Luke Tao

MRGS Research

Topic Abstract

6 Apr 2021

# The Effectiveness of Randomness Test Suites for Block Ciphers

This study aimed to compare the effectiveness of different randomness test suites when used on block ciphers. The strength of an encryption algorithm is partially determined by its randomness. Block ciphers encrypt in chunks instead of continuously. The popular NIST and DieHarder tests suites are rather unsuited for testing block ciphers. This is due to interference from modes of operation which are used to combine the chunks. In addition, the tests have multiple scores which makes interpretation and comparison difficult. CryptoStat is a relatively new test that aims to solve these issues. AES256 with various modes of operation including Electronic Codebook (ECB), Cipher Block Chaining (CBC), Counter (CTR), and Output Feedback (OFB) was used to encrypt 32GB of binary zeroes to ensure randomness came from encryption and not the plaintext. The NIST and Dieharder randomness test suites were run on this ciphertext. The CryptoStat test suite was run on its included AES256 implementation. The results for NIST and Dieharder showed that CBC, CTR, and OFB were random whereas ECB failed almost every test within the suites. AES256 passed every CryptoStat test. CryptoStat gave results consistent with NIST and Dieharder when the latter tests were run on the more cryptographically secure modes of operation: CBC, CTR, and OFB. CryptoStat may be used as an alternative to NIST and Dieharder that is unaffected by the effectiveness and randomness of different modes of operation. Further research should be conducted to replicate these results across other encryption methods.

*Keywords:* encryption, randomness, block ciphers, modes of operation, test suites, NIST, Dieharder, CryptoStat, AES