

Senior Design Project in Electrical & Computer Engineering



Key Generation for Secure Coast Guard Communications

Cadet 1/c Josh Gaidos and 1/c Rebecca Doyle

Advisor: Mr. Herb Holland

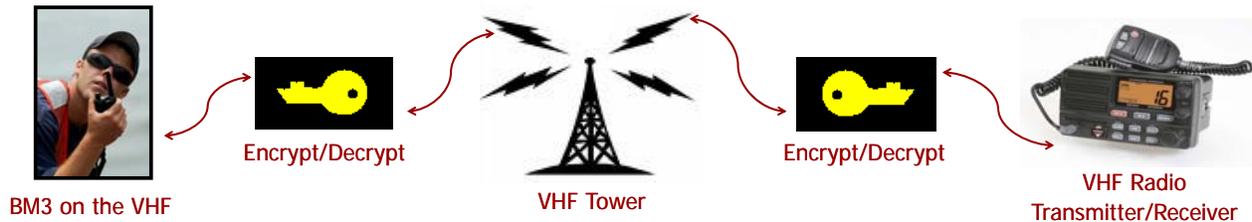
Sponsor: LT Lars McCarter, CG-6

Project Objectives

The main goal of this project is to design and create a program with a Graphical User Interface (GUI) that will generate a random number to be used in data encryption.

Background Information

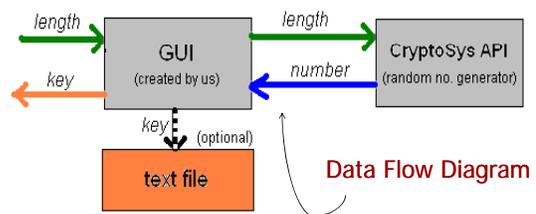
Everyday, the Coast Guard Conducts 78 search-and-rescue missions*, many of which use small boat VHF radio communications. Of these 78 missions, none have *completely* secure radio communication. Information transferred on the Encrypted Automatic Identification System is encrypted but not well-protected. Meanwhile, VHF radio communications between small boats are not encrypted at all. As long as both systems are unprotected in this manner, their integrity is compromised.



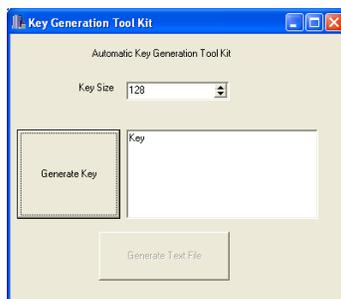
Methods / System Design

We intend to use a code module, called CryptoSys API, which is already written and federally approved for government use. The software will interface with a GUI that, when prompted, will output a random hexadecimal number. The length of the number is determined by the input provided to the GUI by the user.

A primary focus is to make the final product user-friendly and suitable for the Coast Guard.



Graphic User Interface (GUI)



Project Timeline

- Feb. 29: GUI completed
- Mar. 21: Test Plan completed
- Apr. 1: GUI testing completed
- Apr. 4: Design Specifications completed
- Apr. 17: Testing by Sponsor completed
- Mar. 24: Draft of Project Paper completed
- Apr. 24: Response to Sponsor testing completed
- Apr. 29: Project Binder completed

Functional Requirements
Meets NIST standard FIPS 140-2
Must run on Windows XP
Must run in less than 1 minute
Must run in less than 1 Gb of memory
User interface must be a GUI
Output must be ready for copy-and-paste with the option to create a text file
The key must be a variable length (at least 64 bits)
The key must be output in hexadecimal

*http://72.14.205.104/search?q=cache:Hhvk3bBVN9cJ:www.uscg.mil/top/about/doc/uscg_snaps_hot.pdf+everyday+the+Coast+Guard+will&hl=en&ct=clnk&cd=1&gl=us