Encryption is an effective means for providing confidentiality and integrity of data within an organization, especially during data in-motion. There are many different types of encryption algorithms in use today.

# Instructions

For this assignment, you will prepare a comparison matrix between the algorithms listed below:

1. DES
2. 3DES
3. CCMP (AES)
4. Rijndael
5. IDEA
6. CAST
7. Blowfish
8. Twofish
9. RC4
10. RC5

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Algorithm** | **Block Size (bit)** | **Key Size (bit)** | **Rounds of Operation** | **Description** |
| DES | 64 | 56 | 16 | 1977, Easy to crack due to small key size |
| 3DES | 64 | 112 or 168 | 48 DES rounds | 1998, uses the DES algorithm 3 times, depreciated for AES as it uses too many resources |
| CCMP (AES) | 128 | 128, 192, or 256 | 10, 12, or 14 depending on key size | 2000, very strong algorithm, used primarily in HTTPS, FTPS, SFTP, WebDAVS, and OFTP |
| Rijndael | 128, 192, or 256 | 128, 192, or 256 | 9, 11, or 13 depending on key/block size | 2000, NIST selected this for the standard encryption based on AES |
| IDEA | 64 | 128 | 8 | 1991, an improvement on DES due to larger key size |
| CAST-128 | 64 | 40 to 128 in 8-bit increments | 12 or 16 if key size is greater than 80 | 1996, Similar to DES this uses a Feistel cipher |
| CAST-256 | 128 | 128, 160, 192, 224, or 256 | 48 | 1998, improved from CAST-128, was once a candidate for AES |
| Blowfish | 64 | 32 to 448 | 16 | 1993, Designed to replace DES, is faster than AES due to smaller block size |
| Twofish | 128 | 128, 192, or 256 | 16 | 1998, Based on Blowfish, evaluated by NIST but lost to AES |
| RC4 | 1-bit stream cipher | 40 to 2048 | 1 | 1987, no longer recommended for use due to known weaknesses, used in WEP, prohibited in SSL/TLS |
| RC5 | 16, 32, or 64 | 0 to 2048 | 0 to 255 | 1994, Based on RC4, highly customizable in block size, key size, and rounds of operation. |