Diffie-Hellman/Schannel Provider Algorithms

- Article
- 01/08/2021

The purpose of the Diffie-Hellman algorithm is to make it possible for two or more hosts to create and share an identical, secret encryption key, by simply sharing information over a network that is not secure. The information that gets shared over the network is in the form of a couple of constant values, and a D-H public key.

The Microsoft *Diffie-Hellman*/*Schannel* Cryptographic Provider supports the following algorithms.

Algorithm ID	Description	Comments
CALG_DH_SF	Diffie-Hellman store and forward *key exchange algorithm*	Key length: Can be set, 384 bits to 512 bits in 8 bit increments. Default key length: 512 bits.
CALG_MD5	MD5 hashing algorithm.	Provided only for hashing.
CALG_DH_EPHEM	Ephemeral D-H key exchange.	Key length: Can be set, 384 bits to 512 bits in 8 bit increments. Default key length: 512 bits.
CALG_SHA	SHA hashing algorithm.	Must be used for DSS signatures.
CALG_RC2	RC2 block encryption algorithm	Key length: 40 to 88 bits.
CALG_RC4	RC4 stream encryption algorithm	Key length: 40 to 88 bits.
CALG_CYLINK_MEK	DES variant encryption algorithm	Key length: 40 bits.