Updated Vigenere Cipher, Dec 1, 2015

Jared Rankin

Problem Definition

- The original Vigenere cipher was not entirely secure; it was vulnerable to cryptanalysis based on its repeating key

Competitive Analysis

Classical Vigenere cipher without one time pad or substitution table

- Pros: Faster to perform, simpler to implement
- Cons: Vulnerable to techniques that can determine the length of the repeating key, allowing the cipher to be easily broken

Potential Applications

- Protection of information stored in a file
- Authentication (if used as a hash function, as in POSIX crypt())

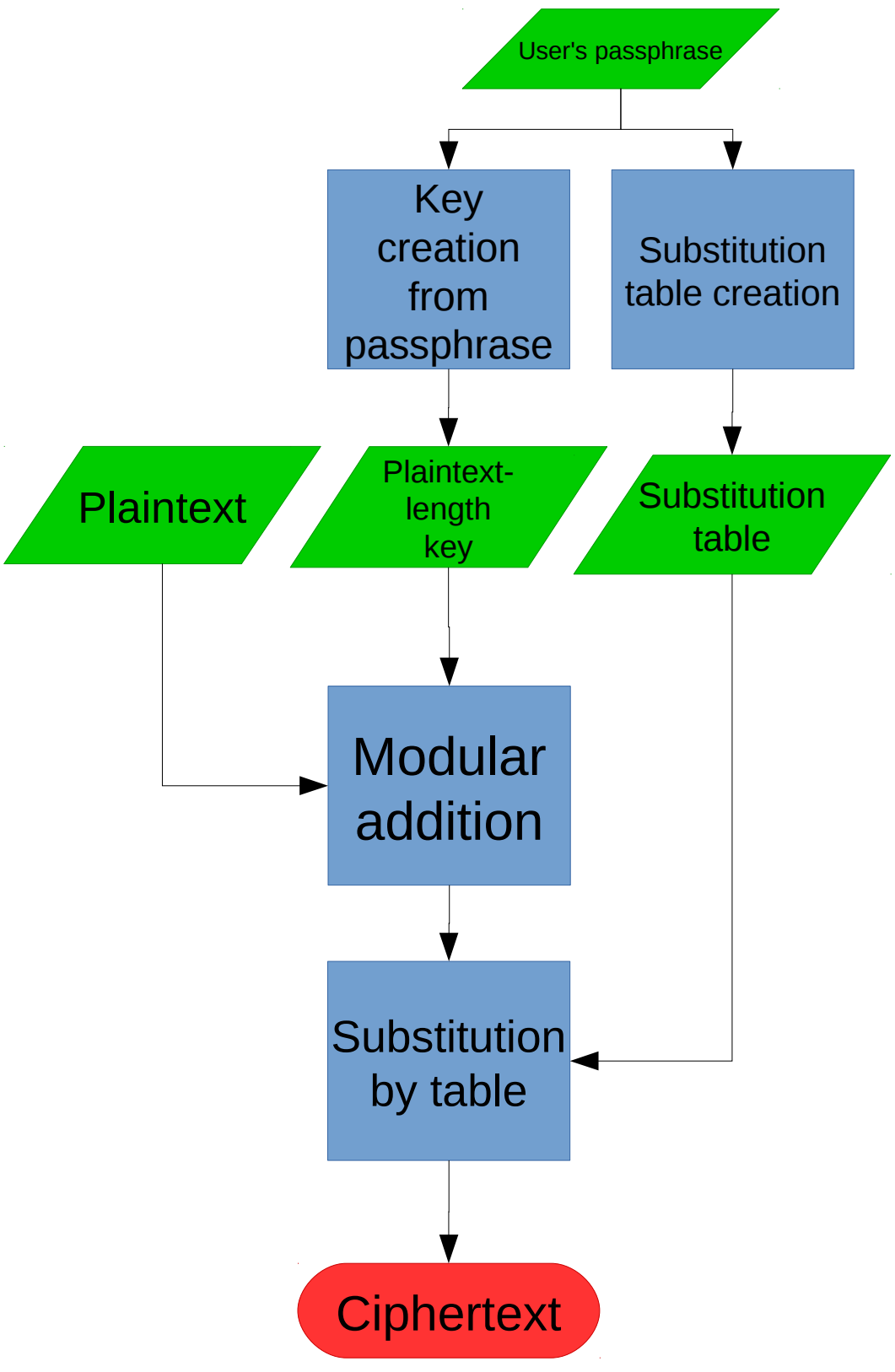
Future Improvement Ideas

- Improve key generation procedure, to reduce efficiency of dictionary attacks against passphrase
- Increase security of keys created from short passphrases

Solution Specifications

- This implementation provides a method for generating a plaintext-length random key from a given passphrase
- It also adds a step to the encipherment process: a substitution table, generated based on the key, applied immediately after Vigenere's modular addition

Components in blue are actions performed by the updated cipher program (implemented in Python)



Clark College EST. 1933
Engineering & Computer Science Departments