A New Method of Cryptography II:

Jacqueline Christy ❖ Dr. James Walker ❖ Mathematics❖ University of Wisconsin-Eau Claire

This project was funded by UWEC Differential Tuition and by the UWEC Foundation.

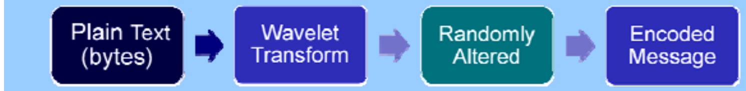
Introduction:

When transferring data, it is important to encrypt the information with an algorithm that cannot be broken. One of the most frequent strategies used to decode messages is frequency analysis, so it is important the algorithm protects against these attempts at decryption. Formerly, an algorithm was devised, and now the bugs have been removed and its performance while encoding sets of alphanumerical data has been studied.

The Program:

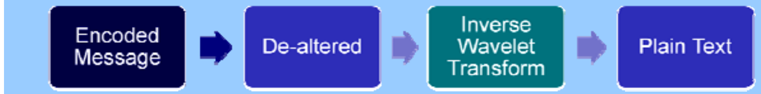
Using Visual Basic 6.0, a program implementing a new cryptographic scheme was developed. The new cryptographic scheme combines the wavelet transform based scheme with a series of random alteration values to encode alphanumerical data.

Coding:



1. Each character from the text is converted into an integer using the key which was developed in which each symbol on the QWERTY keyboard was assigned an integer value based on the frequency with which the symbol commonly appears.
2. The integer values are altered using the wavelet transform.
3. Random alterations are applied using the irrational number δ.
4. Each value is bumped up by 100 to avoid overflow.

Decoding:



1. The set of integers is de-altered by subtracting 100 and the random alterations.
2. The inverse wavelet transform is applied.
3. The key is used to convert the integers back to text.

Testing Reliability:

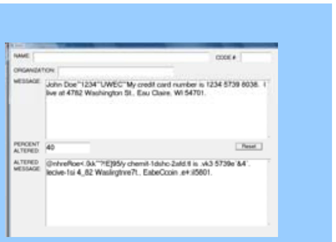
In order to test whether the devised algorithm was secure against frequency analysis attempts at decryption, the program in Visual Basic was altered.

Altered Program:

1) Encodes the message
2) A given percent of the encoded values are altered ± 1
3) The original encoded values and altered values are decoded
4) The original message and the altered message are compared

If there was a connection between the frequency of the characters in the original message and the integers in the encoded message (meaning that certain integers were linked to specific characters), the percent of the altered message that differed from the original message would equal the percent of integers altered.

Two messages were used to test the program. Each message was tested by altering 40, 50, and 60 percent of the message. Each percent was tested five times per message to insure consistency. By comparing the original message with the altered message, the number of readable characters (out of 27 valuable characters*) was recorded.



NAME:

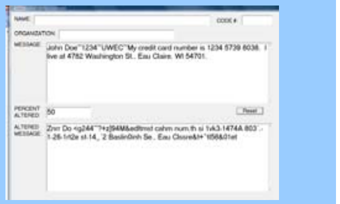
CODE #

ORGANIZATION:

MESSAGE: John Doe~1234~UWEC~My credit card number is 1234 5739 8038. I live at 4782 Washington St., Eau Claire, WI 54701.

PERCENT ALTERED: 40

ALTERED MESSAGE: @nhreRoe<.0kk~?!E]95/y chemit-1dshc-2afd.fl is .vk3 5739e`&4`. lecive-1si 4_82 Waslingtnre7t., EabeCcoin .e+:il5801.



NAME:

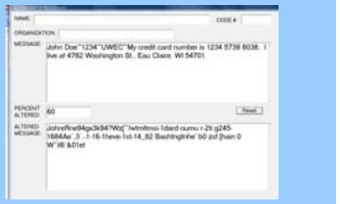
CODE #

ORGANIZATION:

MESSAGE: John Doe~1234~UWEC~My credit card number is 1234 5739 8038. I live at 4782 Washington St., Eau Claire, WI 54701.

PERCENT ALTERED: 50

ALTERED MESSAGE: Zrn Do <g244~?+z]94M&edltmd cahm num.th si 1vk3.1474A 803`.- 1-26-1r!2e st-14,.`2 Baslin0inh Se., Eau Clsore&l+`!t56&01et



NAME:

CODE #

ORGANIZATION:

MESSAGE: John Doe~1234~UWEC~My credit card number is 1234 5739 8038. I live at 4782 Washington St., Eau Claire, WI 54701.

PERCENT ALTERED: 60

ALTERED MESSAGE: JohreRne94gx3k94?Wz[~/wtmltmsi-1dard oumu r-2t g245-16M4Ae`.3`.-1-16-1heve-1ut-14_82 Bashingtnhe` b0 zsf [hain 0 W~#6`&01et

Results:

Percent of Altered Characters (out of 27 valuable characters*)

Message 1

Attempt

Percent Altered	1	2	3	4	5
40	67	74	67	56	74
50	70	85	78	85	81
60	93	89	81	89	93

Message 2

Attempt

Percent Altered	1	2	3	4	5
40	56	74	78	67	70
50	78	70	85	85	82
60	85	85	93	93	89

After testing the devised algorithm by altering the original message by 40, 50, and 60 percent, it was found that the percent of characters that differed in the altered message from the original was higher than the percent of integers altered. This indicates that the algorithm may be secure against frequency analysis attempts at decryption.

*Valuable characters include credit card numbers and addresses