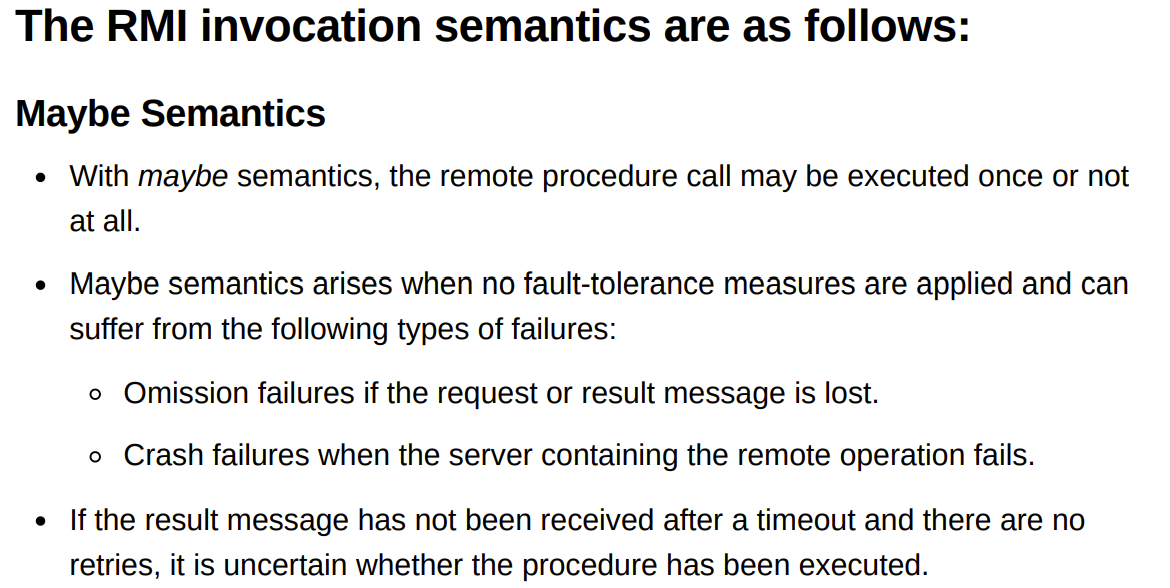
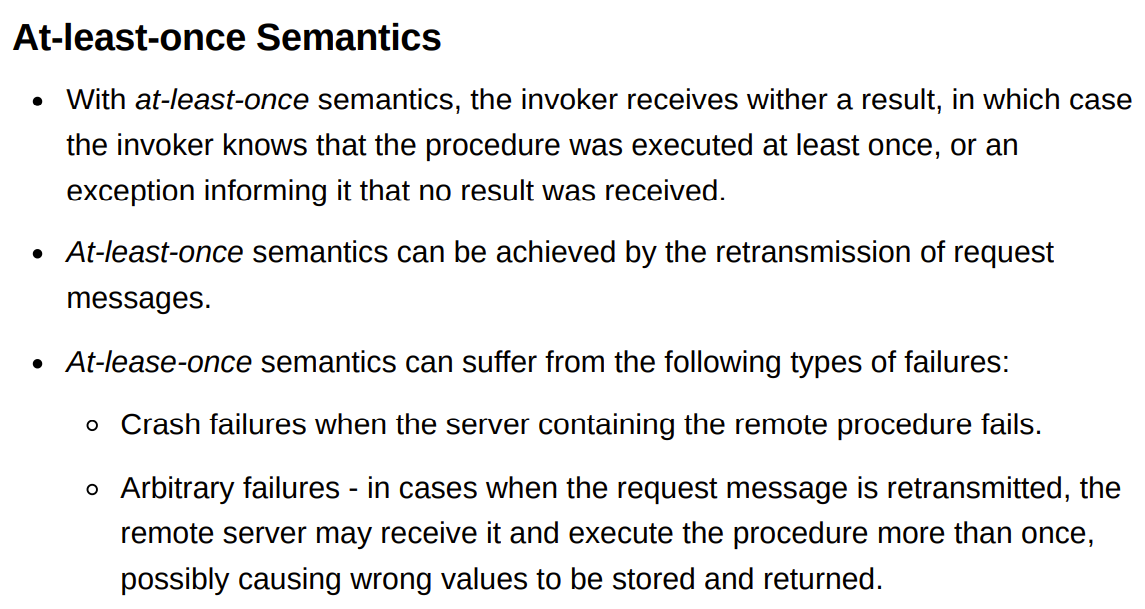
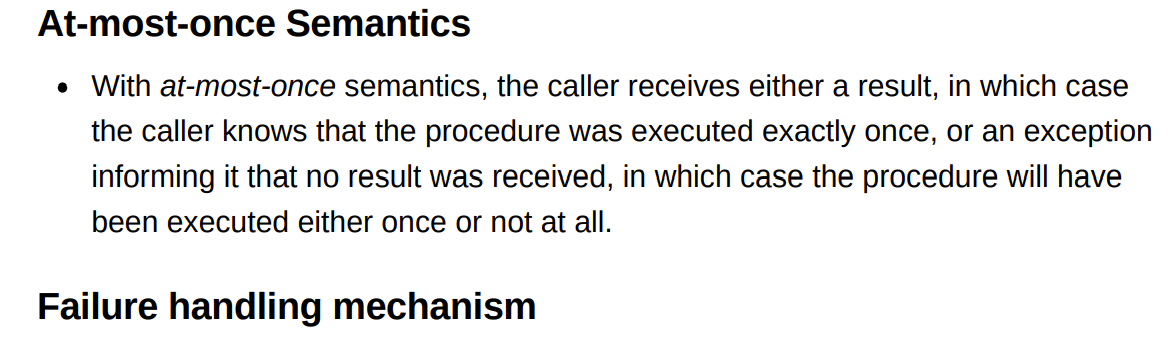
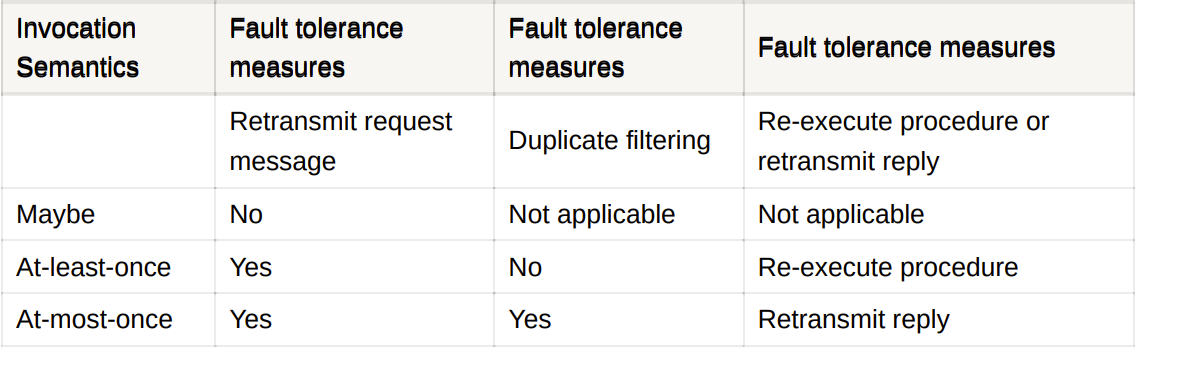
**Question Bank – IA 2**

1. **Discuss RMI invocation semantics and tabulate failure handling mechanism for each.**

****

****

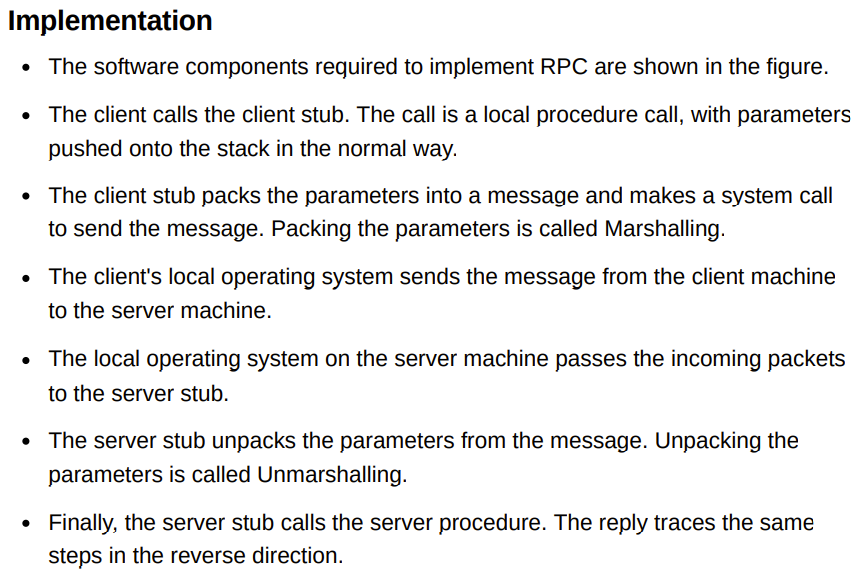
****

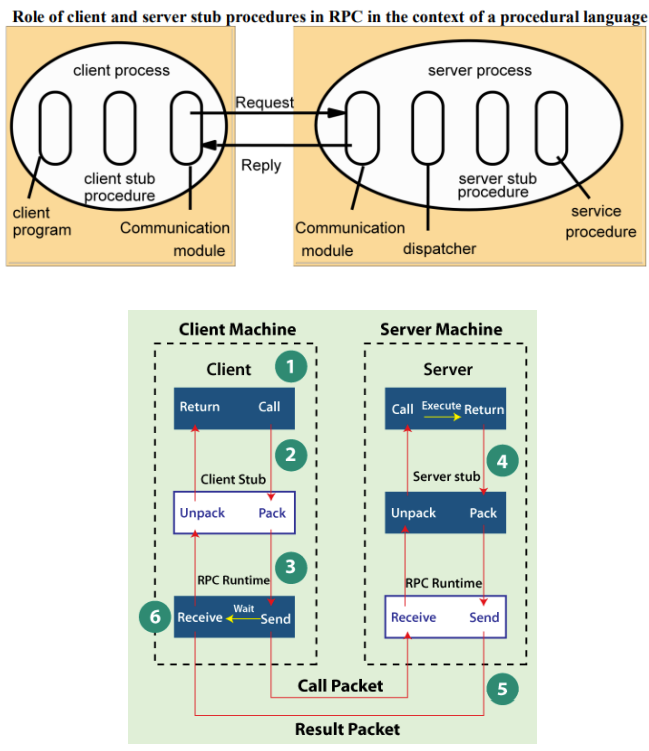
****

1. **Define RPC and With neat diagram explain its implementation**

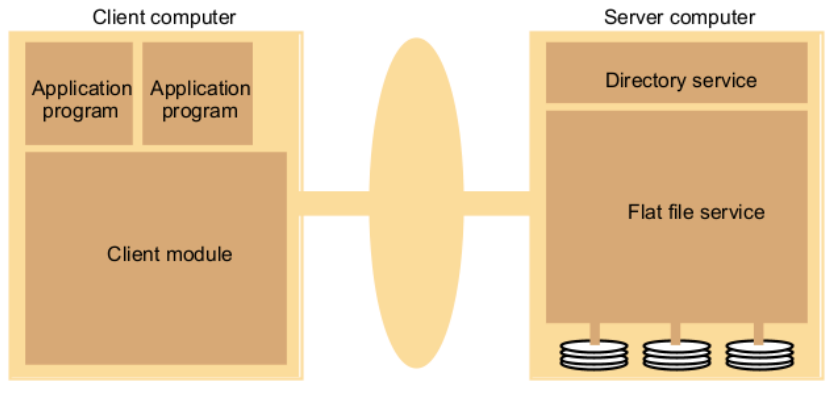
The Remote Procedure Call (RPC) is a protocol that one program can use to request a service from a program located in another computer in a network Distribution Object and RMI 7 without having to understand network details.

An RPC is analogous to a function call. Like a function call, when RPC is made, the calling arguments are passed to the remote procedure and the caller waits for a response to be returned from the remote procedure.

****

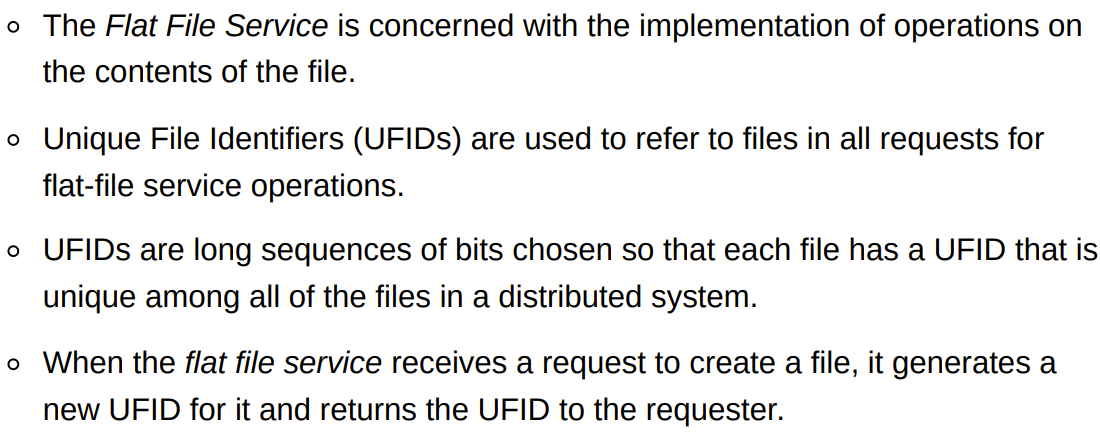
****

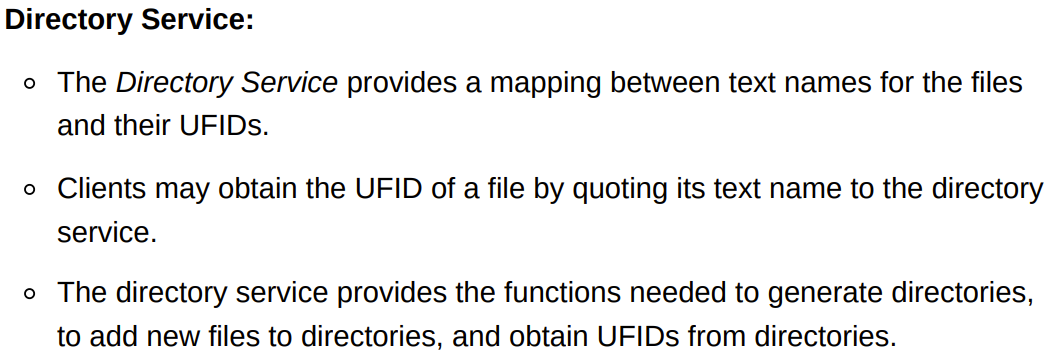
1. **Discuss model architecture of distributed file system and its components.**

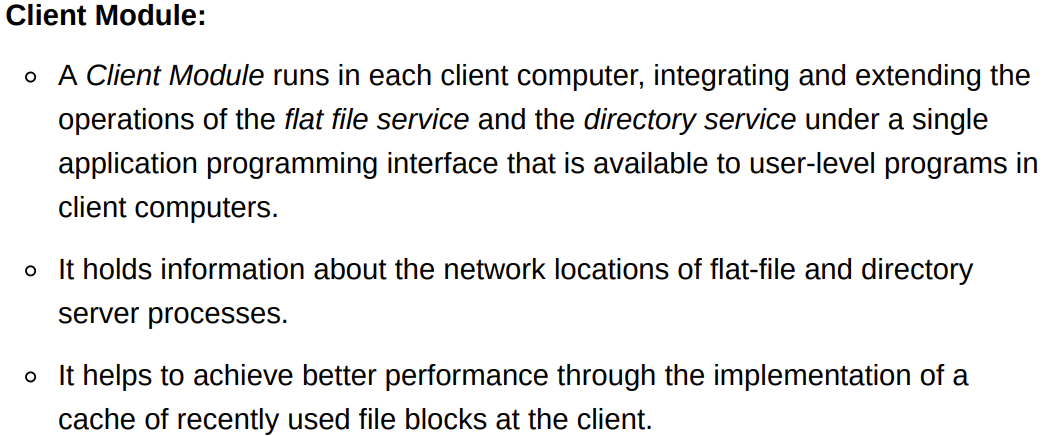
****

File service architecture is an architecture that offers a clear separation of the main concerns in providing access to files is obtained by structuring the file service as three components:

**Flat File Service:**







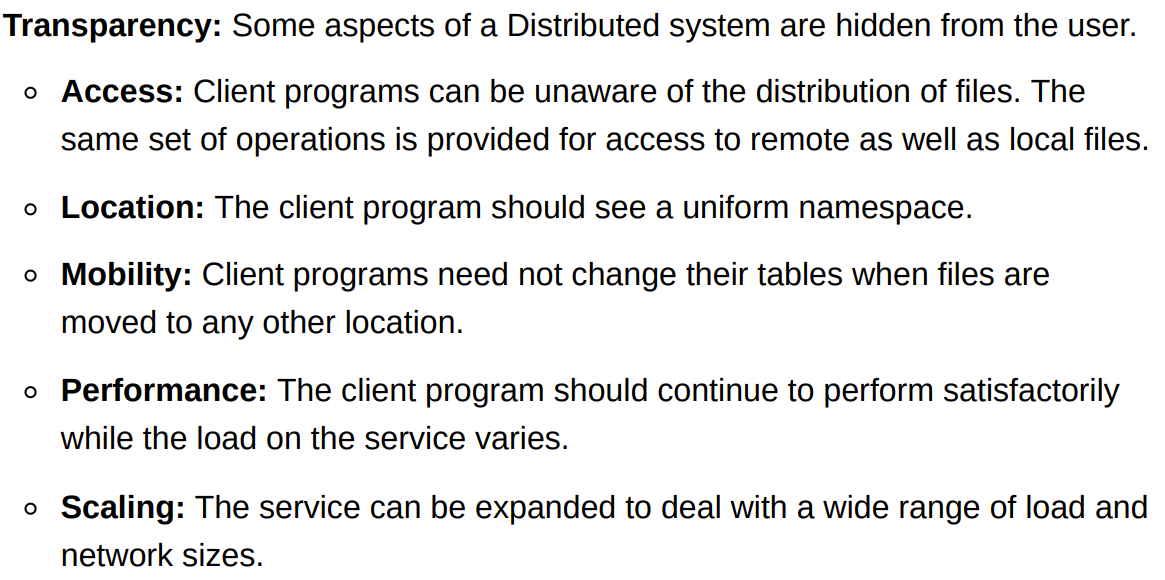
1. **List the various Distributed File Requirements and explain any three in detail.**

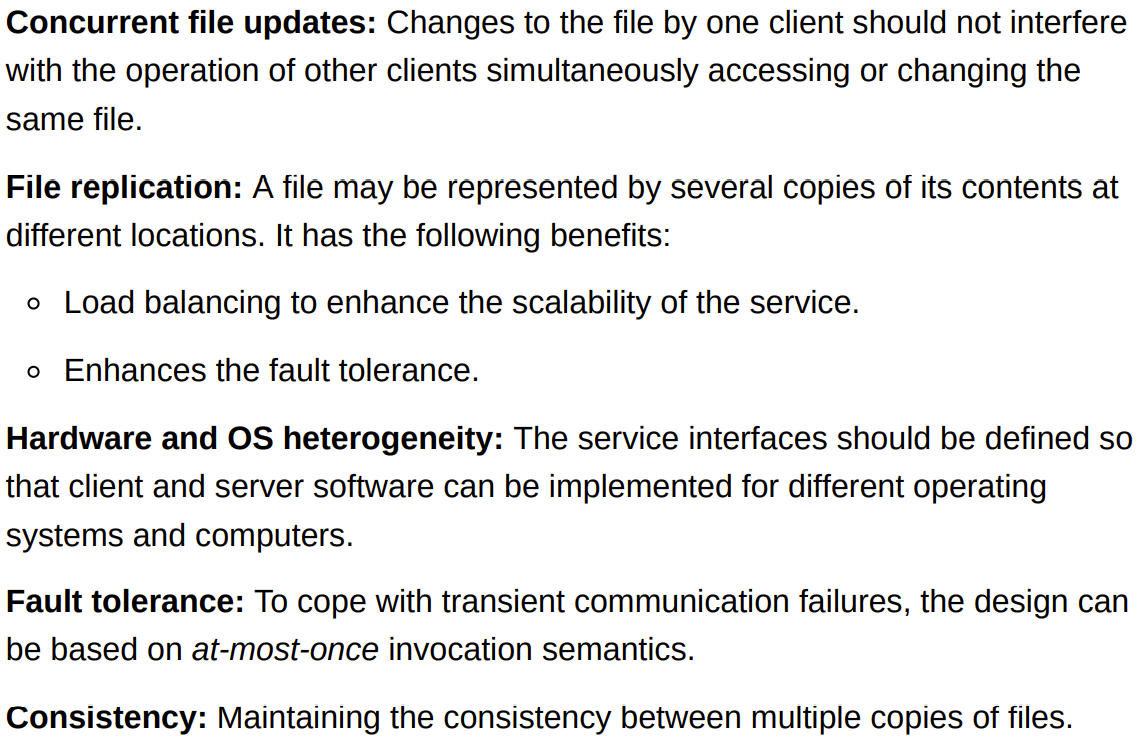
[SAME AS 6]

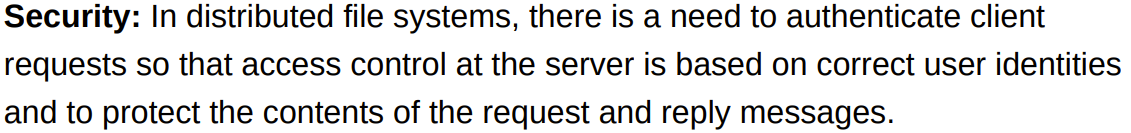
1. **With a neat diagram explain the components of file service architecture in brief w. r .t. following; i) Flat File Service ii) Directory Serviceiii) Client Module**

[SAME AS 3]

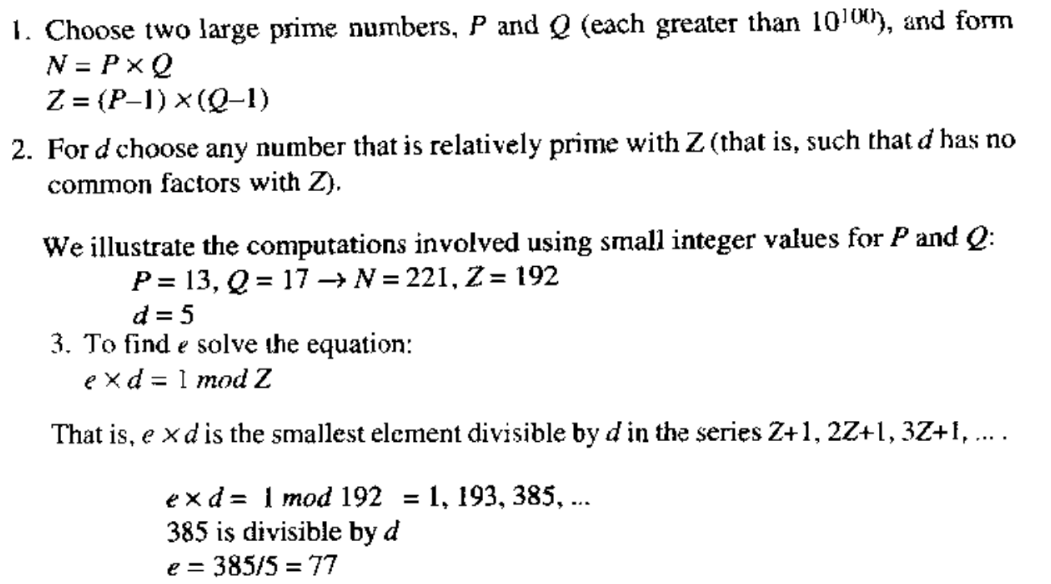
1. **Discuss the distributed file system design requirements.**

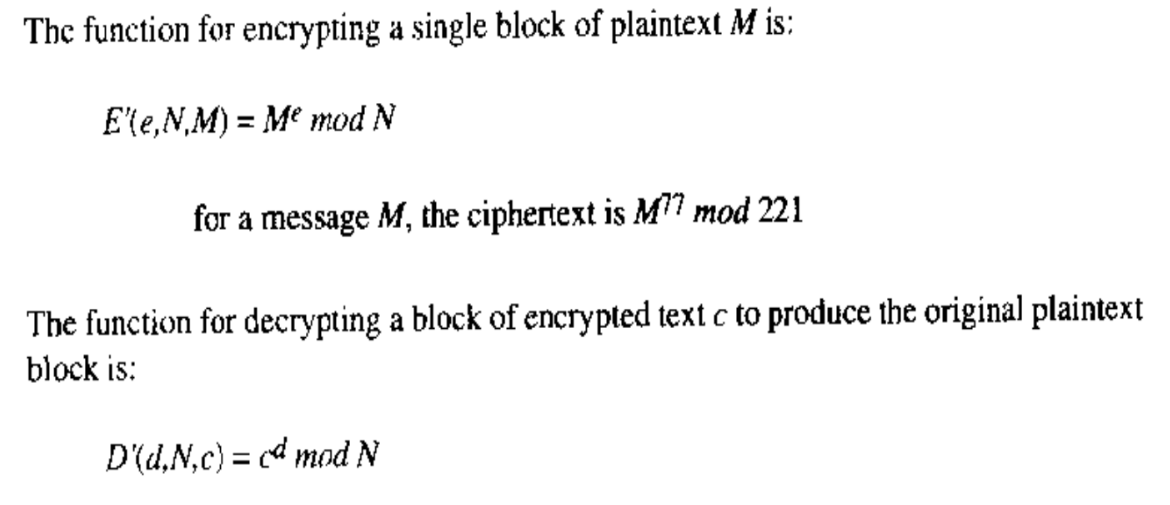
****

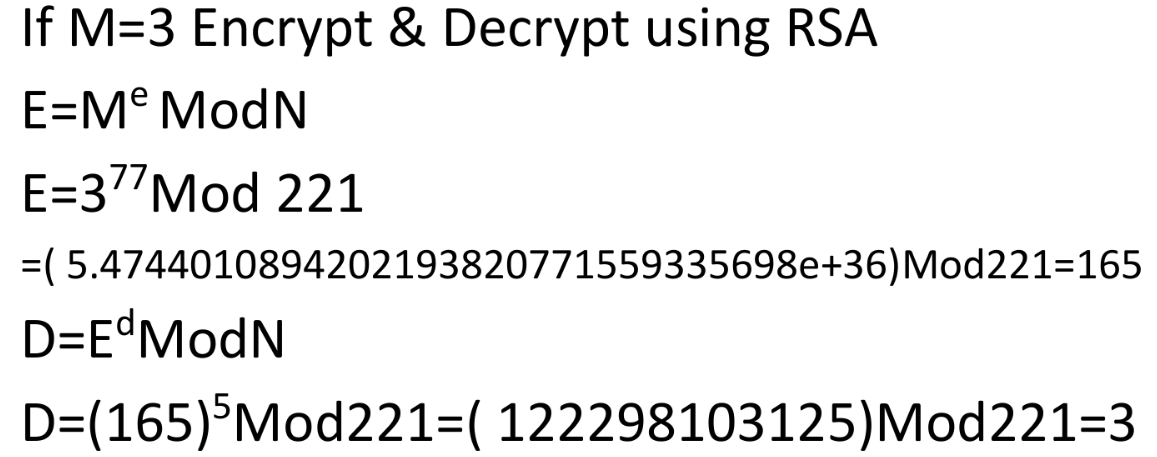
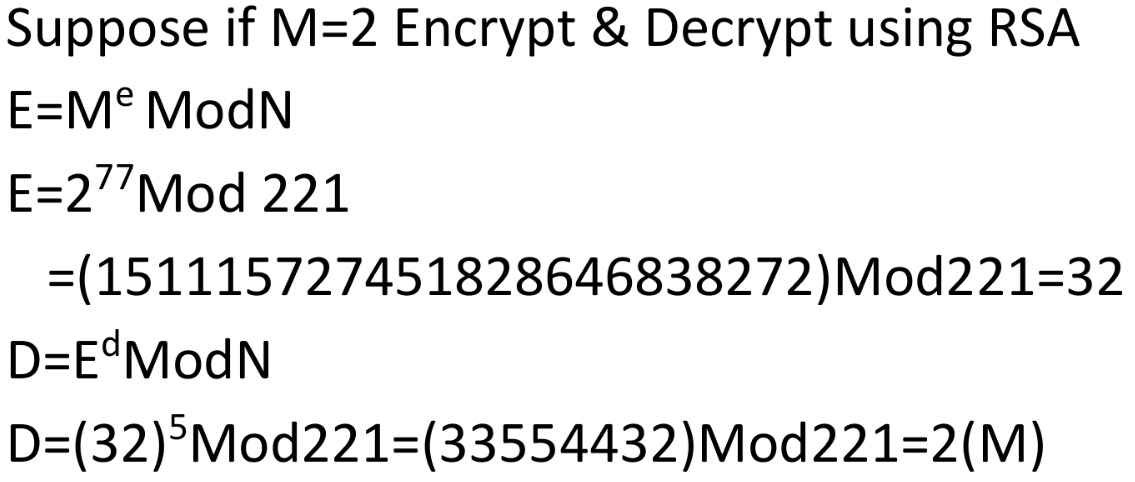
****

****

1. **Write the steps of RSA Algorithm. Illustrate with an example given Message = 8, P=3 & Q=11.**

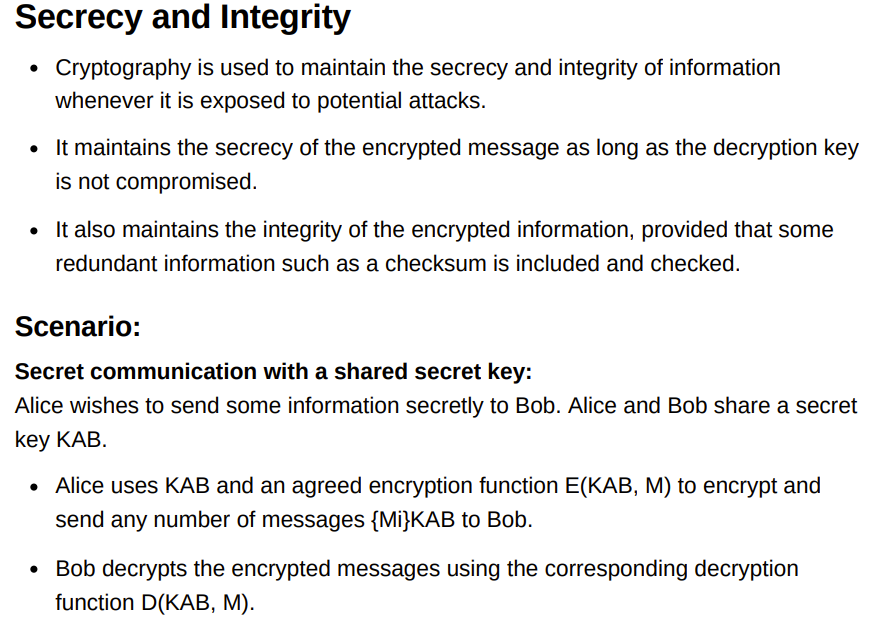
****

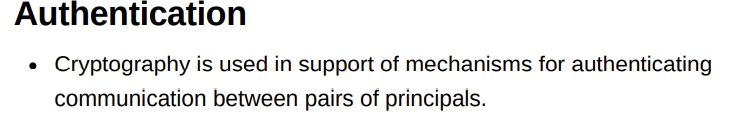
****

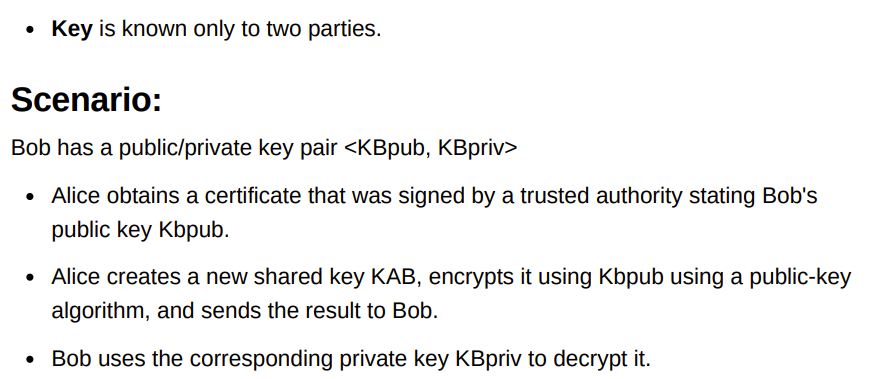
****

1. **Analyze the following uses of Cryptography with suitable scenarios.**

**i) Secrecy and integrity ii) Authentication**

****

****

****

1. **Discuss asymmetric (public/private key pair-based) cryptography technique and how it can be used in supporting security in distributed systems.**

When a public/private key pair is used, one-way functions are exploited in another way. The feasibility of a public-key scheme was proposed as a cryptographic method that eliminates the need for trust between communicating parties. The basis for all public-key schemes is the existence of a trap-door function. A trap-door function is a one-way function with a secret exit- it is easy to compute in one direction but infeasible to compute its reverse unless the secret is known. The pair of keys needed for asymmetric algorithms are derived from a common root. The derivation of the pair of keys from the root is a one-way function. In the case of the RSA algorithm, the large numbers are multiplied together, this computation takes only a few seconds, even for very large primes used. The resulting product, N, is computationally infeasible to derive the original multiplicands. One of the pair of keys is used for encryption. For RSA the encryption procedure obscures the plaintext by treating each block as a binary number and raising it to the power of key, modulo N. The resulting number is the corresponding ciphertext block. The size of N and at least one of the pair of keys is much larger than the safe key size for symmetric keys to ensure that N is not factorizable. For this reason, the potential attacks on RSA are small, its resistance to attacks depends on the infeasibility of factorizing N

1. **Explain following symmetric key encryption techniques i) Block cipher ii) Stream cipher**

**SKIP KARO ISSE! Chodde!**

1. **Write a note on digital signature?**

