Hashing Algorithms

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Acronym | Name | Other Versions | Bit Length(s) | Secure? | Used With | Notes |
| MD5 | Message Digest | MD2, MD4 | 128 | No - collisions | Files, CHAP, NTLM |  |
| SHA | Secure Hashing Algorithm | SHA2 (preferred), SHA3 | SHA-160  SAH2-224,256, 334, 512 | SHA, no – collisions  SHA2, yes, not broken yet |  | SHA2 – most widely used hash algorithm |
| RIPEMD | RACE Integrity Primitives Evaluation Message Digest | RIPMD-160, RIPEMD-256, RIPEMD-320 | 160, 256, 320 | RIPEMD, no, replaced by RIPEMD-160 |  | Based on MD4. |

Hashing Method

|  |  |  |  |
| --- | --- | --- | --- |
| Acronym | Name | Used With | Notes |
| HMAC | Hashed Message Authentication Code | HOTP, PBKDF2, IPSEC, TLS (can use any hash algorithm for the hashing function) | Includes a secret key in the hash to prevent man in the middle attacks. |

SYMMETRIC Encryption Algorithms

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Acronym | Name | Key Size | Method | Used With | Notes | Secure |
| DES | Data Encryption Standard | 56-bit | Block | Diffie-Hellman | Originally used by government and industry. | No, known list of weak keys |
| 3DES | Triple Data Encryption Standard | 168-bit: (3) 56-bit keys | Block | Electronic payment industry, some Microsoft products (passwords), Diffie-Hellman | Replacement for DES | Yes, more secure than DES |
| AES | Advanced Encryption Standard | 128, 192, 258 (default: 128) | Block | WPA2, CCMP, Diffie-Hellman | Replacement for 3DES, now used by government | Yes, more secure than 3DES |
| Blowfish | Blowfish | 32 - 448-bit | Block (64-bit) |  | Very fast block cipher. | Yes |
| Twofish | Twofish | 256-bit | Block (128-bit) |  | Very fast block cipher, more complex key schedule than Blowfish. | Yes, more secure than Blowfish. |
| RC4 | Ron’s (Rivest) Cipher 4 | 40 to 2048-bit | Stream | WEP, WPA, SSL, TLS, BitTorent | Other Versions: RC5, RC6 | Yes, but not with WEP-weak initialization vector (IV) |
| IDEA | International Data Encryption Algorithm | 128-bit | Block (64-bit) | PGP for email |  | Yes |
| OTP | One-Time Pads | Varies (length of message) |  |  | No pattern in key application. Keys are only used once. | Yes, most secure, cannot be mathematically broken |

ASYMMETRIC Encryption Algorithms

|  |  |  |  |
| --- | --- | --- | --- |
| Acronym | Name | Used With | Notes |
| RSA | Rivest Shamir Adleman | SSL, digital signatures, key exchange | Most common asymmetric algorithm |
| DH | Diffie-Hellman | IPSEC, key exchange | Two numbers can be made public and through mathematical computations and exchanges of intermediate values, can separately create the same key |
| EC | Elliptic Curve | Devices with low processor power (mobile devices) | Similar to RSA, but smaller key sizes. Based on sharing a point on an elliptic curve. Needs less computation and power. |
| DHE | Diffie-Hellman Ephemeral | Key Exchange, AES, DES, 3DES | Uses different, ephemeral keys (temporary) that are used once and discarded |
| ECDHE | Elliptical Curve Diffie-Hellman | Key Exchange | Uses elliptical curve instead of prime numbers in its calculation. |
| PGP | Pretty Good Privacy | Windows File Systems, email, digital signatures | Uses symmetric and asymmetric methods for encryption. |
| GnuPG | GNU Privacy Guard | Linux, Unix, and Windows file systems | Free replacement for PGP. |
| Quantum | Quantum | Quantum key exchange (QKE) | Based on characteristics of the smallest particles known. |

Authentication Protocols

|  |  |  |  |
| --- | --- | --- | --- |
| Acryonym | Name | Used With | Notes |
| XTACACS | Extended Terminal Access Controller Access-Control System | Cisco Devices | Second version of TACACS. Provides Authentication, Authorization, and Accounting. |
| TACACS+ | Terminal Access Controller Access-Control System | Cisco Devices | Most recent version of TACACS. Usually used for administrator AAA on Cisco devices, because of granualarity (can restrict to certain commands). Also provides Authorization and Accounting. |
| Kerberos | Kerberos | Windows Domains | Allows for single sign on using key/ticket distribution. Key Distribution Center (KDC) can be a single point of failure. Preferred over NTLM. |
| LDAP | Lightweight Directory Protocol | Windows Active Directory, X.500 directories, online white and yellow pages | Allows queries to be issued to X.500-based directory. Operates at port 389. |
| Secure LDAP | Secure Lightweight Directory Protocol | Windows Active Directory, X.500 directories | Securely allows queries to be issued to X.500-based directory. Made secure with SSL/TLS and uses port 636. |
| SAML | Security Assertion Markup Language | XML | Mainly used with web page and cross-web page authentication |
| CHAP | Challenge Handshake Authentication Protocol | PPP | Designed to stop man-in-the-middle attacks. Generates a random number (hash) during initial authentication. Periodically demands the number. (MSCHAP is Microsoft’s version of CHAP and is used with EAP and PEAP). |
| PAP | Password Authentication Protocol |  | No longer used, sends passwords in plain text |
| SPAP | Shiva Password Authentication Protocol |  | Replaced PAP. Encrypts the username and password. |
| LANMAN | LAN Manager | Windows 95, 98, and ME, LM Hash and two DES keys | Very old, replaced by NTLM. |
| NTLM | NT LAN Manager | Windows NT, MD5 hashing | Replaced LANMAN. Several versions: NTMLv1 and NTLMv2. Still in widespread use, although Keberos is preferred. |
| TOTP | Time-Based One-Time Password | Time-based algorithm, token, and server | Uses time based algorithm to create unique passwords, very secure |
| HOTP | HMAC-Based One-Time Password | HMAC-based algorithm, token, and server | Uses HMAC to create unique passwords |