

wikipedia

hash tree: http://en.wikipedia.org/wiki/Hash_tree

SHA-1: <http://en.wikipedia.org/wiki/SHA-1>

des : http://en.wikipedia.org/wiki/Data_Encryption_Standard

aes: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

cmac: <http://en.wikipedia.org/wiki/CMAC>

WEP: http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

PKCS (riferimenti ai diversi standard PKCS da 1 a 16):
<http://en.wikipedia.org/wiki/PKCS>

WAP: http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

SSL: http://en.wikipedia.org/wiki/Secure_Sockets_Layer

IPSEC: <http://en.wikipedia.org/wiki/IPSec>

non wiki: <http://www.unixwiz.net/techtips/iguide-ipsec.html#ah>

cifrario malleabile:

http://en.wikipedia.org/wiki/Malleability_%28cryptography%29

random oracle model:

[http://en.wikipedia.org/wiki/Standard_Model_\(cryptography\)](http://en.wikipedia.org/wiki/Standard_Model_(cryptography))

cramer shoup

http://en.wikipedia.org/wiki/Cramer-Shoup_cryptosystem