General

Question 1

An intruder has infiltrated a server hosting a law firm's system where critical client data is stored. This intruder has managed to access and encrypt the database containing valuable client information. The intruder is demanding a ransom in exchange for decrypting the database. Which security principles were compromised?

Confidentiality and Authorization.

Integrity and Availability.

Confidentiality and Availability.

Integrity and Confidentiality.

Question 2

In the year of 2084, Danish citizens are facing severe restrictions on internet access, with government surveillance monitoring online activities. A group of activists needs to communicate securely to organize peaceful protests without being tracked. They choose to utilize onion routing via Tor (The Onion Router) for their communication. What should they be aware of that could compromise their anonymity?

A Weak encryption: Tor's layered encryption does not guarantee complete protection. When the packet passes through the nodes, each node removes a layer of encryption, and the closer the packet is to its destination, the easier it is to manipulate or hijack it.

Traffic analysis correlating entry and exit nodes: Despite encryption, sophisticated traffic analysis could correlate entry and exit nodes, potentially compromising anonymity.

Increased browsing speed could tip off surveillance: The additional layers in onion routing provide faster communication, however, in cases where an individual is specifically targeted for surveillance, an increase in browsing speed could draw attention to their activities, prompting further investigation or monitoring.

No metadata concealment: Tor does not conceal such metadata as the fact that an individual is using Tor, the timing and frequency of the data packets, and geolocation. Though the content itself remains encrypted within the Tor network, the metadata available can allow adversaries to deduce certain metadata-related information.

Cryptography

Question 1

Which advanced feature of the SSL/TLS protocol enhances security by preventing an attacker from decryption previously recorded sessions, even if they later obtain the server's private key?

Perfect Forward Secrecy (PFS).

Extended Validation (EV).

Cipher Suite Negotiation.

Public Key Pinning (PKP).

Question 2

Which of the following is a requirement of a hash function to ensure secure storage of passwords?

Pre-image resistance.

Reversibility.

Avalanche effect.

High hash function efficiency.

Question 3

Alice, the expert in cryptography, is explaining the importance of encryption to Bob. In the context of this, what is the main purpose of a Public Key Infrastructure (PKI)?

Generating random keys for secure data transmission.

Verifying the integrity of encrypted data.

Managing and distributing public keys for secure communication.

Performing real-time analysis of network traffic for potential threats.

Question 4

Alice wishes to communicate securely with Bob.

Alice adds a digital signature S to message M, encrypts (S, M), and sends it to Bob using public key cryptography.

This communication will be decrypted by Bob.

Which of the keys in the following sequence is utilized to perform these operations?

Encryption: Alice's private key followed by Bob's private key; Decryption: Alice's public key followed by Bob's public key.

Encryption: Alice's private key followed by Bob's public key; Decryption: Bob's private key followed by Alice’s public key.

Encryption: Alice's public key followed by Bob's private key; Decryption: Bob's public key followed by Alice’s private key.

Encryption: Alice's private key followed by Bob's public key; Decryption: Alice's public key followed by Bob's private key.

Security Protocols

Question 1

An airline has an existing website for online booking and checking in. Basically, customers choose a flight, and to book, they have to enter their name, address, email address and credit card details; for the successful booking they get a booking reference, which we can think of a nonce (that cannot be guessed). To check in, the users have to enter their name and booking reference and get a QR code for boarding. We can also regard this QR code as a nonce.

All the communication between customer browsers and airline website is via TLS (the server refuses unencrypted http).

The system offers users also to make an account, where the user name is an email address and they can choose a password. The server sends a confirmation email to the user containing a link that they have to click to activate the account. After that, one can log in to see all one's bookings, modify, cancel, check-in, etc.

Which of the following statements is **NOT** correct?

1. Making an account is only a matter of convenience, it does not give a higher level of security for the customer.

2. The confirmation email for account verification is actually not necessary for security; its purpose is to prevent accidental misspelling of an email address.

3. The use of TLS is sufficient to ensure the secret transmission of the credit card number from customer to server.

4. The use of TLS is sufficient to ensure the secret transmission of the booking reference and QR code from the server to the customer.

Question 2

The airline from the first tasks wants to design a mobile phone App for integrating online booking, checking in, and showing boarding pass at the airport.

This app avoids the overhead of TLS by using a self-designed light-weight protocol. Upon installation, the user has to enter their name, phone number. The app sends this information, together with a fresh nonce, encrypted with the public key of the airline's server. The server sends a code via SMS (text message) to the claimed phone number, which the user must enter into the app. Next the app generates a strong symmetric key and transmits it together with the SMS code and the previous message, again encrypted by the server. From now on, all communication can just happen encrypted with this key.

Which of the following statements is correct?

1. This design allows for man-in-the-middle attacks.

2. Even if an attacker can see the SMS messages from airline server to user phones, it is impossible to register any account under a false phone number.

3. If an attacker observes all traffic between app and airline server, and finds out the private key of the airline server, then they can decrypt everything. This would however also be the case when using TLS 1.3 instead.

4. If an attacker observes all traffic between app and airline server, and finds out the private key of the airline server, then they can decrypt everything. This would however not be the case when using TLS 1.3 instead.

Question 3

Consider the attached protocol KeyEx.AnB. OFMC finds an attack on this (see KeyEx.attack). What's wrong?

```
Protocol: KeyEx

Types: Agent A,B,S;

    Number g,X,Y,Msg;

    Function pk;

Knowledge:

    A: A,B,S,pk(B),pk(S),g;

    B: A,B,S,pk(B),inv(pk(B)),pk(S),g;

    S: A,B,S,pk(S),inv(pk(S)),pk(B),g;

Actions:

A->B: {A,B,exp(g,X)}pk(B)

B->A: {A,B,exp(g,X),exp(g,Y)}inv(pk(B))

A->B: {| Msg |}exp(exp(g,X),Y)

Goals:

Msg secret between A,B

B authenticates A on Msg
```

```
Open-Source Fixedpoint Model-Checker version 2023b

SUMMARY:  ATTACK_FOUND

GOAL:  weak_auth

ATTACK TRACE:

i -> (x401,1): {x402,x401,g}_(pk(x401))

(x401,1) -> i: {x402,x401,g,exp(g,Y(1))}_inv(pk(x401))
```

```
i -> (x401,1): {|x310|}_(exp(g,Y(1)))
```

1. A's Diffie-Hellman half-key is not authenticated.

2. A dishonest user in role A has used 1 as an exponent.

3. A and B do agree on each other's names.

4. The intruder replays the message of an honest B.

Question 4

Is there a correction for KeyEx.AnB that changes only the "Action" section of the protocol (i.e., without modifying the types, knowledge, and goal sections)?

1. Yes, one can use the third party S to solve this.

2. Yes, the third message must include more information.

3. Yes, A can first generate a fresh key and send it encrypted with the public key of B, and then the rest of the exchange can be protected by that key.

4. No, there is no protocol with this initial knowledge that achieves this goal.

Privacy

Question 1

Consider the following credential system: every use has initially an electronic passport containing name, date of birth, etc., as well as a public key, e.g. of the form

```
{ alice, 17/4/1999, ..., pk(alice) }inv(pk(danish_authorities))
```

where `pk(alice)` is the public key of `alice` in this case and alice only knows the private key `inv(pk(alice))`. The key `inv(pk(danish_authorities))` is the private key of the Danish authorities which we assume to never leak, and everybody knows the corresponding public key.

A user can authenticate to a website by sending their passport and signing with their private key a message specifically for that website (containing the website name), e.g.,

```
{ "I accept the terms and conditions of website XY ..." }inv(pk(alice)).
```

This however means that they have to reveal all information from their passport. Before improving the privacy, let us first see about the security of this electronic passport system. Which of the following statements is NOT true?

1. A malicious user can give or sell their passport to other (malicious) users.

2. An attacker who controls the network and a malicious website can impersonate alice after she has shown her passport to the malicious website.

3. It is impossible to revoke passports in this system.

4. This gives non-repudiation/accountability: a malicious user cannot later deny a signed statement they have given to a website

Question 2

To make the above system privacy friendly, we introduce a new role: brokers. We assume all brokers are honest webservers who perform the following job. Now alice can request a credential from a broker b that she is over 18 years old, if she can prove that to b. To that end, alice generates a fresh public/private key pair `(pubk,inv(pubk))` and send the following request to b:

```
{ over18, b, pubk }inv(pk(alice))
```

together with her passport (as described in the previous task). The broker will then issue the credential

```
{ over18, b, pubk }inv(pk(b))
```

where `inv(pk(b))` is the private key of b and everybody knows the corresponding public key `pk(b)`.

Alice can now authenticate to every website as being over 18 without telling her name and precise date of birth by showing this over18-credential and signing a message for the website with `inv(pubk)`.

Which of the following statements is NOT true?

1. Privacy to the broker: A broker knows all details of the passports of the person who applied for the over18-credential.

2. Impersonation: A malicious website cannot use a credential that belongs to an honest user.

3. No linkability: A malicious website who also controls the entire network cannot tell whether two over18-credentials belong to the same or to different users.

4. Revealing via brokers: If a user does something illegal with an over18-credential, then it is technically possible to revoke their anonymity, by the issuing broker revealing the name of the user.

Access Control

Question 1

The table below shows the access control matrix for the shared drive of a HR department.

	Salaries.xlsx	Holidays.xlsx	Bonuses.xlsx	Courses.mdb	Promotions.docx	Sickdays.xlsx
Alice		R		ORW	ORW	R
Bob		R		RW	R	A
Charlotte		ORW				R
David		RW				ORW
Erica	ORW	R	ORW	R	ORW	R
Fred	R	R	R	R		

Access Rights are defined as “O” = Owner, “R” = Read”, and “W” = write, “A” = append.

Alice and Bob works with employee development, Charlotte and David are responsible for day to day staff administration, Erica heads the HR department and is the only person who should be able to access information related to employee finances except Fred who works for the external auditor, so he should be able to audit all payments made to employees.

The following goals have been defined for the access control policy:

A) Alice can read the “Holidays.xlsx” file to check when people are on holidays before registering them for courses.

B) Alice can write the “Promotions.docx” to recommend promotions based on the improved skills profiles employees obtain through continuing education registered in the “Courses.mdb” database.

C) Bob can read the “Sickdays.xlsx” to reschedule courses that an employee has missed because of illness.

D) Charlotte is the only user who can write the “Sickdays.xlsx” file.

E) Employees who can read the “Salaries.docx” file can also write the “Bonuses.xlsx” file.

F) Erica is the only person that can read and write financial information (files “Salaries.xlsx” and “Bonuses.xlsx”) – except Fred who can also read these files.

G) David can delegate registration of illnesses to Charlotte, when he is on holidays.

H) Only company employees should be able to update company data.

Given the access control matrix shown above, which of the security goals are met.

A, B, C, D

A, B, E, F

A, B, F, G

A, F, G, H

Question 2

In the electronic health record system of Saint Luke's Hospital, different staff members are granted distinct access rights as follows:

Chief Surgeon: view all patient records, add surgical notes, edit post-operative care plans.

Staff Nurse: view patient records, record vital signs, administer medications.

Hospital Administrator: manage user accounts, set hospital policies, oversee system-wide settings.

Medical Records Clerk: view all patient records, edit and manage patient documentation.

Emily is tasked with managing patient documentation, ensuring the accuracy and completeness of records. She has the authority to edit the medical documentation in the electronic system. According to the RBAC permissions, what is Emily's role at Saint Luke's Hospital?

Chief Surgeon.

Staff Nurse.

Hospital Administrator.

Medical Records Clerk.

Question 3

A system administrator in a company is responsible for assigning access rights to different employees, as stated in the table below, along with the description of the job each user does.

User	**Job description**	**Access Rights**
Federico	Developer	Write access to source code repository and specific databases.
Mia	Project Manager	Write access to project planning tools and full access to source code and testing environment.
Sofia	Quality Assurance	Write access to testing environment.
Katerina	Marketing	Write access to content marketing tools.

Which user's access rights do not align with the principle of least privilege?

Mia (Project Manager).

Federico (Developer).

Sofia (Quality Assurance).

Katerina (Marketing).

Question 4

Assume you have the role of security administrator for a financial company. This company has lots of private client data. In an effort to improve data security, you designed access control policies for this company. In this context of access control policies, what is the primary objective of a Policy Administration Point (PAP)?

To enforce policies and make choices on access control

To manage the Policy Store by adding, removing, and modifying policies.

To determine whether to grant or refuse access

To give information to the Policy Decision Point (PDP) regarding model parameters, roles, attributes, and constraints.

Authentication

Question 1

Which of these password attacks involves using precomputed tables of hash values to quickly look up and discover passwords?

Brute Force attack.

Rainbow Table attacks.

Dictionary attacks.

MAC Intermediate attacks.

Question 2

An online platform incorporates a unique salt to each user's password before hashing it. The salts are stored in plaintext along with the hashed passwords. Why is the use of salted hashes preferred over a simple hash function?

To mitigate the risk of rainbow table attacks.

To mitigate the risk of dictionary attacks.

To mitigate the risk of brute-force attacks.

To mitigate the risk of man-in-the-middle attacks.

Question 3

Considering the deployment of the biometric system in Techtopia, which operation is likely being employed to grant access to authorized personnel at the central data hub?

Enrolled for Identification: Individuals' biometric data is captured and matched against a database of enrolled users, allowing the system to identify and grant access based on widespread recognition.

Enrolled for Authentication: Users present their biometric data, which is authenticated against pre-stored templates specific to each individual, ensuring access is granted only upon successful verification.

Enrolled for Encryption: Biometric data is utilized in an encryption process to secure sensitive information, safeguarding the data during transmission and storage.

Unenrolled for Identification: The system employs identification without prior enrollment, recognizing individuals based on their biometric data from a larger database.

Question 4

A large company is using a Single Sign-On (SSO) system for authentication across multiple applications. One day, the IT department notices unusual activity on one of the applications.

They suspect it might be a session hijacking attack. Which of the following would be the most effective countermeasure in this scenario?"

Implement multi-factor authentication for the SSO system.

Increase the complexity requirements for user passwords.

Shorten the session timeout values for the applications.

Encrypt all data stored in the applications.

Software Security

Question 1

You have received an email that looks like coming from your bank and says "We have received a request to transfer 1517 Kr. from your account to [some beneficiary] Please click here to reject, if that wasn't you." In a momentary lapse of judgement you click on the link, getting to your bank's website, but with the error message that the specified page does not exist. You call your bank and they tell you to not worry, no transaction went through and you were not logged in to your bank at the time.

Which mitigation may be in place in the bank's system that prevent an attack in this case?

1. The same origin policy

2. The bank uses a challenge response mechanism against CSRF attacks

3. The bank checks http reference tags

4. All user inputs are sanitized by the bank's server

Question 2

Consider the security labels trusted and untrusted, ordered as trusted <= untrusted. The goal is that an attacker who can control untrusted information cannot have any influence on the trusted information. Consider the following code:

```
trusted int x,y;

untrusted int z;

while (x>0){

  y=y*z;

  x=x-1;

}

if (z>3){

  x=y;

}
```

Which of the following statements is correct?

1. There is no violation of the information flow policy, but this is wrong because trusted should be higher than untrusted, i.e., untrusted <= trusted to achieve the goal above.

2. There is an explicit flow violating the information flow policy.

3. There is an implicit flow violating the information flow policy.

4. There is both an explicit and implicit flow violating the information flow policy.

Network Security

Question 1

As a system administrator, how would you decide what resources should be placed in the demilitarized zone?

By assessing the sensitivity of the data on the resource and the necessary access to the resource.

By evaluating the likelihood of said resource being the target of cybercrime.

By considering how often this resource is accessed by internal users.

By analyzing the resource's processing power and memory requirements

Question 2

The overall risk analysis of the ACME Company estimates an expected annual loss of 42 million kroner from identified security vulnerabilities. A survey of different security technologies identify four different technologies that mitigate one or more vulnerability, these are summarized below:

A Managed Security Service costs 15 million kroner to implement, and 12 million kroner each year for the next 5 years to operate. It is estimated to reduce the annual expected loss by 30 million kroner.

An Intrusion Detection System costs 60 million kroner to implement, and 15 million kroner each year to operate. It is estimated to reduce the annual expected loss by 50 million kroner.

An Internal Security Operations Center costs 25 million kroner to implement, and 6 million kroner each year to operate. It is estimated to reduce the annual expected loss by 23 million kroner.

A Demilitarized Zone costs 35 million kroner to implement, and 3 million kroner each year to operate. It is estimated to reduce the annual expected loss by 18 million kroner.

The company wishes to optimize its investment in computer security, so it will only invest in the single technology that provides the best value for money over the next 5 years. Which technology do you recommend?

The Managed Security Service

The Intrusion Detection System

The Internal Security Operations Center

The Demilitarized Zone

Question 3

Consider the use of IoT (Internet of Things) devices in the home. While IoT devices bear many of the same security concerns as software applications connected to the internet do, they are particularly vulnerable in some areas. Which of the following is one of these areas?

IoT Devices are particularly prone to security issues because their often limited processor speeds result in less effective anti-virus measures.

IoT Devices are particularly prone to security issues because security development can vary vastly in quality between producers and network security is often only as strong as its weakest link.

IoT Devices are particularly prone to security issues because their firmware is often based on Linux which is considered less secure than other mainstream operative systems.

IoT devices are particularly prone to security issues, especially social engineering attacks because the nature of their simpler user interface makes it hard for consumers to identify compromised units.

Question 4

What can best help the ACME company identify that their local DNS server has been hijacked by an intruder?

An Intrusion Detection System.

A Firewall.

A Honeypot.

A Security Information and Event Management system.

Question 5

Your local pizzeria has established a website for users to sign up with their email and a password, save previous orders, and search for different pizzas. Unfortunately, the website is vulnerable to security threats due to a lack of protection for input fields and a blind trust in all users.

Which of the following security aspects should the pizzeria consider?

Implementation of the TLS protocol.

Implementation of input validation and sanitizing.

No implementation is needed, as the users are trusted.

Implementation of the Diffie-Hellman key exchange and input length limitation.

Question 6

A company is seeking to enhance its network security in response to cyberattacks. The network security team is considering the deployment of an Intrusion Detection System (IDS). Which of the following statements accurately describes a key difference between Host-based Intrusion Detection Systems (HIDS) and Network-based Intrusion Detection Systems (NIDS)?

HIDS is more suited for detecting external attacks, while NIDS is better for monitoring internal network activities.

HIDS operates at the network layer, whereas NIDS operates at the application layer.

HIDS is deployed on specific hosts, focusing on system calls and application logs of that host, while NIDS monitors and analyzes network traffic.

HIDS requires more network bandwidth, whereas NIDS requires more processing power.

Question 7

An organization installs a honeypot within its network infrastructure. The honeypot is designed to mimic critical systems, data and services. The honeypot detects several unauthorized access attempts and captures potential malware during operation.

What is the primary purpose of this honeypot deployment?

Actively engage with attackers and retaliate.

Encrypt sensitive data to prevent unauthorized access.

Increase network performance by diverting traffic.

Retain and attract attackers for monitoring and analysis.

Question 8

A small engineering firm has contracted a consulting company to help them establish a new security plan after a recent database breach that leaked internal project quoting numbers, the data/information could be used by competitors to undercut their contracts. The consultant first surveyed the business and defined the overall security goals and requirements of the engineering firm, followed by an investigation into the cause of the breach.

The core-issue of the breach was a 20 year old in-house basic SQL database with no sanitation, that allowed access outside the company intranet. The suggested plan defined clearly stated, unambiguous and complete security goals, and explicitly stated that a new state-of-the-art database solution should be implemented (usually used for much larger organisations).

The proposed solution would be extremely costly and every employee would need a USB key-pass for access, making it hard for them to make new quotes on the move and require retraining all employees. The report also included a verification module to ensure that the new implementation would make sure that the old security risk was eliminated and further security risks were minimised.

Some of the senior team in the business receive the report from the consultant, are worried about the acceptance of the new access control measures and decide to schedule a meeting a few months later to discuss a possible implementation.

Half a year after the report was made the business went through another data breach.

Why did the breach happen again, what went wrong? Select the most appropriate answer:

A risk matrix was undertaken by the business in response to the report, and it was found that the cost of the implementation outweighs occasionally losing competitor valuable data. Therefore no action is taken as this may have just been an unlucky incident.

The consultant failed to analyze acceptance due to its restrictive key passes, while also making the proposed system financially unrealistic for the business. While the business did not provide a structure for accountability, commitment and an implementation timeline.

The business did not address the security flaws within their database, they should have retained their in-house approach and simply filter and sanitize their inputs. This would be significantly cheaper for the business.

The business decided that the consultant had failed to provide a complete security plan, as there was no mention of building security improvements and of any solutions to potential loss of power systems. They decided to contract a new company to make a new report, and had to wait a number of months for the report to be finalized.

Question 9

Assume we've got a TOR network made up of 7500 nodes. Over 1500 requests are made every second. 10% of these requests made are illegal in nature, and we seek to unmask the people behind those requests. To unmask a request, we need to be in control of a certain number of nodes. A user's activity can be tracked by performing a time series analysis of the traffic within controlled nodes. Ideally the nodes must lead into and out of the network. How many TOR nodes must we compromise to unmask 100 illegal requests an hour?

102 nodes.

2 nodes.

1 node.

The anonymity of a TOR network cannot be compromised.

Governance

Question 1

A grocery company located in Denmark wants to collect information regarding the habits of its customers to improve the quality of the service and profits.

Which considerations must the company make when determining its data security policies?

Active customer consent is required, and the company must communicate how it collects, processes, and protects customer data in compliance with privacy laws such as GDPR.

Customer consent is not necessary since the company is focused on improving its services based on spending patterns.

Data security policies should prioritize maximizing data collection efficiency without concerning the customers with intricate details about how their purchase data is handled.

The company should focus on implementing the latest technological solutions for data storage and analysis to enhance security.

Question 2

A retail company with 150 employees across three locations are experiencing problem with unauthorized changes to the schedule of their customer service department. The changes are being carried out from within the trusted user base that requires authorized users to authenticate themselves with a password system when they log in. We assume the log-in process to be secure.

You have been tasked with catching the culprit. All employees must be able to see the schedule, but only managers need to be able to change it. Which of the following measure will help you determine who are making changes to the schedule and possibly prevent similar "attacks" in the future?"

Implementing an access log system that logs all accesses and updates to the schedule.

Implement a new password policy that enforces monthly password updates with high complexity requirements.

Implement a VPN on the public network connecting the three locations.

Implement Role Based Access Control.

Question 3

Which component of a security plan involves defining responsibility for maintaining security as the system evolves?

Show continual vigilance.

Policy definition.

Establish baseline.

Identify requirements.

Question 4

Alice, who works in IT at a company, receives an email from presumably the IT department. The email contains information about a potential security breach and urges her to download a security update which is linked. Alice has recently received security awareness training and she notices some irregularities in the email.

Which scenario should Alice be most worried about?

The email is a phishing attack, attempting to make Alice download malware disguised as a security update.

The email is a spear phishing attack trying to gain access to Alice's personal information.

The email is part of a social engineering scheme to persuade Alice to give up confidential company inform when she visits the link to the update website.

The email contains a link to a fake website designed to get Alice to download paid-for software under the pretext of being a free update to already installed software.