Matthew Haney
Junior Division Mathematics & Computer Sciences
A Taste of Xcode: An Analysis of Security of the RSA Public-Key Encryption Algorithm

The purpose of this experimental endeavor was to find a flaw in the seemingly impregnable armor of the RSA encryption algorithm. This was attempted in an experimental manner, namely by coding an RSA encryption algorithm and inputting related keys to find if corresponding ciphertexts were related in a readily identifiable way. If such relations were found, the RSA algorithm may have been compromised; in such an event, the entire algorithm would be unsecure and could not be used. However, when results were examined, no relations were discerned between the input characters and resultant ciphertext. In this way, the RSA encryption algorithm and public security are sound, for the moment. The only benefits of this experiment have been a greater knowledge of the inner workings of the RSA algorithm, programming and mathematics in general.