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 security attributes ✓ 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 security policy ✓ . 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: masquerade ✓ attack and reply attack. Another attack on communication lines, called traffic analysis ✓ , 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 authentication ✓ , 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 symmetric ✓ 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.

Correct. 5 of 5 marks.

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.

5b9d87cc255d7b1adb3aed75214050dae04c76618becc8c20c8c2bda5bbd26c3 ✓

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
Ipuppfqic9DMDkhAf4/v91bmRHoVf2OHfk4CxV8u679KPor6vEgwkBFw8TJPJjTz
cM0OAWaS4SiEBlxmvQsAn5qGywD1+e93cwsvaB9pYissM3fVueIPnVgyMrnjR+Lb
kXUeZ9b2YHptuHNIPeHY6SjdsVh5ETNeYDNHp1iXQy9EPaCiq99n/FjwPwm8CUwg
DJZY20cBfSdhR2pk1E5OMzNX+OOLMyOuBApwB4SP1aQf3IYg6hyXWS5aOvz9Iisc
4BIL5UGyndJjG3XxglDtTmYN+yNdwq17rJh3wMF7zUtSG9uIKHS5ZV7bR7nKSQc1
VctyKF/hDLtXkyy391wgpp60i93f9/0nsqFfvVQMzh+JX1Dm4MWMYaXk8NrhQrT5
Vk0H7jkDMH0ZqGNIPG4Bq1pB+bnBFhT2LVpwCrGedPHafSQ23w4AstLkVFy5Gwnt
AM7rTRM579PoZPh+0lKUIN/OPLtKw+0wgvk6c8tWXLBUHpFVlHioo6+MXgjQa0/+
Q6JV9BcSWzjwCsIhmNOd+Md13SPRr8LbgDdqN5InDnjfo/usktCyDQQ79CUCAwEA
AQKCAgEAlc1MNhTqTwL1TPMAIB0BSvyWoEdwFVR6Ul6zBVmBfudWxe3QqkBxUW8f
VN4HaP6NUvoAzPzCNEQvuhzB2tc4/Z7RHWVwk0AgTeNyOSfXslOC3g/Q4glsbIsG
P3Go7DRLhNWVcXbJWHcA5kdtUfwvbytG2hB7C5JxSBDBBof9PHsFUf+syBaAlaip
lTSuhWiyrUI9AE/TFPN86FGJTIkormKpUQpzO479IAECdWdWMF2e45LaKWVw1cf7
0fqYZJT18Fw/31c2uHCUOccBETQExxQBUB9GeY/VzhsEUCEZ98focGEFzIkAbdd0
9oYCPKDklEySYVDzpgTI+9v3HJ643bbW6IidJMQEMOOy9UFhuOOCUclWfp7dvG5t
4+T7zTT1TRNDDz3cBPO7zdKzN9XBK229jcivFzpT1Rdv2P0UIPcqqSg46dwI19dS
N7ERcwDcOQeKgo1IvOyq3UA4tmyjzH3DaZH6uAV12sMIp+RL4DAkyBISgVeS97wR
Zw9pMQOvyKNeT/nSwr/S0P3Xkk9rwXqVi86O0JKDUROjQBM/KDXYNI0ZG4meoJiL
nOtfc7zbrgP15QNXD9lhv627/sLOl8mVoRcdgWCp9rDk16tZWeD7kApTt7hi1nqo
RJIGQPTV4EKmnNx9ECq7f3QOIsFo654bMJ53n+SKBMkzh+hzWMECggEBANItZkjb
hOyqHpvs5lF1pPeFfsZvrVycIkm4VSDo0JKeR10KkxL9X5fdVRbhxjwgzIWInSsV
YapnPDgv6De4J871xhEIS1/CTH2RA3TvRViBtCB9pqPpGC11uhOWTFbd4A8Q+ENX
n2hwcCzOMFncZ8F19f3QkcNm2Xq+6ehzADmitX/To0DuIeEO74BPXYd5+eoKkeq1
rIA41eFKpq137DOQBtB1D04apOxhrLMttRIx1nfE1al8vRGlxThOjmFWi1gNncLa
bNjF6nFrUa79H+cbh4YsZGz7WiVhI/tVq4PrXYe2RfCaEY6jOvos3mbo+OGvlME7
9ghWo1R/QA9fzJsCggEBAMa3hXr2R82QtSSfc6lEuJO/bSmPJYyLNm02INkYEAG9
itOwfNXGD/DIO23khketU3btA0+xdmzYKWF598EvYpMtrY8uh4G6qkMyf9VyBTEP
A5MFCqIOLqVsT0pVeOsrhDsut+NBS2Bn3182N14w8sGXcLGZz/+AwIxnHNoldsJi
s27MADyTF4vTF3eM8hmfewFWMOEMljvD5C9HfaeAtc3QEjpdBSm20OSzJHfNaMkI
zW8/vz2vsJnYnoe0XY7H0b/NblmjyqQpMSnEvLr9oAk/VW9pLRf43KkR8TlWOWss
0RNhVh5sP2ZNP0j/LWt+q8VVlWEowekVXkjXLX4abj8CggEBAJFr6ialBI6/klgu
jJl2PcMpcbMZGCIIuoypZvVTQOUBcL0WkPaFqzunX7VqV7/IrdoC0UQ7Eg1WSptR
wmmzGJAhC39Dbut9w3DqAitJVoDLlXcZmVA1+o2RtELTLIS4RcwG4M+vc9NOYL8P
lvLGBmAcHy0Tv5cktXsxVySHVXOLeetM4tsNKRHQRLRRtZQEOH/P+nAcbZN2P74W
6caCgEKY964KIKHY253WYyjCilNhelP6NB+F+EeanB++ctM0j0tIeIyWltNR9Umu
iKD78LP2H0odswqYyyGr2bqP5xFqq5c37aJw5476r9bjbqpjrbhxxQoCU9QnJfFT
7I302dsCggEAcis8iFH5HPTX7guicwzlkxV3TVpN83qEMakbScNWZvmUSl1qy5N4
0xjndBLIx2OgwYIY1e+an5xt4fAmVRq5Yt/qiInuFq29ZtAbu/E/ZFIA73YFDuhh
Cm+4+ncy+sJMvYfw5KM+AEyNfHF0zCwJPQqaF5/Mbfp2JfSUEg1WNwZoGu8f761+
6LnGEMysx+Xl0PXJLXOC2SGJ91P2sIb1bSLvZhLNhZLgX5VBDYe5fU8OYK1aXcGU
ED/xjPwmiILrUmxfyyacpUZ5VYsP98sB6G430sO1wcEcXhLN6ehNIvNjx+Ozi9Ub
c9ZL1s+tM8ZaQA0Uvvaguh6pxeXC4GGlFwKCAQEAqs6LN+T8/lSYTkul7+YGOw5J
YD7sP/E+bHGpLpogjTXCVwFMn8esRMPj2gnOARO9YJXRT2u4kq4RLxM5hfDIpJDc
Lg+5uy6PM+HoFLMgHv0E5RqfFvoB3DPstaVXfXdbAEuklHi4Vi/sH80fVeNnPvm6
O/vzWNqy2D305W5nssaHUPgE8jjBs9C31rhcZgXjLgJp7yLkRQkVH+tlN78mB6mg
JIycJgbsGt+NA3tJWEjO2dh80Z7vWhZHypSG/Sfc+V70LiVEhSa8V/84yrGbIN8E
D1M7Vs1Ly1uIk540ijtG/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 4096 ✓ bits.
- The last byte of prime1 in hexadecimal form is 0x 9b ✓ .

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.

79f2b05296d391e129b54babbc303c05adc3fca819326cbf1832ef567053a1e4 ✓

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?

a8d942b73fc88043fc62b3f5db7c6fae15be151f40b5238fa7b60b65cc644aad ✓

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

a8cd456fa12ea6e550cd9a81e740b3b2e3bb5fb8aba3c0f47eaa561fe72ded0b ✓

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.

Verification Failure ✓

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. C ✓

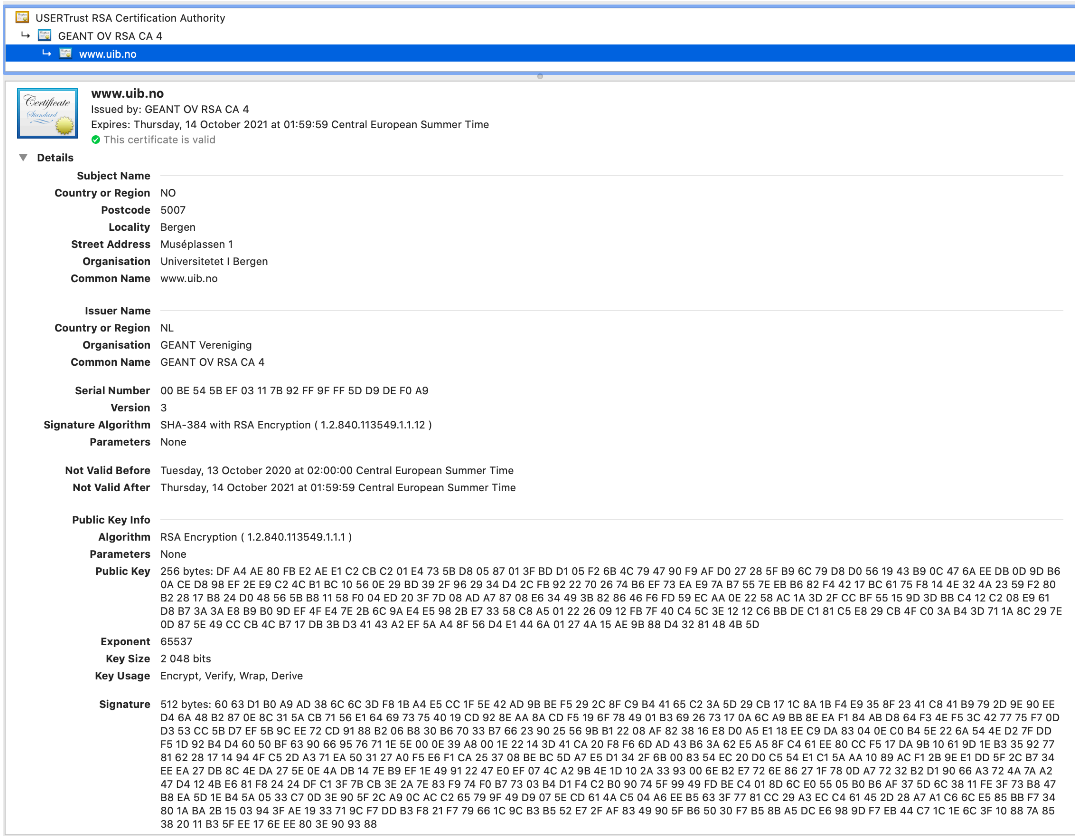
A. MD5 is nearly as secure as SHA256, and it's infeasible to forge the digital signature
B. MD5 is not as secure as SHA256, but it's infeasible to forge the digital signature
C. MD5 is not as secure as SHA256, and it's feasible to forge the digital signature

Correct. 5 of 5 marks.

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/)



USERTrust RSA Certification Authority
↳ GEANT OV RSA CA 4
↳ www.uib.no

www.uib.no
Issued by: GEANT OV RSA CA 4
Expires: Thursday, 14 October 2021 at 01:59:59 Central European Summer Time
✓ This certificate is valid

▼ **Details**

Subject Name
Country or Region NO
Postcode 5007
Locality Bergen
Street Address Muséplassen 1
Organisation Universitetet I Bergen
Common Name www.uib.no

Issuer Name
Country or Region NL
Organisation GEANT Vereniging
Common Name GEANT OV RSA CA 4

Serial Number 00 BE 54 5B EF 03 11 7B 92 FF 9F FF 5D D9 DE F0 A9
Version 3
Signature Algorithm SHA-384 with RSA Encryption (1.2.840.113549.1.1.12)
Parameters None

Not Valid Before Tuesday, 13 October 2020 at 02:00:00 Central European Summer Time
Not Valid After Thursday, 14 October 2021 at 01:59:59 Central European Summer Time

Public Key Info
Algorithm RSA Encryption (1.2.840.113549.1.1.1)
Parameters None
Public Key 256 bytes: DF A4 AE 80 FB E2 AE E1 C2 CB C2 01 E4 73 5B D8 05 87 01 3F BD D1 05 F2 6B 4C 79 47 90 F9 AF D0 27 28 5F B9 6C 79 D8 D0 56 19 43 B9 0C 47 6A EE DB 0D 9D B6 0A CE D8 98 EF 2E E9 C2 4C B1 BC 10 56 0E 29 BD 39 2F 96 29 34 D4 2C FB 92 22 70 26 74 B6 EF 73 EA E9 7A B7 55 7E EB B6 82 F4 42 17 BC 61 75 F8 14 4E 32 4A 23 59 F2 80 B2 28 17 B8 24 D0 48 56 5B B8 11 58 F0 04 ED 20 3F 7D 08 AD A7 87 08 E6 34 49 3B 82 86 46 F6 FD 59 EC AA 0E 22 58 AC 1A 3D 2F CC BF 55 15 9D 3D BB C4 12 C2 08 E9 61 D8 B7 3A 3A E8 B9 B0 9D EF 4F E4 7E 2B 6C 9A E4 E5 98 2B E7 33 58 C8 A5 01 22 26 09 12 FB 7F 40 C4 5C 3E 12 12 C6 BB DE C1 81 C5 E8 29 CB 4F C0 3A B4 3D 71 1A 8C 29 7E 0D 87 5E 49 CC CB 4C B7 17 DB 3B D3 41 43 A2 EF 5A A4 8F 56 D4 E1 44 6A 01 27 4A 15 AE 9B 88 D4 32 81 48 4B 5D
Exponent 65537
Key Size 2 048 bits
Key Usage Encrypt, Verify, Wrap, Derive

Signature 512 bytes: 60 63 D1 B0 A9 AD 38 6C 6C 3D F8 1B A4 E5 CC 1F 5E 42 AD 9B BE F5 29 2C 8F C9 B4 41 65 C2 3A 5D 29 CB 17 1C 8A 1B F4 E9 35 8F 23 41 C8 41 B9 79 2D 9E 90 EE D4 6A 48 B2 87 0E 8C 31 5A CB 71 56 E1 64 69 73 75 40 19 CD 92 8E AA 8A CD F5 19 6F 78 49 01 B3 69 26 73 17 0A 6C A9 BB 8E EA F1 84 AB D8 64 F3 4E F5 3C 42 77 75 F7 0D D3 53 CC 5B D7 EF 5B 9C EE 72 CD 91 88 B2 06 B8 30 B6 70 33 B7 66 23 90 25 56 9B B1 22 08 AF 82 38 16 E8 D0 A5 E1 18 EE C9 DA 83 04 0E C0 B4 5E 22 6A 54 4E D2 7F DD F5 1D 92 B4 D4 60 50 BF 63 90 66 95 76 71 1E 5E 00 0E 39 A8 00 1E 22 14 3D 41 CA 20 F8 F6 6D AD 43 B6 3A 62 E5 A5 8F C4 61 EE 80 CC F5 17 DA 9B 10 61 9D 1E B3 35 92 77 81 62 28 17 14 94 4F C5 2D A3 71 EA 50 31 27 A0 F5 E6 F1 CA 25 37 08 BE BC 5D A7 E5 D1 34 2F 6B 00 83 54 EC 20 D0 C5 54 E1 C1 5A AA 10 89 AC F1 2B 9E E1 DD 5F 2C B7 34 EE EA 27 DB 8C 4E DA 27 5E 0E 4A DB 14 7E B9 EF 1E 49 91 22 47 E0 EF 07 4C A2 9B 4E 1D 10 2A 33 93 00 6E B2 E7 72 6E 86 27 1F 78 0D A7 72 32 B2 D1 90 66 A3 72 4A 7A A2 47 D4 12 4B E6 81 F8 24 24 DF C1 3F 7B CB 3E 2A 7E 83 F9 74 F0 B7 73 03 B4 D1 F4 C2 B0 90 74 5F 99 49 FD BE C4 01 8D 6C E0 55 05 B0 B6 AF 37 5D 6C 38 11 FE 3F 73 B8 47 B8 EA 5D 1E B4 5A 05 33 C7 0D 3E 90 5F 2C A9 0C AC C2 65 79 9F 49 D9 07 5E CD 61 4A C5 04 A6 EE B5 63 3F 77 81 CC 29 A3 EC C4 61 45 2D 28 A7 A1 C6 6C E5 85 BB F7 34 80 1A BA 2B 15 03 94 3F AE 19 33 71 9C F7 DD B3 F8 21 F7 79 66 1C 9C B3 B5 52 E7 2F AF 83 49 90 5F B6 50 30 F7 B5 8B A5 DC E6 98 9D F7 EB 44 C7 1C 1E 6C 3F 10 88 7A 85 38 20 11 B3 5F EE 17 6E EE 80 3E 90 93 88

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 10001 ✓

4. What are the last two hexadecimal digits of n in the user's RSA key? 5D ✓

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? 4096 ✓

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

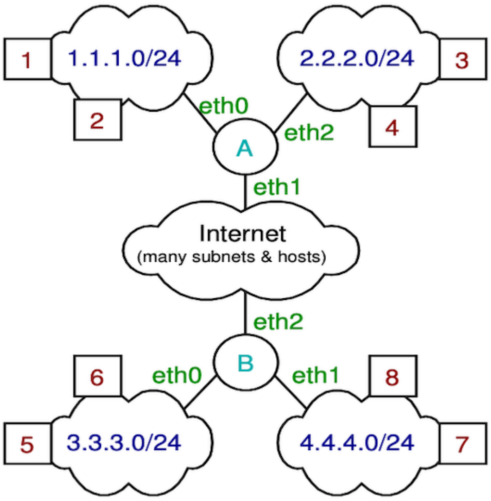
A. GEANT VErenginging
B. Universitetet i Bergen
C. UAERTRUST RSA
D. USA authority

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

Correct. 5 of 5 marks.

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:*	4.4.4.0/24:80	TCP	DROP
	2.2.2.3:*	4.4.4.0/24:443	TCP	DROP
III	4.4.4.8:*	1.1.1.1:22	TCP	ACCEPT
	4.4.4.0/24:*	1.1.1.0/24:*	TCP/UDP	DROP
	4.4.4.0/24:*	2.2.2.0/24:*	TCP/UDP	DROP

Question IV

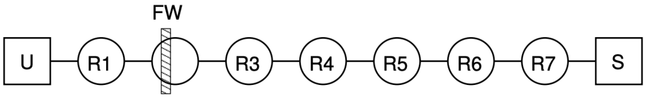
Source	Destination	State
3.3.3.6:50345	2.2.2.4:25	Established
2.2.2.3:50789	4.4.4.8:80	Established

Question V

The packet is accepted by the firewall, since the connection between the IP addresses has been established, and the port numbers match with the port numbers in the SPI table. If the destination port was something other than 50789, the packet would be dropped.

Answered.

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
The firewall have filters blocking HTTP traffic to and from S, but not to and from R5. So a request to R5 can get through the firewall, then R5 can relay that request to S (since it is behind the firewall the filter won't stop it), and send the reply back to U.

Question II
(a) The firewall can only see the destination IP address, which is R5, and the source IP address which is U. The contents of the packet is encrypted, so the firewall cannot read it.

(b) If you use HTTP and not HTTPs with the VPN, the information sent between the VPN and the destination server (i.e. a website) is not encrypted. This means that the data cannot be read if it intercepted between you and the VPN, but it can if it is intercepted between the VPN and the destination server. If you use HTTPs (alot of) the data will be encrypted all the way from you to the destination server (the encryption between you and VPN hide more of the data, like TCP headers, than the encryption between the VPN and the destination server).

Question III
(a) The firewall can only see the destination IP address, which is R4, and the source IP address which is U. The contents of the packet is encrypted, so the firewall cannot read it.

(b) R5 can see the source R4 and it can decrypt the new destination, which is R6. The rest of the data is encrypted, or has been removed from the packet (for instance R4 does not pass on that it received the packet from U).

(c) R7 can see the source of the packet, which is the TOR exit relay, R6, and the destination S. If HTTP is used, R7 can read all the data in the packet. The benefit of HTTPs is that alot of the data will be encrypted, so that R7 can't read it.

Answered.

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)

(93+107)/4=50

Answered.