# Table 4: Hash Functions – Characteristics and Applications

|  |  |  |  |
| --- | --- | --- | --- |
| Hash Function | Output Size (bits) | Features & Characteristics | Common Applications |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| MD5 | 128 | - Fast computation - Vulnerabilities discovered; considered broken - Collisions can be found | - Legacy systems - File checksum (not recommended for security purposes) |
| SHA-1 | 160 | - Once widely used - Vulnerabilities discovered; collision attacks are feasible - Being phased out in favor of SHA-2 and SHA-3 | - Legacy digital signatures - Older certificate generation |
| SHA-256 (Part of SHA-2) | 256 | - Considered secure as of last update - Widely adopted | - Digital signatures - Cryptocurrency (e.g., Bitcoin) - Data integrity |
| SHA-3 | Configurable (e.g., 256, 512) | - Newer standard, different internal structure than SHA-2 - Considered secure | - Digital signatures - Data integrity |
| RIPEMD-160 | 160 | - Designed in Europe - No known vulnerabilities as of last update but less widely studied than SHA-2 | - Digital signatures in some contexts - Cryptocurrency (e.g., Bitcoin addresses) |
| Whirlpool | 512 | - Based on block cipher principles - No known vulnerabilities as of last update | - Data integrity - Digital signatures in specific applications |
| BLAKE2 | Configurable (e.g., 256, 512) | - Faster than MD5, SHA-1, and SHA-256 in software - No vulnerabilities known as of last update | - Cryptographic software - Data integrity |