

## **Encryption Algorithms Contained in Cisco's Products**

**Cisco's products may contain one or more of the following encryption algorithms.**

Accordingly, Cisco's products containing encryption are subject to the U.S. Export Administration Regulations and may be controlled for National Security (NS), Anti Terrorism (AT), and/or Encryption (EI) reasons.

The primary function of encryption in Cisco products falls into two categories:

1. Data Privacy (confidentiality - encrypting user data)
2. Administrative - OAM&P (secure network management - administrative network functions)

### **Data Hashing/Authentication**

MD4  
MD5  
SHA-1  
RIPEMD160  
MICHAEL  
HMAC  
MMH  
CRC32

### **Key Exchange/ Asymmetric Algorithm Strength**

DSA 1024, 1024/1536  
Elliptic Curve Diffie-Hellman (ECDH) 163  
RSA 1024, 2048, 4096  
DSA 1024, 2048  
Diffie Hellman 1024, 1536  
ElGamal 384

### **Data Security Encryption.**

Blowfish 128  
CAST 128  
DES-56 56, 64  
Triple DES 112, 168, 192  
DESX 56/64  
RC2 40, 64, 128  
RC4-128 40, 128  
RC5 128  
AES-128/192/256  
ARCFOUR 128  
SEAL 160  
IDEA 128  
Skipjack

