# A Brief* Performance Comparison between Chameleon Polymorphic Cipher and AES Cipher

| Attribute | Chameleon Polymorphic (CC-192) | AES |
|---|---|---|
| Algorithm | Polymorphic (changes with user key) | Fixed Algorithm |
| Known Attacks | No Known Attacks | Broken |
| Key-dependent Polymorphic Algorithm | Yes (key-dependent algorithm) | No (Fixed Algorithm) |
| S-box | User-key dependent S-ORB | Fixed S-box (public) |
| Variable word size (by the user) | Yes | No |
| Variable Minimum Number of rounds (by the user) | Yes | No |
| Number of rounds are key-dependent | Yes | No |
| Key Size | Variable 192 bits | Variable 128, 192, 256 bits |
| Key Set-up Time | 1849<br>( This relatively large set-up time while the user will not even feel it, yet it is important to prevent Brute Force Attacks since the attacker will spend almost double the time of AES trying to find the key) | 850 cycles |
| Encryption Time | 28 cycles per byte with a total of 672 cycles | 440 cycles |
| Execution time<br>(0n Intel Core2 Duo CPU E6550 @ 2.33 GHz, 4 GB RAM, 32-bit operating system)<br>(on Processor Intel(R)<br><br>Core(TM) i5-3230M CPU @ 2.60GHz, 2.601 Ghz, 2 Core(s), 4 Logical Processor(s), Installed Physical Memory (RAM)8.00 GB, 64-bit operating system)<br>Better performance is achieved with new processors. We have used this processor to correctly | 171-203 milliseconds (depending on word size)<br><br>16 milliseconds | 88-101 milliseconds (Estimate)<br><br>8.2 milliseconds (Estimate) |

| | | |
|---|---|---|
| compare with AES published data. | | |
| Hardware/software Implementation | Suitable | Suitable |
| The probability of guessing the algorithm used | Much Less than $89.68 \times 10^{-45}$ (User key-dependent and is smaller than a brute force attack using 128-bit key) | Well-known algorithm (Probability =1.0) |
| Passed all NIST Tests | Yes | Yes |
| Statistical Parameters of cipher text available to user after encryption | Yes | No |
| Variable throughput depending on word size | Yes | No |
| Security | Very High | High (Broken) |
| Modes for multimedia applications | Can be used in any mode, including the default ECB (no information leakage) | Requires other modes beyond ECB ( with ECB information leakage is possible) |

*The cipher was implemented using C# language under MS Windows operating system. This is a brief comparison between CC-192 and AES; other features such as ASM language, device performance dependency, and other operating system implementations are not included.