Secure Transmission of Sensitive data using multiple Channels

Ahmed A. Belal, Ph.D.  
aabelal@yahoo.com
Faculty of Engineering, Alexandria University, Egypt.

Abdelhamid S. Abdelhamid, M.Sc.  
asaladin@acm.org
Faculty of Engineering, Alexandria University, Egypt.

Introduction
The increase in the dependency on digital communications was a main motivation to the research in the field of data security. Many schemes were developed in order to protect sensitive data from an adversary. This paper studies the effect of hiding the cipher text using in order to increase the difficulty of the adversary task.

Proposed Scheme
The scheme depends on partitioning the output of a block encryption module using the Chinese Remainder Theorem CRT among a set of channels. The purpose of using the CRT and transmitting over multiple channels is to hide the cipher text in order to increase the difficulty of attacking the cipher.

The proposed scheme assumes the existence of $A$ transmission channels between the sender and the receiver parties from which $S$ Channels are chosen using some selection criteria. The selection criterion is based on selecting pseudorandom numbers in the range $[0, A - 1]$. An instance of the generator runs on each side of communication $S$ times to select the $S$ channels using the same start conditions.

The original message or plain-text is divided into units that are referred to as super blocks of $N$ bits. The super blocks are encrypted using an encryption module that operates using a block encryption scheme $E_x(B)$ of block size $N_b$ bits where $N$ is equal to $LN$, for an integer $L$. The encryption is performed using an appropriate mode of operation such as CBC. Each super block is treated as an $N$ bit integer.

A set of $S$ relatively prime moduli $q_0, q_1, ..., q_{S-1}$ are selected such that $2^N \leq q_0 q_1, ..., q_{S-1}$ then the $N$ bit integer CRT remainders with respect to the selected $S$ moduli are calculated and sent over the selected $S$ channels. The Selected $S$ channels are used to transmit the remainders while the rest of the channels carry some irrelevant data in order to decrease the ability of the adversary to determine the used channels.

At the receiver side, the inverse of the CRT is applied to get the original $N$-bit cipher super block, and then a decryption module $D_x(B)$ is used to get the original $N$ bit plain-text.

The application of the CRT to the output of the encryption module aims at hiding the cipher in order to reduce the advantage of the adversary.

To give all the channels equal weights the sizes of the moduli are chosen to be around the value $\lceil N/S \rceil$. The maximum number of channels used in the proposed scheme was estimated as $S_{max} = O(N / \log N)$.

Security Analysis
In order to analyze the security of the scheme two analysis steps were done. In the first step, we analyzed the ability to distinguish the output of the scheme from the output of a random source. The analysis showed that as the actual output does not span the whole possible range of outputs, there is a probability that the adversary distinguishes the scheme output from a random output. The distinguishability of the output was found to dependant on the guess of the CRT moduli that are parts of the key and accordingly this possibility is not of high impact in the application.
In the second step, we have proved that the existence of an algorithm that can return some information about the plain text given the output of the scheme implies the existence of another algorithm that can do the same to the output of the underlying block encryption. So we proved that the scheme is as secure as the underlying block cipher in terms of leaking information about the plain text.

**References:**

[1] Stinson D. R., Cryptography: Theory and Practice, CRC Press, 1995.

[2] Menezes Alfred J., Van Oorschot Paul C. and Vanstone Scott A., Handbook of Applied Cryptography, CRC Press, 2001.

[3] D. E. Knuth. The Art of Computer Programming: Volume 2 / Semi numerical Algorithms. Addison-Wesley, 2nd edition, 1981.

[4] Aho A., Hopcroft J., and Ullman J. The Design and Analysis of Computer Algorithms. Addison-Wesley, Reading, Mass., 1974.

[5] Hellekalek Peter, Inversive Pseudorandom Number Generators: concepts, results and links. Department of mathematics, University of Salzburg, A-5020 Salzburg, Austria 1995.

[6] Goldreich Oded, Ron Dana, Sudan Madhu, Chinese Remaindering with errors. Proceedings of the Thirty-First annual ACM Symposium on Theory of Computing 1998.

[7] Gao, Shuhong. “Chinese Remainder Theorem (CRT) and Interpolation”, MTHSC 985 course notes, Clemson University. Fall 2001.