Secure Shell, or SSH, is a cryptographic (encrypted) network protocol to allow remote login and other network services to operate securely over an unsecured network.[1]

SSH was designed as a replacement for Telnet and for unsecured remote shell protocols such as the Berkeley rlogin, rsh, and rexec protocols. Those protocols send information, notably passwords, in plaintext, rendering them susceptible to interception and disclosure using packet analysis.The encryption used by SSH is intended to provide confidentiality and integrity of data over an unsecured network, such as the Internet, although files leaked by Edward Snowden indicate that the National Security Agency can sometimes decrypt SSH, allowing them to read the content of SSH sessions

SSH provides a secure channel over an unsecured network in a client-server architecture, connecting an SSH client application with an SSH server.Common applications include remote command-line login and remote command execution, but any network service can be secured with SSH. The protocol specification distinguishes between two major versions, referred to as SSH-1 and SSH-2.

The most visible application of the protocol is for access to shell accounts on Unix-like operating systems, but it sees some limited use on Windows as well. In 2015, Microsoft announced that they would include native support for SSH in a future release.

https://en.wikipedia.org/wiki/Secure\_Shell

https://okeanos.grnet.gr/support/user-guide/cyclades-what-are-ssh-keys-and-how-can-i-use-them/