**University of Kent**

**May/June 2020**

# **Examination Answer Document**

|  |  |
| --- | --- |
| Exam Paper Release Date and Time | * 19.05.2020 * 10:00 British Summer Time (BST) |
| Exam Paper Submission Date and Time | * 20.05.2020 * 14:30 British Summer Time (BST) |

Before starting this examination, you **MUST enter your Examination Number** above **(double click)**; failure to provide this means your mark cannot be recorded and **you may be awarded a 0 (zero)** for this examination.

|  |  |
| --- | --- |
| Question Number: | 1 |

1a)

In biometrics *Possession* is something which the user physically has that is connected to the system they are trying to connect to. This could be a proximity key-fob that can be used to gain access to buildings or something more general like a mobile phone with an authenticator app used to validate access to an online service.

In biometrics *Inherence* is something that is naturally owned by the individual. This could be any traditional form of biometric scanning like fingerprint scanning, iris or retina scanning, etc.

The possession authentication factor can be difficult to determine whether there has been a security attack. This is because it is hard to establish whether the user has just lost their possession or if it has been stolen. Regardless of this, it would be a simple process to revoke access to whatever device has been stolen, e.g. removing the permissions off a key-fob or an online authenticator. Then it is a simple case of replacing the key-fob or being given access to a new authenticator ID to re-establish the secure connection.

The inherence authentication factor is very, very difficult to compromise without the user noticing. It would require exceptional planning and stealth to create copies of fingerprints, eye details, etc. If this plan was successful though, it would be extremely difficult to determine that an attack had taken place. It would also be difficult to re-establish a secure connection as a user cannot create a new fingerprint or new eyes. If the system featured a fingerprint scanner then after the attack they could switch to an iris scanning system, as a possibility.

1b)

i)

The Diffie-Hellman protocol is a process for allowing two computer-users to generate a shared private key to allow them to exchange information across an insecure channel. This does not require the users to have any prior knowledge of one-another. Anyone eavesdropping on the channel will not be able to determine what the shared key is.

Both members participating in these key-exchange (A and B) both decide on a shared public key. This key would be visible to anyone eavesdropping. This public key is then mixed with an individual private key that both A and B create. A and B both send these mixed keys to each other. Anyone eavesdropping will have no way to ‘unmix’ these messages but now both A and B have a message comprised of both of their private keys and the public key. This means they share the same key, allowing them to decrypt messages. In the Diffie-Hellman protocol, these keys are modular arithmetic values.

ii)

The Diffie-Hellman protocol is vulnerable to man-in-the-middle-attacks as the original protocol features no authentication. This could occur when an attacker (C) intercepts the messages sent between A and B, allowing C to substitute their own key instead of the keys A and B were sending to each other. This would allow C to read any of the exchanges taking place and modify any of the messages before passing them on to A or B. Both A and B would be unaware this attack was taking place.

iii)

Ephemeral Diffie-Hellman protocol differs from the standard DH protocol as it uses new private keys each session to enable forward security. This means that if an attack took place on an exchange, all prior exchanges would be safe as they used a different key. This protocol also doesn’t handle authentication, like standard DH, this means it would be as vulnerable, if not more, to man-in-the-middle-attacks as the original protocol. As new private keys are used each connection, it can be difficult to tell whether the key has been obtained from the intended party, making man-in-the-middle-attacks arguably easier to carry out.

|  |  |
| --- | --- |
| Question Number: | 3 |

A)

i)

A firewall is a form of network security that monitors incoming and outgoing traffic network traffic. The firewall controls this traffic based on a set of pre-determined security rules. Firewalls act as the first line of defence for any computer connected to a network.

ii)

Firewalls are used predominately to prevent unauthorised access to or from a private network and to protect systems from potential threats They are useful for validating access. All messages entering or leaving the local network you are connected to must go through the firewall which ensures that any packets entering or leaving the network are secure. The firewall evaluates whether these messages meets the predefined security criteria. Firewalls can also be used to limit what a user can access from inside the network, e.g. some schools or businesses may block games or social media sites.

b)

One of the main advantages of using a firewall is the extra level of privacy and security it grants the user. Firewalls can be used to block access to user information and data that would otherwise be accessible to anyone listening to the network. Firewalls can also monitor traffic passing through the network, allowing an administrator to access data trends which could prove useful. It also allows an admin to be able to spot discrepancies in the connections which could be an early-warning to an incoming attack.

Another advantage of firewalls is that it can be used to stop attackers gaining access to connect to machines/ports inside of the network. This means that even if a hacker had managed to remotely install malicious software in the system, they would have no way to execute these exploits from outside of the system. This is an example of how effective firewalls can be at reducing the risk of remote code execution. There are still instances or exploits that allow an attacker to bypass a firewall and perform an RCE attack but these are rare.

Setting up a standard firewall for a home-network is a relatively simple and an increasingly automated task. The same cannot be said for commercial firewalls. One of the biggest drawbacks of using a firewall at these commercial levels would be the extensive training and setup times. The more complicated a firewall, the more time it takes to set up and the more highly trained a professional is needed to perform the setup. If the firewall setup is done incorrectly then it can lead to a network that is far less secure than one that had no firewall at all. Firewalls of this scale also require a considerable amount of maintenance and upkeep, meaning a paid professional is usually required on a long-term basis. These factors make enterprise-level firewalls an expensive and somewhat daunting task.

Although it can only be a marginal difference, firewalls can also slow down internet speeds. This is because it has to check every packet going in or out of the network. This means that the larger the number of packets being sent and received, the more noticeable the speed difference will be due to the bottleneck of having to scan a larger and larger volume of packets. Firewalls also have the drawback of occasionally blocking processes the user would wish to go through the firewall. This is especially apparent when a program needs access to listen to a server or a port but the firewall blocks this, meaning the program cannot function properly.

c)

A packet filtering firewall is a firewall that evaluates the incoming packets to determine whether they are allowed access to the network. This packet filtering firewall looks at the source and destination addresses, the source and destination ports and the protocol used to send the packets. This is faster than DPI as it only evaluates the headers of the packet, not the content inside the packet which is faster than the DPI algorithm which does consider packet content.

|  |  |
| --- | --- |
| Question Number: | 4 |

A)

i)

Shift alphabet letters 7.

O - > H

L -> E

S -> L

S -> L

V -> O

Answer = Hello

ii)

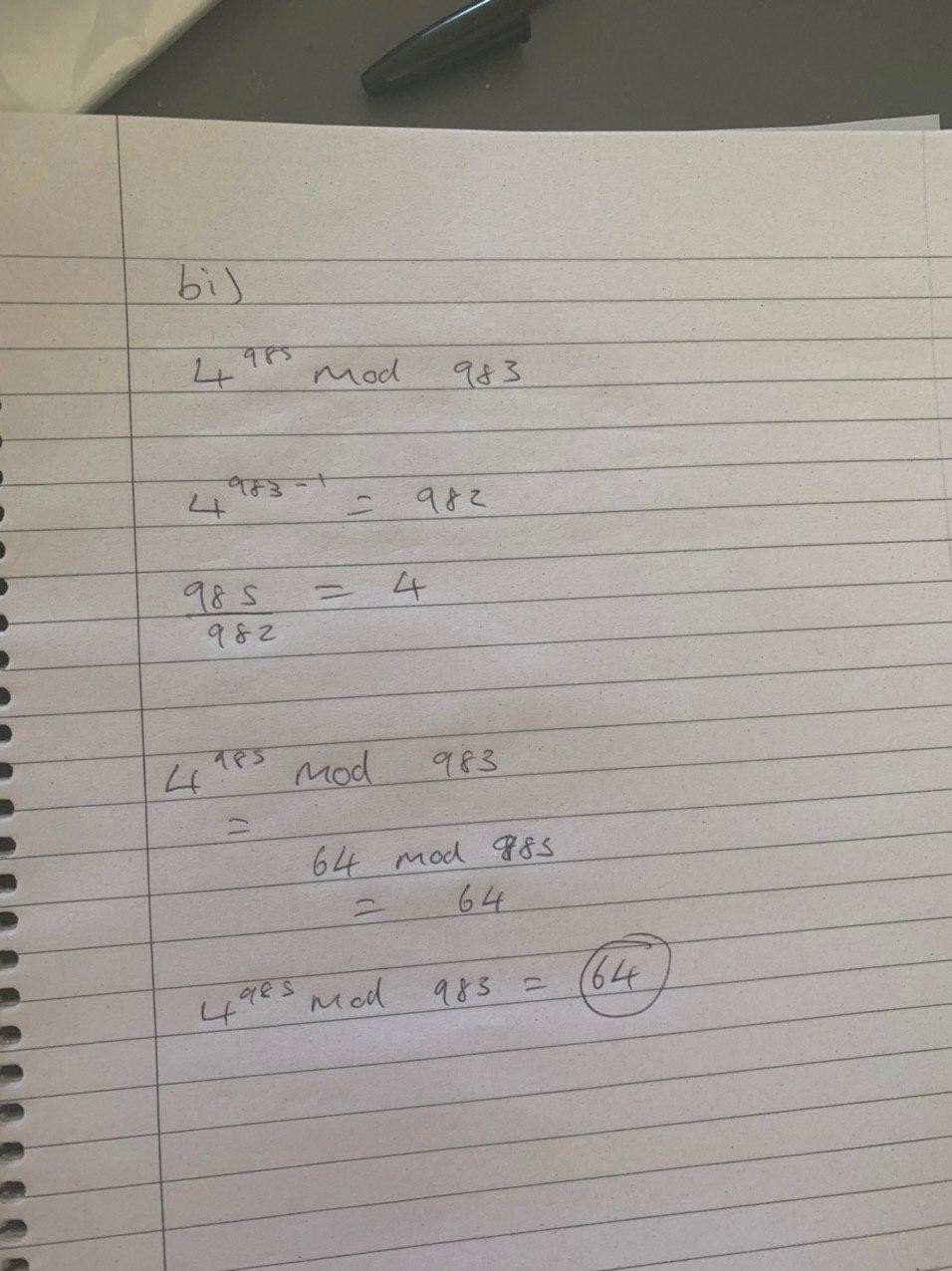
Key = Value

Cipher text = rochf

1. (26 + 17 – 21) mod 26 = W
2. (26 + 14 – 0) mod 26 = O
3. (26 + 2 - 11) mod 26 = R
4. (26 + 5 - 20) mod 26 = L
5. (26 + 7 - 4) mod 26 = D

Answer = World

B i)



B ii)

489733667310 x 871352249115 mod 100 == ((489733667310 mod 100) \* (871352249115 mod 100) mod 100

489733667310 mod 100 = 10 (Remainder of 100, so last two digits)

871352249115 mod 100 = 15 (Remainder of 100, so last two digits)

((15) \* (10)) = 150

150 mod 100 = 50

Answer = 50.

B iii)

3 ^ -1 mod 8 == 1/3 mod 8 = 1/3

B IV)

