Diffie-Hellman Key Exchange

The potential of public-key encryption was discussed in the paper, “

New Directions in Cryptography”by Whitfield Diffie and Martin Hellman in 1976. Public-key algorithms represented arevolutionary change to how encryption had been done to date.The Diffie-

Hellman protocol also heavily relied on the work Ralph Merkle did in public key distribution. It has been suggested by many people including Hellman that the protocol would be better named, “Diffie-

Hellman-Merkle”.

The patent for the key exchange (4,200,770) lists Diffie-Hellman Merkle as the inventors

The Diffie-Hellman key exchange protocol allows two parties to securely exchange “a secret” (i.e. a secret key) over an insecure communications channel. This key can then be used for whatever its intent is, but typically the “secret” exchanged is a “secret key” used in the symmetric encryption for a larger amount of data. This

Key exchange protocol fills a void in the symmetric key implementation of securely distributing the secret key.

Note that the Diffie-Hellman key exchange is an unauthenticated exchange protocol and is not an encryption algorithm.

Symmetric encryption uses the same key to encrypt and decrypt messages. The encryption and decryption of messages is implemented by various algorithms (DES, 3DES, AES, etc.) that direct the manipulating of the bit representation of the message

that results in various substitutions and transpositions

of the message. With public-key (asymmetric) encryption there

are two keys: a public key and a private key. The public key

is generally made available to a person that isto receive/send

communications to/from the person that possesses the private key. The private key is securely kept by one party who can send/receive messages to a party that possesses the public-key.

The two keys, private and public are linked together mathematically such that a message encrypted/decrypted with one key can be encrypted/decrypted with the other key.