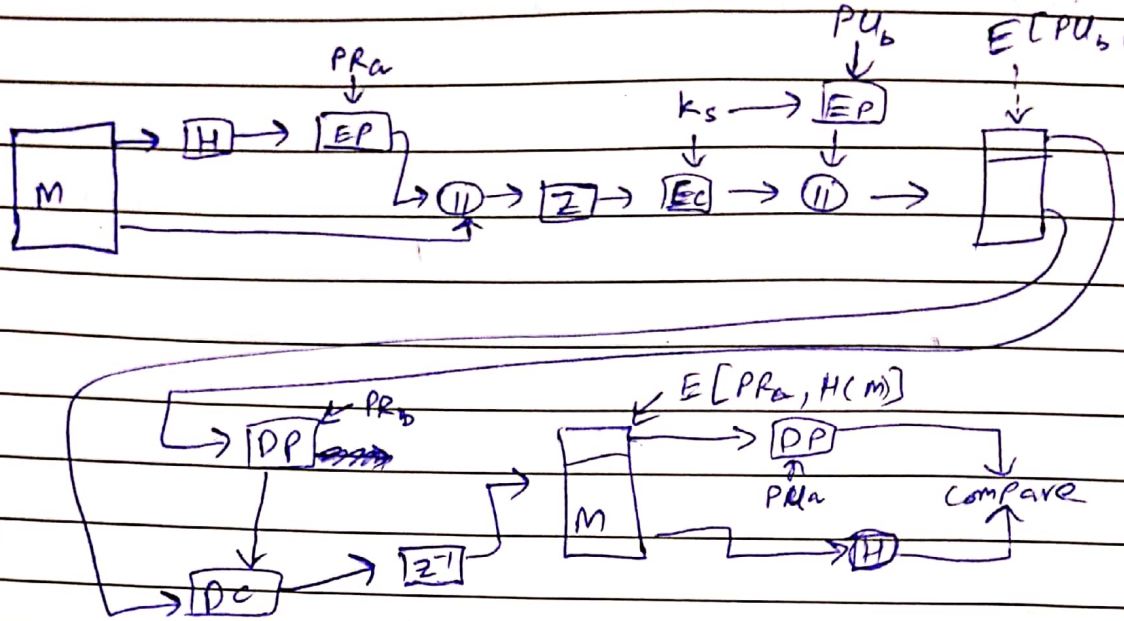
M. Wajahat Ali Khan 16L-4010

day / date

NS - Final Exam (BCS - 8A)

Q1 (a)



⇒ For authentication hashing would be used. The hash of the message is computed then encrypted with the private key of the user. When the message reaches the destination it will decrypt it using public key of user and compare the hash value with the again computed hash of message.

⇒ For confidentiality asymmetric encryption would be used. After the hash appended with message is compressed then it is encrypted with the session key and the session key itself is encrypted by the public key of the destination so that only the destination that has the specific private key can decrypt it

⇒ For encryption RSA will be used because computing prime factors of such large numbers is not feasible given the time or computation resources for someone

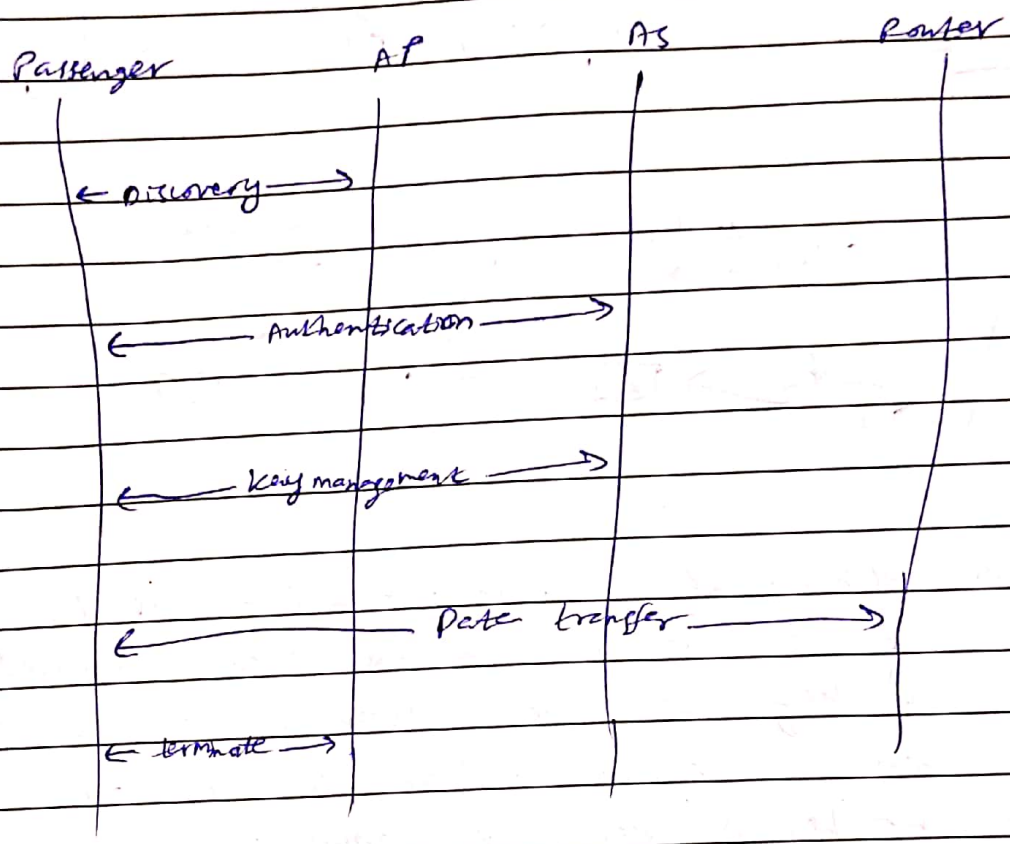
⇒ For hashing SHA-2 would be used. This is because that SHA-1 has already been broken and there are concerns about its

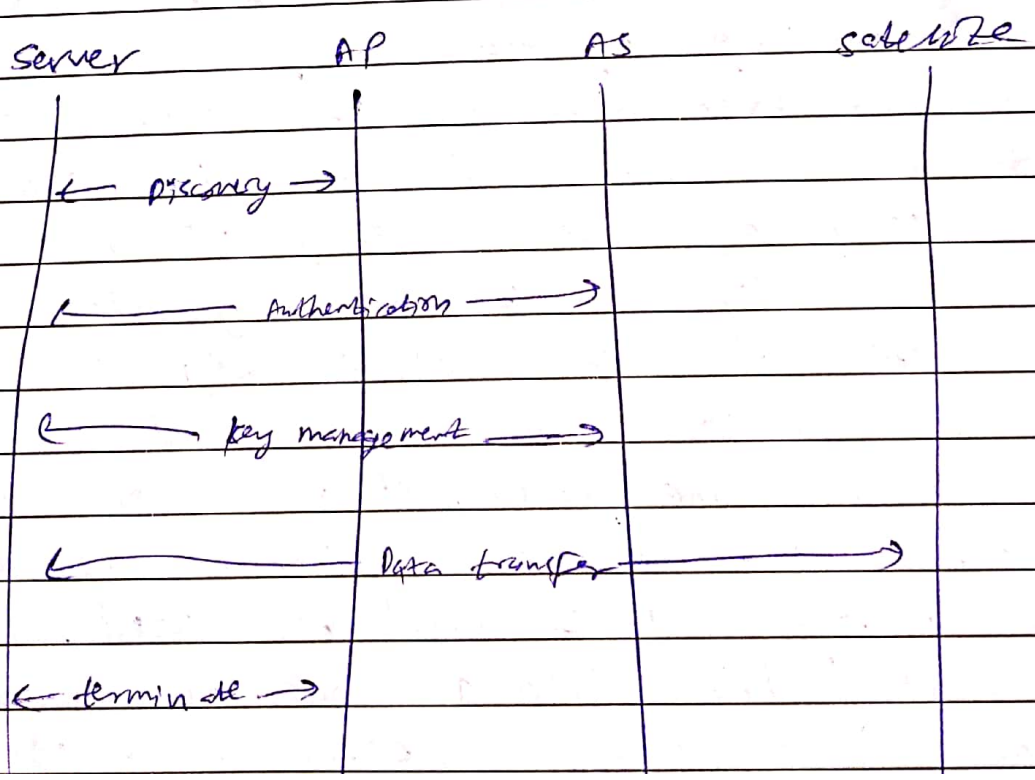
M. Wajahat Ali Khan 16L-4010

day / date

safe or unbreakable nature.

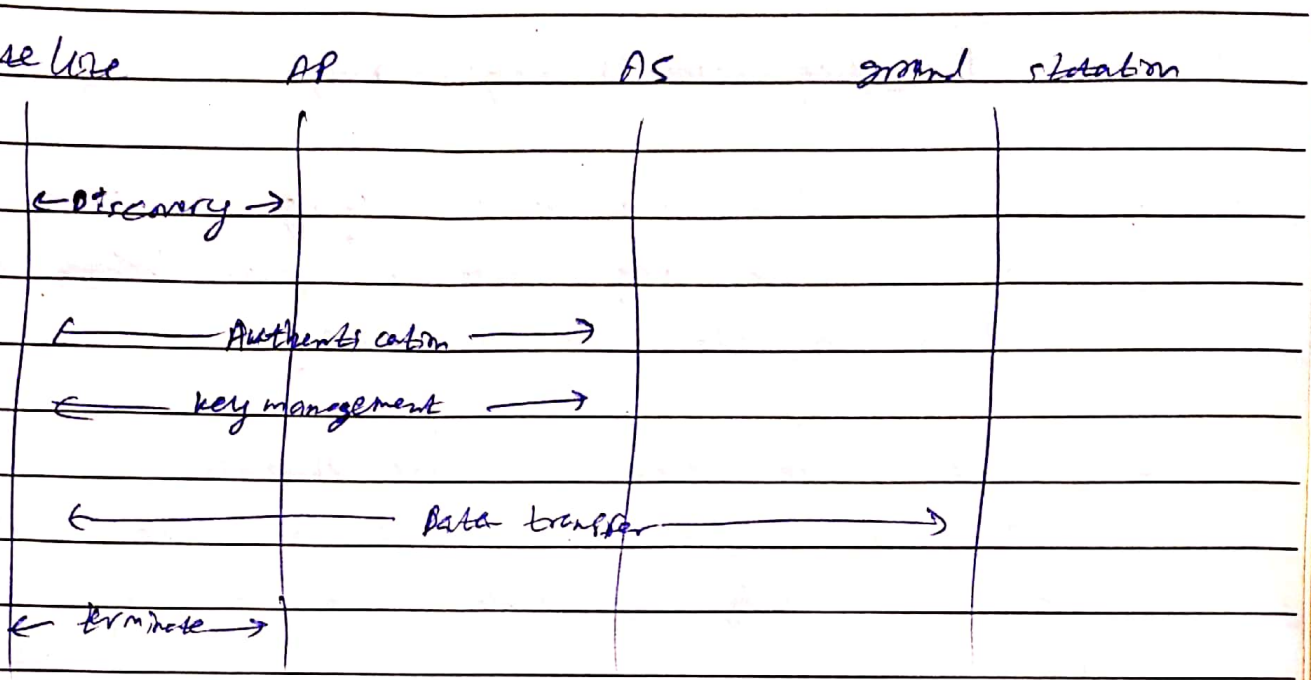
Q1 (b)





M. Wajahat Ali Khan 16L-4010

day / date



Q1 (c) As now the computation has been halved so instead of RSA, AES can be used for encryption as it is much faster than RSA. The key that will be generated by AES can then be encrypted by RSA for greater security as well as keeping in mind the computation resources. One more change that can be done is that instead of SHA-2, SHA 3 can be used that is not only much more secure than SHA2 but also much faster. Also there is compression being done that now need not to be done as now limited computation resources are available.

M. Wajahat Ali Khan 16L-4010

day / date

Q2(a) For Requirements engineering.

(1) Specify functional requirements employing use cases
- To know the requirements in depth looking at each entity in the system properly.

(2) Specify abuse cases and model threats
- To know beforehand what are the possible threats so to be ready to tackle them at any moment.

(3) Perform risk analysis on threats
- It is important as we should know beforehand that how much damage each threat can cause.

(4) Specify security requirements to mitigate threats
- It is important as to prevent those threats some requirements are needed.

(5) Select security mechanisms for security requirements
- It is important as to know which mechanisms will be used for those security requirements chosen

(6) Specify functional requirements for selected security mechanisms
- To make sure those mechanisms are implemented properly

(7) Assess security index
- To get a value of how secure the system is to be sure if more work is needed or not on the security.

M. Wajahat Ali Khan 16L-4010

day / date

(8) Perform inspections on the completed requirements specifications
- To check if the specifications are correctly setup

For Design Phase

(9) Construct detailed design
- To know the system in detail to access the requirements are addressed properly

(10) Perform design inspections
- To know or identify any security vulnerabilities in the design

(11) Remove security vulnerabilities in design
- To remove the defects in design identified in previous step

(12) Assess if another round of design inspections is required.
- To be sure if the design is perfect to be forwarded towards the next step

(13) Design specification-based embedded security monitor
- To monitor any security breaches or threats based upon the design to quickly fix it

(14) For Implementation, ~~Assurance~~ Security ~~and Maintenance phase~~

(14) Select a secure programming Language
- To be sure that programming language not cause to be a threat

Finally Biro

day / date

(15) Following secure coding standards and guidelines
- To be sure coding does not create any threat to the software or system

(16) Unit testing
- to be sure that each unit is doing what it is intended to do

For Assurance Phase

(17) Code inspections and static analysis
- Important as to check for errors in code

(18) Generating test cases
- To be sure each and every condition is being checked without leaving any surprise or new inputs.

(19) Integration, acceptance, and penetration testing
- To be sure that software is working and is acceptable to the user

(20) For Maintenance Phase

(20) Observe softwares behaviour for deviations from specifications
- To check if any vulnerabilities exist

(21) Locate vulnerabilities for identified deviations
- To remove them they need to be located first

(22) perform rework to remove vulnerabilities
- Important as to be sure that the software does not contain any vulnerabilities or threats

Finally Biro

M. Wajahat Ali Khan 16L-4010

day / date

Q2 (b) The activity of access if another round of design inspections is required is not needed if the budget is cut in half. This is because one design inspection is enough as in previous steps enough requirement specifications have already been specified that will already reduce any threats, and those that are still left can be caught in further steps when testing and monitoring is being done. Second activity that can be removed is that to select a secure programming language. This activity is not the most important one as even if the programming language is not secure further steps that include testing and fixing of vulnerabilities can take care of it. Another activity that can be removed is that of unit testing as integration and other types of testing are already done and any defect can be caught in those testing techniques.