**Comparison Table of Popular Encryption Algorithms**

**From** http://www.kellermansoftware.com/t-ArticleStrongestAlgo.aspx

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Algorithm** | **Created By** | **Key Size** | **Block Size** | **Algorithm Structure** | **Rounds** | **Cracked?** | **Existing Cracks** |
| Rijndael | Joan Daemen & Vincent Rijmen in 1998 | 128 bits, 192 bits, 256 bits | 128 Bits | Substitution-Permutation Network | 10, 12 or 14 | No | Side channel attacks |
| Twofish | Bruce Schneier in 1993 | 128 bits, 192 bits or 256 bits | 128 bits | Feistel Network | 16 | No | Truncated differential cryptanalysis |
| Blowfish | Bruce Schneier in 1993 | 32-448 bit in steps of 8 bits. 128 bits by default | 64 bits | Feistel Network | 16 | No | Second-order differential attack |
| RC4 | Ron Rivest in 1987 | Variable | Variable | Stream | Unknown | Yes | Distinguishers based on weak key schedule |
| RC2 | Ron Rivest in 1987 | 8-128 bits in steps of 8 bits. 64 bits by default | 64 bits | Source-Heavy Feistel Network | 16 Mixing 2 Mashing | Yes | Related-Key attack |
| TripleDES | IBM in 1978 | 112 bits or 168 bits | 64 bits | Feistel Network | 48 | No | Theoretically possible |
| DES | IBM in 1975 | 56 bits | 64 bits | Feistel Network | 16 | Yes | Brute force attack, differential crypanalysis, linear cryptanalysis, Davies' attack |

**Date of article:** 7/16/2008