Introduction to Computer Forensics and Security (6G7Z1009_1819_9Z6)

Diffie-Hellman Key exchange- Further explaind using the video

A useful video (start from c.2mins) for explaining Diffie-Hellman(-Merkle) key exchange: a method to allow two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

It also highlights the cryptographic value of a one-way function and the difficulty of finding the discrete logarithm.

Click http://drtomcrick.com/2013/09/16/visualising-diffie-hellman-key-exchange/ link to open resource.