# Table 1: Overview of Cryptographic Algorithms

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Algorithm | Key Length (commonly used) | Description |
| Symmetric Encryption |  |  | Algorithms where the same key is used for both encryption and decryption. |
|  | AES (Advanced Encryption Standard) | 128, 192, 256 bits | A block cipher that is widely accepted as the standard for encrypting data. |
|  | DES (Data Encryption Standard) | 56 bits | An older block cipher that was widely used but now is considered to be broken and insecure. |
|  | 3DES (Triple DES) | 168 bits | A more secure variant of DES which applies the DES algorithm three times to each data block. |
|  | RC4 | 40-2048 bits | A stream cipher that was widely used in protocols like SSL, but is now considered insecure. |
| Asymmetric Encryption |  |  | Algorithms where different keys are used for encryption and decryption (public and private keys). |
|  | RSA | 1024, 2048, 3072 bits | Widely used for secure data transmission and digital signatures. |
|  | ECC (Elliptic Curve Cryptography) | 160-512 bits | Provides the same security as RSA but with shorter key lengths. |
|  | DSA (Digital Signature Algorithm) | 1024, 2048, 3072 bits | Used for digital signatures. Not for encryption. |
| Hash Functions |  |  | Algorithms designed to produce a fixed-size output from any input, ideally in a unique way. |
|  | MD5 | 128 bits | Now considered broken and not recommended for further use. |
|  | SHA-1 | 160 bits | Has vulnerabilities and is being phased out in favor of stronger variants. |
|  | SHA-256 | 256 bits | A part of the SHA-2 family, widely used and considered secure. |
| Key Exchange | Diffie-Hellman | Various, based on group | Allows two parties to each generate a pair of values and derive a shared secret. |
|  | ECDH (Elliptic Curve Diffie-Hellman) | Based on chosen curve | A variant of Diffie-Hellman that uses elliptic curves. |