Discussion: Fri 1:30pm

Team: 28 [Custodes Arcanarum]

Name: Connie Qi, Zachary Herbst, Adam Johnson

Uniqname: connieqi, zmherbs, ajlj

Project

#### (a) Code

Code attached to CTools submission.

## (b) Sample Output

## **Test Vector**

#### Key

 $14074904626401341155369551180448584754667373453244490859944217516317499064576\\ (0x1f1e1d1c1b1a191817161514131211100f0e0d0c0b0a09080706050403020100)$ 

#### Plaintext:

154358840404572640889229863092020605801 (0x74206e69206d6f6f6d69732061207369)

## Ciphertext:

187646149816416544869629532715157534824 (0x8d2b5579afc8a3a03bf72a87efe7b868)

#### Tests

#### Command:

./simon -k

14074904626401341155369551180448584754667373453244490859944217516317499064576 -p 154358840404572640889229863092020605801

#### **Output:**

ciphertext: 187646149816416544869629532715157534824

#### Command:

./simon -k

14074904626401341155369551180448584754667373453244490859944217516317499064576 -c 187646149816416544869629532715157534824

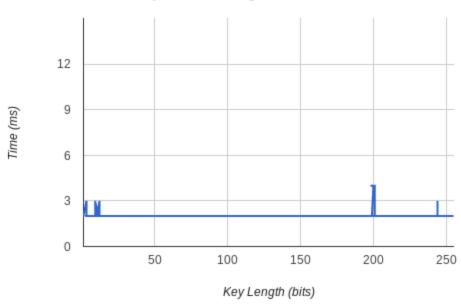
#### **Output:**

plaintext: 154358840404572640889229863092020605801

# (c) Performance

This experimentation was done on an ASUS Zenbook Prime UX31A, with an Ivy Bridge Core i7 rated at 1.7GHz.

# Simon Cipher Running Time



# Simon Cipher Running Time

