7VqV7/IrdoC0UQ7Eg1WSptR

wmmzGJAhC39Dbut9w3DqAitJVoDLlXcZmVA1+o2RtELTLlS4RcwG4M+vc9NOYL8P
lvLGBmAcHy0Tv5cktXsxVySHVXOLeetM4tsNKRHQRLRRtZQEOH/P+nAcbZN2P74W
6caCgEKY964KlKHY253WYyjCilNhelP6NB+F+EeanB++ctM0j0tlelyWltNR9Umu
iKD78LP2H0odswqYyyGr2bqP5xFqq5c37aJw5476r9bjbqpjrbhxxQoCU9QnJfFT
7l302dsCggEAcis8iFH5HPTX7guicwzlkxV3TVpN83qEMakbScNWZvmUSl1qy5N4
0xjndBLIx2OgwYIY1e+an5xt4fAmVRq5Yt/qilnuFq29ZtAbu/E/ZFlA73YFDuhh
Cm+4+ncy+sJMvYfw5KM+AEyNfHF0zCwJPQqaF5/Mbfp2JfSUEg1WNwZoGu8f761+
6LnGEMysx+Xl0PXJLXOC2SGJ91P2sIb1bSLvZhLNhZLgX5VBDYe5fU8OYK1aXcGU
ED/xjPwmilLrUmxfyyacpUZ5VYsP98sB6G430sO1wcEcXhLN6ehNIvNjx+Ozi9Ub
c9ZL1s+tM8ZaQA0Uvvaguh6pxeXC4GGlFwKCAQEAqs6LN+T8/lSYTkul7+YGOw5J
YD7sP/E+bHGpLpogjTXCVwFMn8esRMPj2gnOARO9YJXRT2u4kq4RLxM5hfDIpJDc
Lg+5uy6PM+HoFLMgHv0E5RqfFvoB3DPstaVXfXdbAEuklHi4Vi/sH80fVeNnPvm6
O/vzWNqy2D305W5nssaHUPgE8jjBs9C31rhcZgXjLgJp7yLkRQkVH+tlN78mB6mg
JIycJgbsGt+NA3tJWEjO2dh80Z7vWhZHypSG/Sfc+V70LiVEhSa8V/84yrGblN8E
D1M7Vs1Ly1ulk540ijtG/Ey3cUNOSYKVywU+wAPRosRlgoLhB8HzcDZHC4eT0w==
-----END RSA PRIVATE KEY-----

Save the above private key in a file privateRSA.pem (download link) and answer the following questions

- The modulo n in the RSA public key has _____ bits.
- The last byte of prime1 in hexadecimal form is 0x __ .

You want to send your public key inside the above private key to your friend Maria. Therefore, you use an openssl command pkey to obtain the public key in the plain text form (in addition to the encoded form), store it in a file pubRSA.txt, and then send the pubRSA.txt together with its SHA256 hash to Maria.

What is the SHA256 hash of pubRSA.txt in hexadecimal form? Given your answer below.

3. You have a travel plan with Maria to Spain in near future. You have been in charge of booking all flight tickets for the travel and Maria is in charge of tourism routine.

Unfortunately, you just received a message from the Airline which informs you that the flight is cancelled due to the COVID-19 situation as in the following message.

Dear passengers, due to the situation with COVID-19, the flight DY5529 on Dec. 15 between Bergen and Barcelona is cancelled. You are entitled for refund of your flight and you should claim for compensation no later than Nov. 15, 2020.

You need to forward this message to Maria. Both you and Maria have learned cryptography from INF140, so you decide to send the above message together with a digital signature.

You copy the message and store it in a file message.txt (download link), use your RSA private key in the above (stored in the key file privateRSA.pem) and generate a signature sig.bin on the SHA256 hash of message.txt. Then you mail the message.txt together with the signature sig.bin to Maria.

- What is the SHA256 hash of the message?

- What is the SHA256 of the sig.bin in hexadecimal form? Given your answer below.

4. Suppose Maria has agreed with you in advance that all your signatures will be calculated with SHA256. Upon receiving your mail, Maria wants to verify the signature of message.txt containing the bad news.

Suppose the content in the message.txt was modified by an attacker as: Nov. 15 modified as Nov. 30). If your OpenSSL command is correct, what is the OpenSSL output? Copy the result in the blank below.

In the above process, if SHA256 is replaced by a MD5 in digital signature, which of the following statement below is true? Choose A, B or C. B

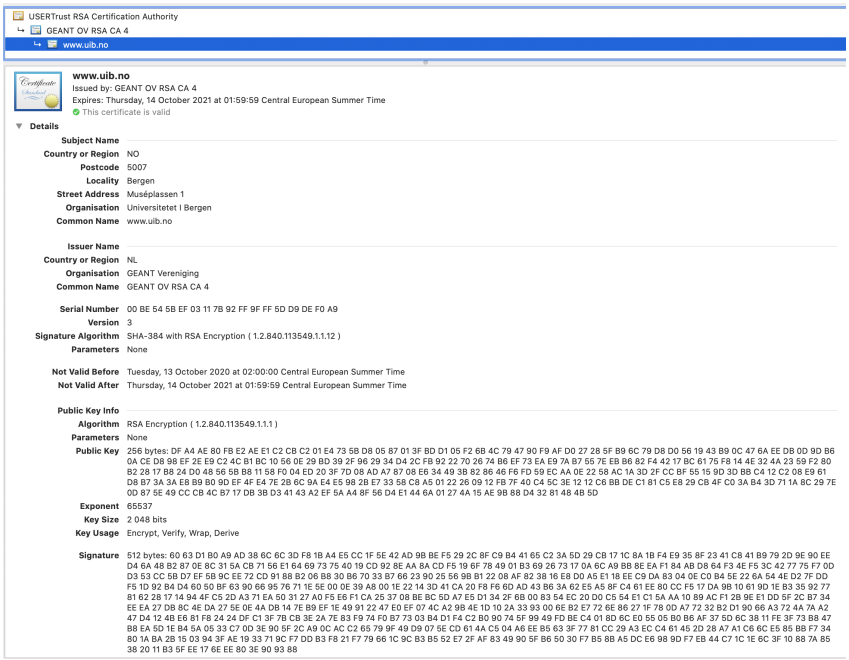
A. MD5 is nearly as secure as SHA256, and it's infeasible to forge the digital signature
B. MD5 is not as secure as SHA256, but it's infeasible to forge the digital signature
C. MD5 is not as secure as SHA256, and it's feasible to forge the digital signature

Maks poeng: 5

33 Marks for answers:

- no/wrong alternative gets 0 pt
- each correct alternative gets 0.5 pt
- all correct alternatives get 5 pt

Consider the X.509 certificate in the following (If it's too small, open it in a new tab in your browser or directly visit https://www.uib.no/)



1. Which of the following are the correct subject and issuer of this certificate? D

A. GEANT VErenginging, Universitetet i Bergen
B. Universitetet i Bergen, UAERTRUST RSA
C. GEANT VErenginging, UAERTRUST RSA
D. Universitetet i Bergen, GEANT VErenginging

2. What is the size of this public key? 2048 bits.

3. What is the hexadecimal of e in the user's public key? 0x B0

4. What are the last two hexadecimal digits of n in the user's RSA key? D9

5. What is the hash algorithm used in the signature? SHA-384

6. What is the expiry date of this public-key certificate? Provide the answer in the format of dd/mm/yyyy. 14/10/2021

Open a new tab in your browser and **visit https://uib.no**. Answer your following question

7. What is the size of the public key of GEANT VErenginging? 2048

8. Which of the following are the correct issuer of UAERTRUST RSA? B

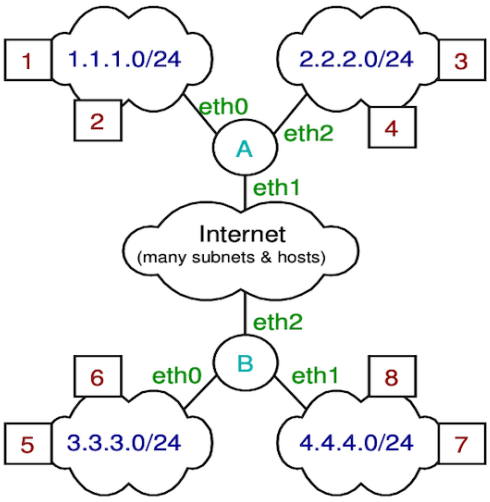
A. GEANT VErenginging
B. Universitetet i Bergen
C. UAERTRUST RSA
D. USA authority

9. Which of the following attack is the public key certificate is designed to prevent? D

A. Denial of Service Attack
B. Replay Attack
C. Meet-in-the-Middle Attack
D. Man-in-the-Middle Attack

Maks poeng: 5

34 The following figure shows a network topology. On the 4 subnets, assume there are many hosts (although only two hosts are shown for each subnet due to space). The host IP addresses are obtained from the subnet address and the host number, e.g. host 2 has IP 1.1.1.2. Each of the two routers has three interfaces.



Suppose you are the IT administrator for the two subnets 1.1.1.0/24, 2.2.2.0/24 attached to router A and need to add a rule to the firewall running on router A. The default policy for the firewall is **accept**. Stateful Packet Inspection is enabled on the firewall.

For each of the following policies, write a rule that implements it by filling in the table. You may use 1 or more rows, but the rules should be as simple as possible. (E.g.: Use the format "1.1.1.1:22" to show both IP address and port number in the "Source" and "Destination" columns). For each part, assume initially there are no firewall rules; i.e. your answer in Question (ii) is independent of your answer in Question (i).

Question I. Block all hosts on network 4.4.4.0/24 from accessing any SSH servers on network 1.1.1.0/24 (1pt)

Question II. Block host 3 from browsing to any websites in network 4.4.4.0/24 (1pt)

Question III. Block all hosts in network 4.4.4.0/24 from accessing internal servers, except host 8 should be able to access the SSH on host 1 (1pt)

Consider the same network as in Figure 1. Now assume the default policy is drop. The current firewall table is:

Source	Destination	Protocol	Action
1.1.1.1:*	4.4.4.0/24:22	TCP	Accept
3.3.3.6:*	2.2.2.0/24:25	TCP	Accept
4.4.4.0/24:53	1.1.1.1:*	TCP	Accept
2.2.2.0/24:*	4.4.4.8:80	TCP	Accept
1.1.1.0:*	*:443	TCP	Accept

The following TCP SYN packets have recently been received by the firewall

- Packet 1 arrived on interface eth0 with source 1.1.1.2:40123 and destination 3.3.3.6:25
- Packet 2 arrived on interface eth1 with source 3.3.3.6:50345 and destination 2.2.2.4:25
- Packet 3 arrived on interface eth2 with source 2.2.2.3:50789 and destination 4.4.4.8:80

Question IV. Draw the SPI table at the firewall. (2pt)

Source	Destination	State

Question V. With your SPI table from the answer above, now assume a TCP Data segment arrives on interface eth1 with source 4.4.4.8:80 and destination 2.2.2.3:50789. Explain what happens to the TCP Data segment and why. (2pt)

For Questions I - III, fill in your answer in a table as below (You can create a table with the icon of table in the tool bar)

Question	Source	Destination	Protocol	Action
I				
II				
III				

Fill in your answer here

Question	Source	Destination	Protocol	Action

I	4.4.4.0/24:*	1.1.1.0/24:22	TCP	Drop
II	2.2.2.3:* 2.2.2.3:*	4.4.4.0/24:80 4.4.4.0/24:443	TCP TCP	Drop Drop
III	4.4.4.8:* 4.4.4.0/24	1.1.1.1:22 *:*	TCP *	Accept Drop

Question IV:

The first packet is blocked since it doesnt mach any of our firewall rules

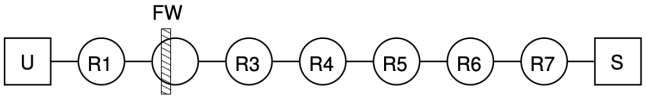
Source	Destination	State
3.3.3.6:50345	2.2.2.4:25	Established
2.2.2.3:50789	4.4.4.8:80	Established

Question V:

The TCP segment is accepted by the firewall becuse the connection between the two enteties are established.

Maks poeng: 7

35 Consider the internet below, with a web browser running on computer U and a web server on S. There are seven routers shown (router 2 is also running as a firewall, FW), however assume there are more routers in the path. For example, although not shown, assume there are additional routers between R4 and R5, and between R5 and R6.



In your answers to the following questions use the device name to refer to the IP address. For example, the IP address of the computer running a web browser is U. The IP address of the firewall router is FW.

Assume the firewall is using packet filtering only and contains a rule to block packets destined.

Question I. First consider the case of a web proxy running on R5. The web browser uses the proxy to access the web site S. Explain why a web proxy can be used to bypass a packet filtering firewall when U is using HTTP. (1 pt)

Question II. Now consider that a VPN server is running on R5 (instead of the web proxy). Computer U is configured to use the VPN.

(a) If HTTP is used by U, and FW intercepts the packet sent by U, explain what the firewall can "see". What are the IP source and destination addresses? What does the firewall know about the contents of the packet? (2 pt)

(b) Explain the differences in security achieved when using HTTP with a VPN versus using HTTPs with a VPN. In other words, what extra security objectives are met by using HTTPS, that are not met when using HTTP? (2 pt)

Question III. Now consider that Tor is being used on computer U and a Tor connection has been established on the relays on R4, R5 and R6. R6 is the exit relay.

(a) If the firewall intercepts the packet from U, explain what the firewall can see or knows. That is, what source/destination addresses does it see, what content can it see and who does it know is communicating. (1 pt)

(b) When R5 receives the packet, explain what R5 can see or knows. (1 pt)

(c) When R7 receives the packet, explain what R7 can see or knows. What is the security advantage when U is using HTTPs instead of using HTTP? (1 pt)

Fill in your answer here

Question I:
When the U is using a proxy to access S, the firewall will see that U tries to connect to R5 and not S. Therefore the firewall will accecpt the request because U is not directly connected to S

Question II:
a)
The firewall can only see the source and the destination because the the content of the packet is encrypted along the way
b)
When you use HTTPS and VPN nobody including the VPN server cannot see any of the user U's data along its destination. When using HTTP everybody inn between the user and VPN can see the data including the VPN

Question III:
a)
The firewall will read that the packet it intersepted is comming from U and its destination is R4, also the firewall cannot read any of the data beacuse its encrypted.
b)
Just as the firewall R5 cannot read any of the data, but it can see that the source is R4 and the destination is R6
c)
Since R6 was the exit relay the content is no longer encrypted by Tor. So R7 can see that te source is R6 and the destination is S, but it depends on what protocol the packet was sent with whether or not R7 can read the content of the file. If HTTPS is used then R7 cannot read the content, however if HTTP is used the file is no longer encrypted and R7 can read it.

Maks poeng: 8

36 This question is intended for collecting points in the two mandatory assignments.

Important information:
Only press « deliver exam» when you are absolutely sure you are ready!

Provide your marks for the two mandatory assignments here in the form (A1+A2)/4=Total, e.g, (80+92)/4=43. (Your mark will be checked)

(94+99)/4=48

Maks poeng: 50