Cheatography

Security+ Cheat Sheet

by rmn498 via cheatography.com/39195/cs/12216/

Symmetric Encryption

Name	Keysize	Blocksize	Type
DES	56	64	Block
3DES	56, 112, 168	64	Block
IDEA	128	64	Block
Blowfish	32 - 448	64	Block
Twofish	128, 192, 256	128	Block
AES	128, 192, 256	128	Block
RC4	40 - 2,048	-	Stream

Symmetric Encryption uses the same key to encrypt and decrypt. Faster than Asymmetric Encryption, but less secure due to key-sharing problems. Does not scale well.

Asymmetric Encryption

Name	Notes
RSA	Static keys from 1,024-4,096 bits
ECC	Elliptic Curve Cryptography
DHE	Diffie-Hellman Ephemeral exchange
ECDHE	Uses DHE with ECC
Quantum Cryptography	Uses photons

Asymmetric Encryption uses a key pair (1 public, 1 private). Public key is distributed by a trusted third party using PKI. Requires more processing and is slower than symmetric encryption, but more secure. No key-sharing problem.

Transport Encryption

Name	Port	Notes
SSH (Secure Shell)	22	SFTP, SCP, Telnet
HTTPS	443	HTTP using SSL/TLS
IPSec	51	HMAC for auth header; Can use ESP with AES or 3DES.

Transport Encryption (cont)

SSL	Secure Sockets Layer	FTPS, HTTPS
TLS	Transport Layer Security	Replaced SSL

Hashing

Name	Length
MD5	128 bits
SHA-1	160 bits
SHA-2	224, 256, 384, 512 bits
SHA-3	224, 256, 384, 512 bits
HMAC	Integrity AND authentication
RIPEMD	128, 160, 256, 320 bits
LANMAN	Used for Windows 9x systems. Pads password to 14 chars. Converts to UPCASE. Hashes (2) 7-char strings.
NTLMv1	Replaced LANMAN on NT systems. Uses MD4 orLANMAN.
NTLMv2	Uses MD5

Hashing provides integrity. Small changes to input result if large changes to output. One way function.

Email Encryption

Name		Algorithm
S/MIME	Secure/Multipurpose Internet Mail Extensions	RSA
PGP/GPG	Pretty Good Privacy / GNU Privacy Guard	RSA

May use only Asymmetric Encryption or may use Asymmetric Encyption to send Symmetric Key allowing faster encryption/decryption.

Authentication

Name		
PAP	Password Authentication Protocol	Cleartext; last resort
CHAP	Challenge Handshake Authentication Protocol	Server challenges client
MS-CHAP	Microsoft-CHAP	Proprietary version of CHAP
MS-CHAPv2	Microsoft-CHAPv2	Mutual authentication
RADIUS	Remote Authentication Dial-In User Service	Centralized AAA server; Encrypts password only; Must handle all 3 A's
Diameter	Improved RADIUS	Supports EAP
XTACACS	Extended Terminal Access Controller Access-Control System	Cisco proprietary; Improvement to TACACS
TACACS+	Terminal Access Controller Access-Control System Plus	Cisco proprietary; Can work with Kerberos; Encrypts entire auth process

By **rmn498**
cheatography.com/rmn498/

Not published yet.
Last updated 1st July, 2017.

Sponsored by **Readability-Score.com**
Measure your website readability!
https://readability-score.com