# Table 8: Comparative Analysis – Algorithm Efficiency

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Algorithm Category | Algorithm Name | Key Length (for comparison) | Equivalent Symmetric Key Strength | Time to Process 1MB Data (ms) | Notes |
| Symmetric Encryption | AES | 256 bits | 256 bits | 2.5 | Widely accepted standard; good balance of security and performance. |
|  | 3DES | 168 bits | ~112 bits | 7.5 | Slower and less secure than AES; being phased out. |
|  | RC4 | 128 bits | ~80 bits (now considered weak) | 1.2 | Deprecated due to vulnerabilities. |
| Asymmetric Encryption | RSA | 2048 bits | 112 bits | N/A (used for small data) | Used mainly for key exchange and digital signatures, not bulk data encryption. |
|  | ECC (P-256) | 256 bits | 128 bits | N/A (used for small data) | More efficient than RSA for similar security levels; used in modern protocols. |
| Hash Functions | SHA-256 | N/A | N/A | 4 | Part of the SHA-2 family; widely used and considered secure. |
|  | MD5 | N/A | N/A | 1 | Fast but broken; not recommended for security purposes. |
| Key Exchange | Diffie-Hellman | 2048 bits | 112 bits | N/A (used for key agreement) | Used in many secure communication protocols for key exchange; ECC variants are more efficient. |