# Table 8 (Expanded): Comparative Analysis – Algorithm Efficiency

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Algorithm Category | Algorithm Name | Key Length (for comparison) | Equivalent Symmetric Key Strength | Time to Process 1MB Data (MS) | Memory Footprint (KB) | Notes |
| Symmetric Encryption | AES | 256 bits | 256 bits | 2.5 | 5 | Standard for encrypting data; good security and performance balance. |
|  | 3DES | 168 bits | ~112 bits | 7.5 | 8 | Older standard; being phased out due to decreased security compared to AES. |
|  | RC4 | 128 bits | ~80 bits (now considered weak) | 1.2 | 3 | Deprecated due to vulnerabilities. |
|  | Blowfish | 128 bits | ~80 bits | 2 | 4 | Older algorithm, still used in some legacy systems. |
| Asymmetric Encryption | RSA | 2048 bits | 112 bits | N/A (used for small data) | 10 (small data ops) | Popular for digital signatures and key exchange. |
|  | ECC (P-256) | 256 bits | 128 bits | N/A (used for small data) | 2 (small data ops) | Efficient alternative to RSA for key exchange and digital signatures. |
|  | DSA | 2048 bits | 112 bits | N/A (used for small data) | 8 (small data ops) | Used mainly for digital signatures. |
| Hash Functions | SHA-256 | N/A | N/A | 4 | 1 | Widely used hash function. |
|  | MD5 | N/A | N/A | 1 | 0.5 | Deprecated due to vulnerabilities. |
|  | SHA-3 | N/A | N/A | 3.5 | 1 | Newer hash standard with a different structure than SHA-2. |
| Key Exchange | Diffie-Hellman | 2048 bits | 112 bits | N/A (used for key agreement) | 5 (key agreement ops) | Traditional method for secure key exchange. |
|  | ECDH (with P-256) | 256 bits | 128 bits | N/A (used for key agreement) | 2 (key agreement ops) | Elliptic curve-based key exchange; more efficient than traditional Diffie-Hellman. |