|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CRYPTOGRAPHY STANDARDS | | | | |
| STANDARD | **SYMMETRY** | **HOW IT WORKS** | **VARIATIONS** | **POSSIBLE ATTACKS** |
| CONSIDERED SECURE | | | | |
| AES (Advanced Encryption Standard) | Symmetric | Processes data in 128-bit blocks | AES-128, AES-192, AES-256 | Brute force, side-channel attacks |
| RSA (Rivest-Shamir-Adleman) | Asymmetric | Uses public and private keys for encryption and decryption | RSA-1024, RSA-2048, RSA-4096 | Side-channel attacks, padding oracle attacks |
| ECC (Elliptic Curve Cryptography) | Asymmetric | Uses mathematical properties of elliptic curves for encryption and decryption | NIST P-256, NIST P-384, NIST P-521 | Side-channel attacks, invalid curve attacks |
| Twofish | Symmetric | Block cipher | A symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits.  NOT RECOMMENDED | Known key and related key attacks. |
| Serpent | Symmetric | Block cipher | A symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits.  NOT RECOMMENDED | - |
| CONSIDERED INSECURE | | | | |
| IDEA | Symmetric | Block cipher | A symmetric key block cipher with a block size of 64 bits and a key size of 128 bits. | Differential cryptanalysis attacks |
| RC2 | Symmetric | Block cipher | A symmetric key block cipher with a block size of 64 bits and a key size of up to 128 bits. | Key recovery attacks |
| RC4 | Symmetric | Stream cipher | A variable key size stream cipher. | Bias attacks, key recovery attacks |
| Blowfish | Symmetric | Processes data in 64-bit blocks | - | Brute force, birthday attacks |
| DES (Data Encryption Standard) | Symmetric | Processes data in 64-bit blocks | - | Brute force, meet-in-the-middle attacks |
| RC4 (Rivest Cipher 4) | Symmetric | Processes data in stream cipher | - | Bias attacks, weak keys |