NETWORK SECURITY

Answers must be in English.
The contribution of each question to the final mark (100 points) is indicated at the end of each question. A complete and correct answer will get all the points indicated. Partial answers will get only some of the points.
[The final mark will be then normalised base 10, i.e. 80 → 8, 75 → 8, 74 → 7]
To whom it applies, the assignment's mark is added to the total score before the normalization.

1) What is the difference between a block cipher and a stream cipher? [2 points]
Describe in detail how DES can be used to work as a stream cipher. [8 points]

2) Describe in detail how 3-DES works. Why designers have chosen that particular configuration? [6 points]
Why encrypting twice with the same key is not secure enough? [4 points]
Why encrypting twice with two different key is not secure enough? [4 points]

3) Examine the following protocol:

$A \rightarrow T$: A,B
$T \rightarrow A$: $(A,K_{A+},[A,K_{A+}]K_{T-}), (B,K_{B+},[B,K_{B+}]K_{T-})$
$A \rightarrow B$: $[Ks,TA,[Ks,TA]\, K_{A-}]K_{B+}, [A,K_{A+}]K_{T-}$

Where K_{A+} is the public key of A, K_{A-} is the private key of A, K_{B+} is the public key of B, K_{T-} is the private key of T, K_S is the session key and TA is a timestamp.
Is this protocol secure? If not why? [10 points]

4) What is the purpose of a firewall? [3 points]
What is a bastion host? [3 points]
Describe two different firewall configurations, mentioning advantages and disadvantages for each of them [8 points]

5) What is an Access Control List (ACL)? [3 points]
What is a capability? [3 points}
For which system ACLs are the best mechanism to implement access control and why? [4 points]
For which system capabilities are the best mechanism to implement access control and why? [4 points]
Describe which mechanism is used in Unix and how it is used? [4 points]

6) Some public-key algorithms are usually used in combination with hash functions to generate digital signatures, why? [4 points].
Why is it essential for hash functions to be collision free and one-way to be used in generating digital signatures with legal value? [8 points]

7) Why do digital signatures need to be timestamped? [6 points]

A wants to send a timestamped digital signature to B. Describe in detail a protocol she can use to achieve this goal. [10 points]

8) Let us assume a system with the following security labels and subjects:

Object	Current Labels
Pointy Object	SECRET (NUCLEAR)
Shaved Poodle	TOP SECRET (NATO, NUCLEAR)

Subject	Current Clearance
Moe	
Curly	

The system follows the Bell-LaPadula model so implementation must allow read-down and write-up.

Which clearance must Moe have to be able to write Pointy Object? [3 points]
Which clearance must Curly have to be able to read Shaved Poodle? [3 points]