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** |
| DES | 64 | 56 | 16 |
| 3DES | 64 | 168 | 48 |
| CCMP (AES) | 128 | 128,192 or 256 | 10 12 14 |
| Rijndael | 128 | 128,192 or 256 | 10 12 14 |
| IDEA | 64 | 128 | 8.5 |
| CAST-128 | 64 | 40 - 128 | 12 or 16 |
| CAST-256 | 128 | 128 ,160 ,192 ,224 256 | 48 |
| Blowfish | 64 | 32-448 | 16 |
| Twofish | 128 | 128, 192 or 256 | 16 |
| RC4 | 2064(1684) | 40-2048 | 1 |
| RC5 | 32, 64 or 128(64 suggested) | 0 – 2040 (128 suggested) | 1-255 (12 suggested) |