The Three Pass Protocol is a key exchange protocol in the Diffie Hillman, that establishes secret keys.

History

The development of The Three Pass Protocol was a significant milestone in the history of cryptography. Before secure key exchange required a pre-shared key or a trusted third party. The protocol allowed for secure key exchange without the need for a pre-shared key or trusted third party.

Encryption Process

The Three Pass Protocol involves three passes or steps:

1. The two parties agree on a large prime number and a generator of a finite field. Each party then chooses a secret value and computes a public value based on the chosen prime, generator, and secret value using modular exponentiation.

2. Each party sends its public value to the other party. They then use the received public value and their own secret value to compute a shared secret value using modular exponentiation.

3. Each party sends a message to the other party that is encrypted using the shared secret key obtained in the second pass. This ensures that the communication is secure.

Security

The Three Pass Protocol provides a secure method for two parties to exchange secret keys without the risk of interception. The security of the protocol is based on the difficulty of solving the discrete logarithm.

While The Three Pass Protocol is a proven and effective method for secure key exchange, it has some limitations.

-The protocol assumes that no one is following each phase. The protocol does not provide authentication, which means that there is a risk of man-in- the-middle attacks.