

Why use 2PC?

Achieves coordination among all involved parties. In order to prevent everything coming to a halt, the process should abort if it all times out.

However, messages can get lost or nodes/coordinator can crash. Timeouts and other strategies address this problem.

Why use Base64?

Prevents corruption during transmission and ensures that all 64 characters are safe for transmission across all media.

RMI: registry, stub

Registry maps names to remote objects. Objects must be added to the registry so that way they can be found.

Stub provides an interface for an object. It appears local but actually loads the object and handles the network communication for the calling process.

Message Integrity attempts to guarantee that whenever a message has been tampered with this is immediately and easily recognized. ~~The~~ The message is then rejected.

DES uses 64-bit blocks and is now insecure and inefficient, while AES uses a ~~minimum~~ minimum of ~~128~~ 128-bit and up to 256.

MAC is only used to help identify if a message was tampered with during transmission, it is not encryption.

Best solution: Encrypt then MAC \rightarrow protects ciphertext and thereby ~~also~~ ^{also} plaintext.