Encryption is the process of converting data into a coded form so that only authorised users have access to it. Cryptography is the most common technique that converts plain text to ciphertext. Algorithms such as AES, DES, 3DES, BLOWFISH and IDEA are compared based on Fitness Function designed by us.
Computation time, memory usage and output byte, key length, block size, possible keys, cipher type, security.
DES takes least encryption time. Memory usage of AES outperforms others.

AES: advanced encryption standard, it takes 128 bits of data and encrypts it giving 128 bits of ciphertext with some key (128,192,256). We do substitution for confusion and permutation for adding diffusion. It takes this 16 byte(128 bit) data and creates a 4x4 grid and applies subs. and perm. to it and also add key(here key is expanded in every round). Steps: xor with key->substitution->shifting rows and then mixing columns for perm->add key this is one round. This has 10(128), 12(192) and 14(256) rounds.

DES: Digital Encryption standard, 56 bit keys with 64 bit block cypher. Then news of DES encrypted messages being cracked came frequently, then came 3DES.

3DES: Triple Digital Encryption standard, three times strength of DES, K1 is used to encrypt a message (p) resulting in C1 cipher text. K2 is used to decrypt C1 resulting in C2 cipher text, K3 is used to encrypt C2 resulting in C3 cipher text. 3 56 bit keys are used. Effective key length is then 168 bits.

BLOWFISH: It is a symmetric key block cipher. Same key is used for both sides. 64 bits block size and key size is variable from 32 to 448 bits therefore more secure. Uses steps are key generation and then data encryption.

TWOFISH: next generation of blowfish with 128 bit block size and 256 bit key size.

Key generation

1) Key array -> k1k2k3..kn (each of 32 bits n lies btw 1 to 14)
2) Parray -> P1p2…p18, max 18 words of 32 bit size.
3) S boxes -> 4 substitution boxes S0 to S255 each
4) Initialize parray and sbox with hexadecimal values.
5) P1=P1 xor K1 …. Upto K14 then P15 xor K1 ..
6) 64 bit plain text assigned with 0

Data Encryption

1) Plaintext is taken and divided into two halves 32-32
2) P1 xor 32 bits is given to a function(uses sbox and xor operation) and output of this is xor with the remaining 32 bits.
3) Outputs are swapped and then this process continues for P2 upto P18.
4) Now all the 32 bits are merged to get ciphertext.

IDEA: international Data Encryption algorithm, symmetric key block cipher. Input is 64 bits block size with 4 16 bit parts. Key size is 128 bits divided into 52 subkeys with 17 rounds. With 4 keys for odd rounds and 2 keys for even number rounds.

Parameters:

1) Block size: directly proportional.
2) Key size: key is basically a lock, directly proportional.
3) Rounds: directly proportional.
4) Avalanche effect: the amount of change in the ciphertext if a single bit change is changed in plain text or key. A good cipher must have at least 50% avalanche effect.
5) Encryption time: inversely proportional.
6) Decryption time: inversely proportional.

All the weights in the fitness function are set based on the priority of the parameter. Avalanche effect>key size>block size>rounds>times(as they are sys dependent but out ff is designed in such a way that relative values remain constant).

Results using different file sizes: As per the needs of end user one must know the requirements and available trade-offs.

1) Based on fitness function: AES performed best among all and second was TWOFISH.
2) Based on encryption and decryption time: AES proves to be least time taking and second ws 3DES.
3) Based on Avalanche effect: AES performed best among all and second was TWOFISH and least was for DES and 3 DES.

Average value of ff from all file sizes gives: AES>TWOFISH>BLOWFISH>3DES>IDEA.