17

Hill cipher application to Multimedia Security

N. Nikitakos
Lcdr Hellenic Navy
P.O. Box 80318 Piraeus 18510 Greece , tel: +301 4625993
e-mail: nikitas @ naxos.esd.ece.ntua.gr

Abstract

The protection of valuable data in a multimedia system is one of today's most challenging tasks for information technology. Hill cipher belongs in the polygram substitution case of ciphers and gives an inexpensive, easy and robust tool for multimedia security. The theory of Hill cipher and the related cryptosystem implementation is presented. The application of Hill cryptosystem to a Command and Control system and the related discussion conclude the paper.

Keywords

Hill Cipher, Hill Algorithm, Multimedia Security, Cryptography, Command and Control System.

1 INTRODUCTION

As Multimedia systems have evolved to prolific practical data processing systems. we have come to relay on these systems to process and store data we have also come to wonder about their ability to protect valuable data. A classical way for data security is the substitution ciphers. There are four types of substitution ciphers: simple substitution, Homophonic substitution, Polyalphabetic substitution, and polygram substitution. Simple substitution ciphers replace each character of plaintext with a corresponding character of ciphertext.

In Homophonic substitution ciphers each plaintext character is echiphered with a variety of ciphertext characters. Polyalphabetic substitution ciphers use multiple mapping from plaintext to ciphertext characters and polygram substitution ciphers are the most general, permitting

R. Posch (ed.), *Communications and Multimedia Security*

arbitrary substitutions for groups of characters. Hill cipher belongs in the polygram substitution case of ciphers and gives an inexpensive, easy and robust tool for multimedia security.

In this paper the Hill cipher initial application to multimedia security system is presented and particular to protect data (written instructions) for a Command Control and Communication system through unprotected communication channels.

The paper is organized as follows: In section 2 the Hill cipher is briefly presented. In section 3 the robustness concerning deciphering is discussed. In section 4 a brief description of a possible application of Hill cipher to multimedia security is presented and, finally section 5 summarizes our conclusions

2 THE HILL CIPHER

Of special interest in systematic cryptography is the linear transformation:

$$\begin{aligned} c_1 &= (k_{11} m_1 + k_{12} m_2 + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots + k_{1f} m_f) + k_1 \\ c_2 &= (k_{21} m_2 + k_{22} m_2 + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots + k_{2f} m_f) + k_2 \\ &\;\cdot \\ &\;\cdot \\ c_f &= (k_{f1} m_1 + k_{f2} m_2 + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots + k_{ff} m_f) + k_f \end{aligned} \tag{1}$$

in which f is any positive integer, and the variables c_i and m_i as well as the coefficients k_{ij} and k_i are elements of an arbitrary finite field or infinite set. Since the integers modn with addition and multiplication form a commutative ring where the laws of associativity, commutativity and distributivity hold the linear the linear transformation described by (1) becomes:

$$\begin{aligned} c_1 &= (k_{11} m_1 + k_{12} m_2 + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots + k_{1f} m_f) \bmod n \\ c_2 &= (k_{21} m_2 + k_{22} m_2 + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots + k_{2f} m_f) \bmod n \\ &\;\cdot \\ &\;\cdot \\ c_f &= (k_{f1} m_1 + k_{f2} m_2 + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots + k_{ff} m_f) \bmod n \end{aligned} \tag{2}$$

Expressing M and C as column vectors $M = (m_1, m_2, \ldots\ldots m_f)$ and $C = (c_1, c_2, \ldots\ldots\ldots c_f)$ we can write:

$$C = E_k(M) = KM \bmod n \tag{3}$$

where E_k is the enciphering transformation from M to C using a key K which is defined as the square matrix of linear transformation coefficients of f-order namely:

$$K = \begin{pmatrix} k_{11} \cdot k_{12} \cdots\cdots k_{1f} \\ k_{21} \cdot k_{22} \cdots\cdots k_{2f} \\ \cdot \\ k_{f1} \cdot k_{f2} \cdots\cdots k_{ff} \end{pmatrix} \qquad (4)$$

The deciphering procedure is done using the inverse matrix K^{-1} where $KK^{-1} \bmod n = I$ and I is the fxf identity matrix.

If the determinant of the matrix K is primary we say that the procedure is a normal transformation and can be proven that the matrix K has a unique inverse K^{-1}. Given any pair of inverse normal transformations K and K^{-1} we have a tool which may be applied to an alphabet :

1. to convert any message sequence of n letters into a corresponding cipher sequence of n letters and

2. to convert the cipher sequence back into the message sequence from which it came.

In other words, we have all the apparatus of an extraordinary effective polygraphic cipher system. The following elementary example shows the Hill cipher application. Let n be 26 , f =2 and let K , K^{-1} be as follows:

$$\overset{K}{\begin{pmatrix} 3 & 2 \\ 3 & 5 \end{pmatrix}} \overset{K^{-1}}{\begin{pmatrix} 15 & 20 \\ 17 & 9 \end{pmatrix}} \bmod 26 = \overset{I}{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}} \qquad (5)$$

Suppose we wish to encipher the plaintext message A D which corresponds to the column vector (1,4). We compute

$$\begin{pmatrix} c \\ c_2 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 3 & 5 \end{pmatrix} \begin{pmatrix} 1 \\ 4 \end{pmatrix} \bmod 26 = \begin{pmatrix} 11 \\ 23 \end{pmatrix} = \begin{pmatrix} K \\ W \end{pmatrix} \qquad (6)$$

getting the ciphertext C=(11,23) or K W . To decipher we compute

$$\begin{pmatrix} 15 & 20 \\ 17 & 9 \end{pmatrix} \begin{pmatrix} 11 \\ 23 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 \\ 4 \end{pmatrix} \qquad (7)$$

3 HILL CRYPTOSYSTEM IMPLEMENTATION

The implementation of the polygraphic cryptographic algorithm has some features described in [Pat-88]. Particularly in the implementation program where mod 67 has been selected for all arithmetic's and largest key size of 254 allowed exist the following useful features

- The usage of prime modulus of 67 gives the advantage that the algorithm is using Galois Field GF(67) arithmetic

- The algorithm utilizes a plaintext vector rather than a plaintext matrix. This difference is important because each byte of the plaintext is utilized in creating each byte of the ciphertext. If the plaintext was a matrix then only one row of the plaintext matrix would be used for operation.

- The security desired can be traded off again the speed of cryption.

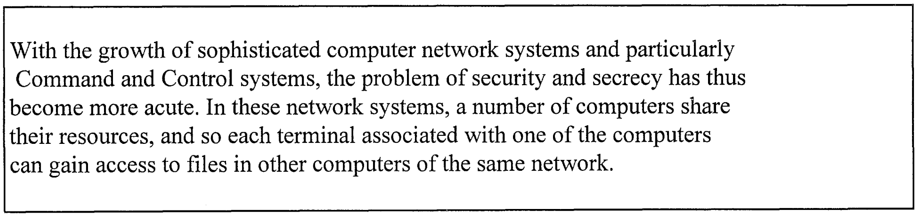
- Key sizes ranges from 24 bits (=2x2x6) to 387096 bits (=254x254x6). This is over four orders of magnitude variability in key size.

- The eight bit of ASCII characters can be randomized.

- When the program reads in a 8-bit data value it splits it into two 4-bit nybbles. To each nybble is appended two random bits (yielding two 6-bit values). Therefore, each 8-bit value is expanded to 12-bits. Although this results in the ciphertext being larger than the cleartext it adds considerable security against various attacks.

- Because multiplication is one of the slowest operations in a computer, the program uses a lookup table to pre-store the modulo multiplication answers. This speed the program up considerably.

Figures 1 and 2 show an example of plaintext (3360 bits) and a resulting ciphertext using a 56 order Hill cryptosystem which totally produces a 56x56x6=18816 bytes key (it took 1 sec on a 80486-50 Hz personal computer)



With the growth of sophisticated computer network systems and particularly Command and Control systems, the problem of security and secrecy has thus become more acute. In these network systems, a number of computers share their resources, and so each terminal associated with one of the computers can gain access to files in other computers of the same network.

Figure 1 Plaintext example

```
LcrHRTJpJJgAhYI)FZCnanjaSR2bVyCWCJBVPqKjVkAmfR!Lwink)H6s
BHU1uxSk1HDet34lxNZ6YB2UA8!pQ8]R]!NvCQAfoeC1Sonnr4OHtc2D
BlgtBvHLo0R1r!pLmYOGu0y2yVwH1gAek!z(VUAQK9h!)aoSSUmeLv0B
zC3ws17mjxpQ0k8[]gjf5b2Rrve6pSK36t[G(kI]xrO(yVRYx(UR582w
v[jjw3M1Vi(3kz)8PZbi9nUu63[JxMSV5lqKzvK(d!71i0DCOcWaxOym
)UVQ1id5]eUeYAyPxQV5lRTe48Vjfs[2yPUGZ6PYZQV9QmoYdM12UCr3
yLLY3y2T166hr5brjX(s0rp[1av1Z!gtegxdCyHtknqzaR[UVvqFuPvu
Qfhv]K5XszovROhm)AJQ0uFCmN6hjiKMIH5JkLWdgJ!uF!haC[FRNTTp
hEdy5]vzsthiyun()llAm(AaWvBWWXL7CunA4q(O6Wt8CC5sfs3ftTHW
0JHFZf]8YiRz88gD1Tcz!rbd2tklm5TrrHLsbg0Al8)UIu[N97mj(Mv(
2qLpisMb)G)0M6B6zwU[uYcdLKwlJCmEj]ZxEjmoM7kfvI1JPcuN77H!
]x6ye2BNQWZ4pgTOBquOhsMPR)nK)7GjkVaV3CtuqJkZ5c2]k!]qANQC
5CLr)PPNt2H095)P8D4Hvop6G1WakGW!8ps49o4eAdUeLG[nbINc6ume
dn(rsM0zp!IoO5zhM[el!a4MWaZy9aExmygmWUkBzxXAPpFX1WyEzImo
```

Figure 2 Resulting ciphertext from Hill cryptosystem application

In the context of evaluation of proposed cryptosystem arises the question of the systems security against a cryptanalysis attack. There are two most likely attack against the cryptosystem. One is the "known plaintext attack" which is believed to be a sufficient metric for the security of a cryptosystem. In a known plaintext attack, the cryptanalyst has obtained a large amount of plaintext - ciphertext pairs. Then, the cryptanalyst tries to determine the algorithm and the key. In the second kind of attack called "chosen plaintext attack" the cryptanalyst has the ability to choose the plaintext which is encrypted, and then to try to break the system.

For both the cryptanalytic attack the Hill algorithm can express strong security due to following reasons.

1. Number of bits :Traditional methods encrypt one, two, or three characters of plaintext per encrryption operation utilizing a human-readable key. With our method we can crypt 100 or more bytes at a time per matrix-by-vector multiplication. the key is pure random bit stream. Because both the keys and the ciphertext involve so many bytes, no frequency analysis is possible.
2. Difficulties having the numerical ciphertext vector: Although the ciphertext is known, this does not easily yield the ciphertext vector. This is because the ciphertext is printable ASCII which has been mapped from the numeric representation of the ciphertext vector. This mapping of the ciphertext vector is either a permutation of P values into printable ASCII or a one-to-many mapping
3. Influence of a random number generator: Since the algorithm easily add a random number stream to a plaintext prior to encryption, a known plaintext attack is not possible.
4. Additional security features: Inserting blocks of encrypted random "garbage" into the ciphertext file results in additional security by not allowing the cryptanalyst to known where the "true ciphertext" is.

5. Huge amount of data: Even when both plaintext and ciphertext vectors are known, these fact represents a very small amount of the information since the key matrices are much larger than the plaintext and ciphertext vectors.

4 APPLICATION TO A COMMAND AND CONTROL SYSTEM

The growing scope of large on-line communication systems has generated new requirements and has imposed additional burdens on the computer and intercomputer technologies.. New such systems are being developed from variety of sources and incorporated in a single comprehensive programme.

The task of these systems is to establish and provide an accurate real time information status for problems confronting an organization which will give it the means for decision making. The decision making may be manual or automatic and may be conducted at top management level or low down in the chain of command.

With the improvement of sophisticated computer network systems and particularly command and control systems, the problem of security and secrecy has thus become more acute. In these network systems, a number of computers share their resource, and so each terminal associated with one of the computers can gain access to files in other computers of the same network.

The command and control system where Hill algorithm has proposed to apply is consisted of a map updated in real time with geographic details and other sensitive information which can be reached via a hypertext like system. The algorithm is applied where specific information are requested (i.e. status of available resources of a platform) by a particular user or where this information is to be send to another user via an unsecure communication channel.

Another major issue in command and control system which utilizes multimedia technology, is its ability to establish a secure system-to-system initial connection, using a proper authentication protocol. This secure connection would guarantee that the two or more communicating system are indeed the ones that are suppose to communicate.

Since a command and control system should be considered, in great many cases, as security-critical, it is evident that the strength of the Hill-cipher should be combined with the strength of a system-to-system authentication protocol. Such a protocol has been recently proposed in the literature, and its strength has been demonstrated [Gri-92]. Combination of the two procedures would, thus , provide a command and control systems with a potential to both:

- Identify and authenticate positively the other system it communicates with

- Transmit securely the information required to utilize a multimedia platform

At this time the name of the file where the daily key belongs is requested and in negative case an enciphertext like the one in Fig.2 appears. This is one more software security against unauthorized release of classified information. The initial generation and key distribution has been made by the control unit of the network.

5 CONCLUSIONS AND FUTURE DIRECTIONS

In this paper, an algorithm based on Hill cryptosystem for multimedia security is presented and proposed for implementation in a command and control system. The proposed modified Hill cipher has been proven to be easy to implement , secure and robust to cryptanalysis attack.

Furthermore, the combination of Hill algorithm with system-to-system authentication protocols provides a command and control system with potential to both authenticate the other end of the communication channel, and to transmit in a secure way the information required to utilize a given multimedia platform (e.g. a map, etc)

In the future, it is expected that the algorithm -together with the authentication protocol- will be integrated in a whole command and control system for performance evaluation in a real time system. Also application of Hill algorithm for ciphering digitized mapping data will be examined.

6 REFERENCES

Denning D. (1983) *Cryptography and Data Security* . Addison Wesley, New York.

Gritzalis D., Katsikas S., Gritzalis S., (1992) A Zero-Knowledge Probabilistic Login Protocol, in *Computers & Security,* Vol. 11, No 8, 733-745.

Hill L.S. (1922) Cryptography in an Algebraic Alphabet, in *American Mathematical Monthly*

Hill L.S. (1931) Concerning certain Linear Transformation Apparatus of Cryptography, in *American Mathematical Monthly*

Morris D.J. (1985). *Introduction to Communication Command and Control* . Pergamon Press,.

Patti T. edited (1988) *Cryptosystems Journal* , Vol.1 ,No2 ,

7 BIOGRAPHY

Nikitas V. Nikitakos was born in Piraeus, Greece, Greece, in 1959. He received his B.S. in Naval Engineering from Hellenic Naval Academy in 1980 and both his M.Sc. in Applied Mathematics and M.Sc. in Electrical engineering from the Naval Postgraduate School in California, USA in 1988. He holds also a University degree in Economics from University of Piraeus (1986). In 1990 Mr. Nikitakos joined the Department of Electrical and Computer Engineering at the National Technical University of Athens, Greece, where he is currently working toward a Ph.D. degree. His area of interest include computer security, radar and sonar theory and techniques, and communication systems.. He is a Lieutenant Commander in the Hellenic Navy.