# Table 3: Asymmetric Key Algorithms – Key Lengths and Security

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Algorithm | Key Length (commonly used) | Equivalent Symmetric Key Strength | Features & Security Concerns |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| RSA | 1024, 2048, 3072 bits | 80, 112, 128 bits | - Widely used and well-studied - Vulnerable to quantum attacks - 1024 bit is now considered weak; 2048 or higher recommended |
| ECC (Elliptic Curve Cryptography) | 160, 224, 256, 384, 521 bits | 80, 112, 128, 192, 256 bits | - Provides high security with shorter key lengths - Faster and requires less power - Also vulnerable to quantum attacks |
| DSA (Digital Signature Algorithm) | 1024, 2048, 3072 bits | 80, 112, 128 bits | - Used mainly for digital signatures - Not for encryption - Similar key strength considerations as RSA |
| ElGamal | 2048, 3072 bits and higher | Varies based on implementation | - Can be used for both encryption and digital signatures - Tends to be slower and produce larger ciphertexts than RSA |
| Lattice-based cryptography | Varies; emerging area | Varies based on implementation | - Resistant to quantum attacks - An area of active research for post-quantum cryptography |
| DH (Diffie-Hellman) | 2048, 3072 bits and higher | 112, 128 bits | - Used for secure key exchange - Vulnerable to "man-in-the-middle" attacks unless combined with a way to authenticate keys |