

# Diffie-Hellman (DH) Key Exchange protocol

The Diffie-Hellman algorithm is based on the principle that:  $(x^a)^b$  and  $(x^b)^a$  are both equivalent to  $x^{(a*b)}$

The overall IPsec key management framework is **Internet Security Association and Key Management Protocol** or **ISAKMP** from **RFC 2408**. Within that framework is the Internet Key Exchange, IKE, protocol in **RFC 2401**. IKE relies on yet another protocol known as OAKLEY and it uses **Diffie-Hellman** as described in **RFC 2412**.

It is typical practice to use a symmetric system to encrypt the data and an asymmetric system to encrypt the symmetric keys for distribution.

DH is a mathematical algorithm that allows two remote sites to generate an identical shared secret, even though those systems may never have communicated with each other before. The shared secret can then be used to securely exchange a cryptographic encryption key. This cryptographic encryption key then encrypts application data traffic between the two remote sites.

Diffie-Hellman is not an encryption mechanism as we normally think of them in that we do not typically use it to encrypt data. Instead, it is a method to **securely exchange the keys that encrypt data**.

Diffie-Hellman accomplishes this secure exchange by creating a **"shared secret"** (sometimes called a "Key Encryption Key" or KEK) between two devices. The shared secret then encrypts the symmetric key for secure transmittal. The symmetric key is sometimes called a **Traffic Encryption Key (TEK)** or **Data Encryption Key (DEK)**. Therefore, the KEK provides for secure delivery of the TEK, while the TEK provides for secure delivery of the data itself.

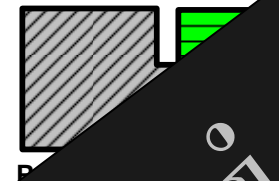
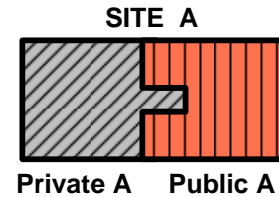
The process begins when each side of the link generates a private key and each side then generates a public key, which is a derivative of the private key. The two sites then exchange their public keys. Each side's communication now has their own private key and the other sites public key.

Noting that the public key is a derivative of the private key is important – **the two keys are related**. Note, in order to "trust" this remote site, you must accept that you cannot disclose the private key to the public key.

Once the key exchange is complete, the process continues. The Diffie-Hellman "secrets" – identical cryptographic key shared by each side of the communication. By running the mathematical operation against your own private key and the other's public key, they also generate a value. The important point is that the "Shared Secret" that can encrypt information between the two sites.

In most real applications of the Diffie-Hellman protocol, the shared secret **encrypts a symmetric key** for one of the sites to use to encrypt data securely, and the distant end decrypts it with the same symmetric key.

Which side of the communication generates the shared secret is most common for the initiator of the communication.



COPYRIGHT  
©ITcharts.com

Diffie-Hellman "Oakley" Group 1 (modulus 2^768 - 2^704 - 1 + 2^64 \* { [2^638 pi] + 149686 } )  
during the key exchange  
bits, Group 2 (modulus 2^768 - 2^704 - 1 + 2^64 \* { [2^638 pi] + 149686 } )  
If mismatched, the generator is not a primitive root of the modulus.  
generator is not a primitive root of the modulus.  
more...