Name(s)	Project Number
Sarah H. Kazmie	**S1412**

Project Title

Smart Code

Abstract

Objectives/Goals

Modern credit card terminals store and transmit a purchaser's account information using standard computer protocols, which can be hacked and intercepted. In several recent attacks, hackers have used simple key loggers and packet sniffers to intercept millions of transactions.

My goal was to develop SMART CODE:
    A Secure, Merchant-coded, Augmented Recording and Transmission using Character Optimized, Dynamic Encoding.

Methods/Materials

I developed a variation on the Huffman compression routine, where a sorted frequency table is weighted and skewed to produce a unique variable bit-length encryption. I created a function to artificially weight the symbol frequency table based upon the digits of one or more simple pin codes.

To test my algorithm, I created a C# application which can automatically compare and quantify the results of my compression algorithm on varying sets of multiple multi-digit code variations.

I also converted my SMART CODE algorithm into C and programmed it into a PSOC 4 dev board to demonstrate that it could be embedded in a micro-controller.

Results

I tested more than 990,000 samples of two three-digit pin codes, and more than 6 million samples from a random progression through three four-digit pin codes. In the more than 7 million total test comparisons, no messages could be fully decoded with even a single digit change in any of the pin codes. I wrote a function to quantify the difference in two resulting strings and not one of the 7 million sample comparisons, scored a difference value of less than 20,000, where 0 indicates identical text and 50,000 is completely random.

Conclusions/Discussion

SMART CODE successfully executed with three four-digit pin codes in less than 0.07 seconds. A continuous run of 990,000 samples, on a fast PC, took about 12 hours to complete. This represents the time it would take to find a match using all combinations of only 2 3-digit codes. If you had to try all combinations of two four-digit codes, it would take 100 times longer, and if the series were expanded to to include a third four-digit code, it would take about 12,000,000 hours or 1,369.8 years.

Summary Statement

An adjusted weighted Huffman Coding algorithm can be used to create a very secure and efficient encrypted credit card processing system.

Help Received

A family friend loaned me a PSOC dev board and taught me how to use it.