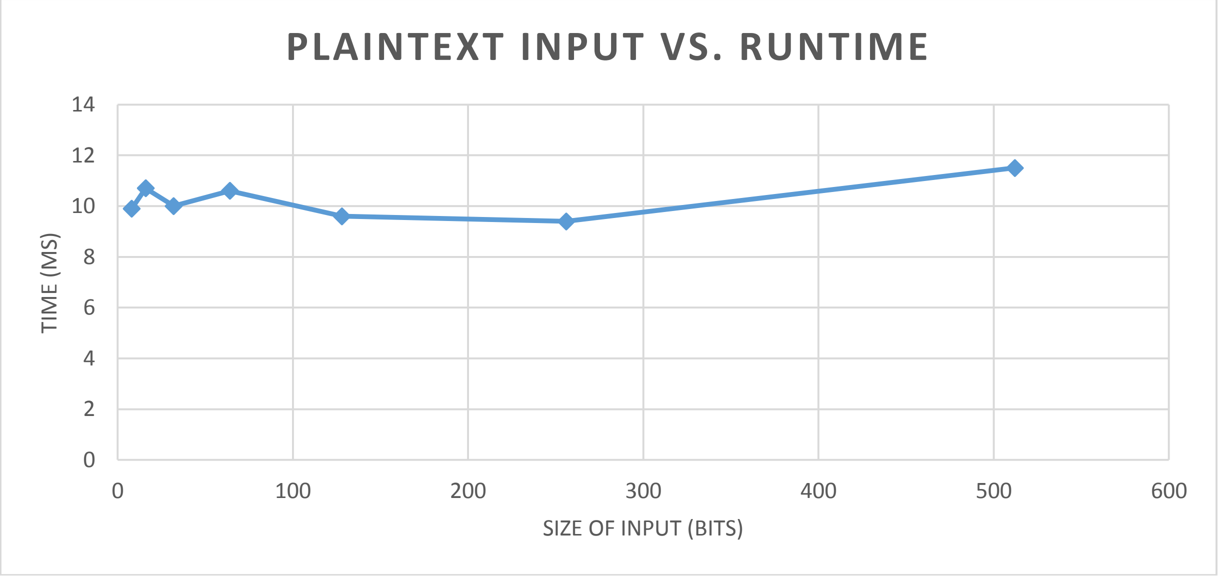
Montgomery Marauders
nolang@umich.edu
pasikzak@umich.edu
sads@umich.edu

PERFORMANCE ANALYSIS OF SPECK BLOCK CIPHER

After running performance tests based on input size (plaintext/ciphertext) on our implementation of 128/192 SPECK, we found that the runtime of our algorithm is constant. Regardless of the number of bits in the input plaintext/ciphertext, or even keys, our program always takes around 8-12 milliseconds to execute a decryption or encryption.

The reason for this is that our encryption and decryption functions are both O(T), where T is the number of key expansions performed. Because our implementation is of a predefined 128/192 SPECK cryptosystem, we have T equal to a constant value. That is the explanation for why our runtime is not a function of key/input size. Had there been complex or costly arithmetic done on the input, the runtime would have increased, but all steps of encryption and decryption can be done using bit shifts, bitwise or's, addition and subtraction. Below is a graph of the data we collected:


PLAINTEXT INPUT VS. RUNTIME
TIME (MS)
SIZE OF INPUT (BITS)