IPSEC (Internet Protocol Security) Made up of several sub-protocols:

AH: Provides Authentication and Integrity. To provide integrity, AH uses an ICV (Integrity Check Value), which is essentially the same as a Message Authentication Code (provides system based, aka data origin authentication). This integrity check is performed on the whole packet, not just the data. This ensures that neither the data nor headers/trailers have been altered. This can cause problems with NAT.

ESP (Encapsulating Security Payload) provides encryption, authentication, and integrity checking on just the payload, so it is compatible with NAT.

IPSEC can operate in transport or tunnel mode.   
Transport mode is used for securing communications between end users on a network. Just the payload is encrypted.

Tunnel Mode is for securing WAN communication. Data, headers, trailers encrypted.

An SA (Security Association) functions in a manner similar to a socket. It tracks each secured session and contains information about that session and allows multiple IPSec connections to/from the same system. Each connection has two SA’s, one on each end. Computer A will have an SA to identify connection1 to Computer B—that SA might be called “1234”. Computer B will have an SA to identify it’s session with Computer A. That SA could be called “4321”. The point is, though the SA is known by different “names” on each computer, it’s really identifies the one connection.

There are two ways IPSEC manages keys. Each device wishing to communicate can be configured with a symmetric key, SA info, and other info. Or, the Internet Key Exchange (IKE) can be used. IKE is made up of two protocols, ISAKMP—Internet Security Association and Key Management Protocol-- and Oakley).   
How does this come into play?

If I want to establish a secure VPN connection between two routers, those routers will use a handshaking process to exchange security parameters like algorithms, key size, etc. This is information that you would not want a hacker to acces. Here’s where IKE comes in. First IKE is used to establish a secure channel between the routers. It uses Diffie Hellman to get a secure session key on each end.   
Second, that session key is used to encrypt VPN parameters. These parameters are stored as a part of the SA. Now, the data can be transmitted securely.