Journal of Zhejiang University SCIENCE A
ISSN 1673-565X (Print); ISSN 1862-1775 (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

Comment:

Comments on "How to repair the Hill cipher"

Y. RANGEL-ROMERO, R. VEGA-GARCÍA, A. MENCHACA-MÉNDEZ, D. ACOLTZI-CERVANTES, L. MARTÍNEZ-RAMOS, M. MECATE-ZAMBRANO, F. MONTALVO-LEZAMA, J. BARRÓN-VIDALES, N. CORTEZ-DUARTE, F. RODRÍGUEZ-HENRÍQUEZ[†‡]

(*Computer Science Department, CINVESTAV-IPN, Av.IPN No. 2508 Col. San Pedro Zacatenco, Mexico City 07300, Mexico*)

[†]E-mail: francisco@cs.cinvestav.mx

Received June 26, 2007; revision accepted Sept. 13, 2007; published online Jan. 11, 2008

Abstract: A modification of the Hill cipher algorithm was recently proposed by Ismail *et al*.(2006), who claimed that their new scheme could offer more security than the original one due to an extra non-linearity layer introduced via an elaborated key generation mechanism. That mechanism produces one different encryption key for each one of the plaintext blocks. Nevertheless, we show in this paper that their method still has severe security flaws whose weaknesses are essentially the same as that already found in the original Hill cipher scheme.

Key words: Hill cipher, Symmetric encryption, Image encryption
doi:10.1631/jzus.A072143 **Document code:** A **CLC number:** TN918; TP309

INTRODUCTION

Invented in 1929, the Hill cipher became the first polygraphic substitution cipher that could be used in practice (Hill, 1929; 1931). However, by now the Hill cipher has not been utilized in professional practice due to its inherent weaknesses against known-plaintext attacks (Saeednia, 2000; Overbey *et al*., 2005).

Recently, it was claimed in (Ismail *et al*., 2006) that the security flaws of the Hill cipher could be repaired by introducing an elaborated key generation mechanism which is able to produce as many keys as the number of blocks in the plaintext message. In this paper we show that the new scheme proposed in (Ismail *et al*., 2006) would still be attacked under the known-plaintext attack scenario. To illustrate our analysis, we present three specific attacks, which can completely reveal the secret key and/or learn important details of the plaintext message.

HILL CIPHER SCHEME

Let us consider an arbitrary plaintext string of length l, defined over an alphabet of order n. We divide that plaintext into b blocks of length m, where m is an arbitrarily chosen positive integer and $b=\lceil l/m \rceil$. It is noticed that if the length l is not a multiple of m, the last plaintext block must be padded with $l-bm$ extra characters. Additionally, each character in the alphabet is coded with a unique integer in $\{0, 1, \ldots, n-1\}$, in other words, all the characters in the alphabet are mapped to the ring Z_n.

The b plaintext blocks can be rewritten as an $m\times b$ matrix $\boldsymbol{P}$ over Z_n using the one-to-one mapping between the original alphabet and the ring Z_n explained above. Additionally, an $m\times m$ matrix $\boldsymbol{K}$ with coefficients in Z_n must be chosen as the secret key matrix. According to the above definitions, Hill encryption can be performed by computing

$$\boldsymbol{C} = \boldsymbol{E}_{\boldsymbol{K}}(\boldsymbol{P}) = \boldsymbol{K}\boldsymbol{P} \bmod n. \tag{1}$$

Similarly, decryption is performed by computing

$$\boldsymbol{P} = \boldsymbol{D}_{\boldsymbol{K}}(\boldsymbol{C}) = \boldsymbol{K}^{-1}\boldsymbol{C} \bmod n. \tag{2}$$

There might be some complications with the proce-

‡ Corresponding author

dure outlined above due to the fact that not all the matrices $\boldsymbol{K}$ have an inverse $\boldsymbol{K}^{-1}$ over Z_n. In fact, those matrices $\boldsymbol{K}$ with determinant 0, or with a determinant that has common factors with the modulus n, will be singular over Z_n, and therefore they will not be eligible as key matrices in the Hill cipher scheme (Overbey *et al*., 2005). Furthermore, due to its linear nature, the basic Hill cipher succumbs to known-plaintext attacks. Indeed, it is easy to show that an opponent able to obtain m^2 plaintext/ciphertext character pairs has a high probability of completely breaking the system, i.e., he/she can obtain the matrix $\boldsymbol{K}$ by solving the linear system determined by Eqs.(1) and (2) (Trappe and Washington, 2006).

MODIFIED HILL CIPHER

In order to repair the security flaws of the original Hill cipher, Ismail *et al*.(2006) proposed to use a different $m\times m$ key matrix for encrypting each one of the b plaintext blocks of length m. By this, each of the b extra key matrices is derived from the preceding key according to the following equation:

$$\boldsymbol{K}_i=\begin{cases}\text{Original Hill matrix } \boldsymbol{K}, & i=1,\\ \text{Adjustment of } \boldsymbol{K}_{i-1}, & i=2, 3, ..., b.\end{cases} \tag{3}$$

As described in the algorithm of Fig.1, the adjustment procedure for generating a new key matrix consists of modifying, one by one, each row of the matrix key by multiplying the current key matrix with an initial vector $\boldsymbol{IV}$ that has been previously determined by the encryption entity. As a consequence, if the original $m\times m$ Hill matrix $\boldsymbol{K}$ is given as

Input: $\boldsymbol{K}$, $\boldsymbol{IV}\in Z_n$, m in Z^+. Where $\boldsymbol{K}$ is an $m\times m$ key matrix, with m a positive integer and $\boldsymbol{IV}$ a $1\times m$ initial vector.
Output: An $m\times m$ modified key matrix $\boldsymbol{K}'$.
Main Procedure:
1. $\boldsymbol{K}'=\boldsymbol{K}$;
2. for i=1 to m do
   2.a $\boldsymbol{R}_i=\boldsymbol{IV}\cdot\boldsymbol{K}' \bmod n$;
   2.b Replace the ith row of $\boldsymbol{K}'$ by $\boldsymbol{R}_i$;
3. end for
4. Return($\boldsymbol{K}'$);

Fig.1 Main procedure for producing a new key matrix $\boldsymbol{K}'$

$$\boldsymbol{K}=\begin{bmatrix}k_{11} & k_{12} & \cdots & k_{1m}\\ k_{21} & k_{22} & \cdots & k_{2m}\\ \vdots & \vdots & \ddots & \vdots\\ k_{m1} & k_{m2} & \cdots & k_{mm}\end{bmatrix}.$$

Then, after executing the first iteration of the loop in Steps 2~3 of the algorithm in Fig.1, the resulting $m\times m$ matrix $\boldsymbol{K}'$ becomes

$$\boldsymbol{K}'=\begin{bmatrix}k'_{11} & k'_{12} & \cdots & k'_{1m}\\ k_{21} & k_{22} & \cdots & k_{2m}\\ \vdots & \vdots & \ddots & \vdots\\ k_{m1} & k_{m2} & \cdots & k_{mm}\end{bmatrix},$$

where the m coefficients of the first row of matrix $\boldsymbol{K}'$, namely, k'_{1j} for j=1, ..., m, are obtained by computing the $1\times m$ vector $\boldsymbol{R}_1$ given as $\boldsymbol{R}_1=\boldsymbol{IV}\cdot\boldsymbol{K} \bmod n$. When the ith iteration of the algorithm in Fig.1 has been executed, all the first i rows of the original matrix $\boldsymbol{K}$ would have been updated as

$$\boldsymbol{K}'=\begin{bmatrix}k'_{11} & k'_{12} & \cdots & k'_{1m}\\ k'_{21} & k'_{22} & \cdots & k'_{2m}\\ \vdots & \vdots & \ddots & \vdots\\ k'_{i1} & k'_{i2} & \cdots & k'_{im}\\ \vdots & \vdots & \ddots & \vdots\\ k_{m1} & k_{m2} & \cdots & k_{mm}\end{bmatrix}.$$

Finally, when the m iterations of algorithm in Fig.1 have been executed, all the m rows of the resulting matrix $\boldsymbol{K}'$ will have been modified when compared with the original matrix $\boldsymbol{K}$.

Fig.2 shows the proposed encryption process that Ismail *et al*.(2006) called HillMRIV (Hill Multiplying Rows by Initial Vector). They claimed that the HillMRIV scheme was able to repair the security of the Hill cipher due to the extra non-linearity layer introduced by the b key matrices utilized in their system.

We briefly describe next the dataflow of the algorithm in Fig.2. Algorithm in Fig.2 performs b iterations, where b is the number of plaintext's blocks. In the very first iteration (i.e., i=1), the original Hill matrix $\boldsymbol{K}_1$ is used in Step 1.a, so that the first encrypted block is generated as $\boldsymbol{C}^{(1)}=\boldsymbol{K}_1\cdot\boldsymbol{P}^{(1)} \bmod n$.

Thereafter, a new matrix $\boldsymbol{K}_i$ for i=2, ..., b will be used for each of the remaining $b-1$ blocks, where $\boldsymbol{K}_i$ is obtained from the preceding key matrix by invoking in Step 1.b, the algorithm of Fig.1 previously described.

Input: $\boldsymbol{K}$, $\boldsymbol{IV}$, $\boldsymbol{P}^{(1)}$, $\boldsymbol{P}^{(2)}$, …, $\boldsymbol{P}^{(b)}\in Z_n$, m, b, n in Z^+. Where $\boldsymbol{K}$ is an $m\times m$ key matrix with coefficients in Z_n, with m, n positive integers; $\boldsymbol{IV}$ is a $1\times m$ initial vector; $\boldsymbol{P}^{(i)}$ is an $m\times 1$ plaintext column vector with i=1, 2, …, b, where b is the total number of blocks of length m in the plaintext.
Output: The $\boldsymbol{C}^{(1)}$, $\boldsymbol{C}^{(2)}$, …, $\boldsymbol{C}^{(b)}\in Z_n$, $m\times 1$ ciphertext column vectors.
Main Procedure:
1. for i=1 to b do
   1.a if (i==1) then
      $\boldsymbol{K}_i=\boldsymbol{K}$;
   1.b else
      $\boldsymbol{K}_i=mod\_Key(\boldsymbol{K}_{i-1}, \boldsymbol{IV})$;
   1.c end if
   1.d $\boldsymbol{C}^{(i)}=\boldsymbol{K}_i\cdot\boldsymbol{P}^{(i)}$ mod n;
2. end for
3. Return($\boldsymbol{C}^{(1)}$, $\boldsymbol{C}^{(2)}$, …, $\boldsymbol{C}^{(b)}$);

Fig.2 HillMRIV algorithm (Ismail *et al*., 2006)

Ismail *et al*.(2006) also noted that the Hill cipher can be directly adopted for encrypting grayscale images by defining an alphabet of 256 symbols, i.e., using n=256. Moreover, they report the strength of their scheme by producing encrypted images with low degree of correlation with respect to the original image.

Nevertheless, as shown in the rest of this paper, the HillMRIV still has severe security flaws. We will show in the next section that the HillMRIV scheme can be attacked in a number of ways, most of them being slight variations of the attacks previously reported on the original Hill scheme.

ATTACKS

Perhaps the most natural attack against the HillMRIV scheme can be launched observing that according to Eq.(3), the first block of every message is encrypted using a key matrix $\boldsymbol{K}_1$ that is still identical to the one defined in the original Hill scheme. If the encrypting entity utilizes the same key across several messages (a relatively common practice in symmetric cryptography), then a passive attacker would just need to collect m pairs of column vectors $(\boldsymbol{P}_i^{(1)},\boldsymbol{C}_i^{(1)})$ as defined in the algorithm of Fig.2, in order to be able to launch the same known-plaintext attack as described in the preceding section against the original Hill cipher. Once the attacker has the master key matrix $\boldsymbol{K}$, it is trivial to find the initial vector $\boldsymbol{IV}$ by solving a set of equations. For easy illustration, a simple example for the case m=2 is described next.

Let us assume that by launching the attack described above, an attacker has been able to obtain the value of the 2×2 master key matrix $\boldsymbol{K}_1$, given as

$$\boldsymbol{K}_1=\begin{bmatrix} a & b \\ c & d \end{bmatrix}. \tag{4}$$

Then, we want to find the two coefficients of the initial vector, say, $\boldsymbol{IV}$=[e, f]. From the algorithm of Fig.1, $\boldsymbol{K}_2$ is given as

$$\boldsymbol{K}_2=\begin{bmatrix} ae+cf & be+df \\ (ae+cf)e+cf & (be+df)e+df \end{bmatrix}.$$

According to the algorithm of Fig.2, the key $\boldsymbol{K}_2$ is used to encrypt the second plaintext block, namely, $\boldsymbol{P}^{(2)}=[p_3, p_4]^{\mathrm{T}}$, as shown next,

$$\begin{Bmatrix} c_3 \\ c_4 \end{Bmatrix}=\begin{bmatrix} ae+cf & be+df \\ (ae+cf)e+cf & (be+df)e+df \end{bmatrix}\begin{Bmatrix} p_3 \\ p_4 \end{Bmatrix} \bmod n,$$

which implies

$$\begin{cases} c_3=[(ae+cf)p_3+(be+df)p_4] \bmod n, \\ c_4=\{[(ae+cf)e+cf]p_3+[(be+df)e+df]p_4\} \bmod n. \end{cases}$$

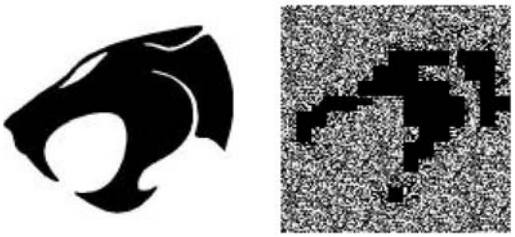
Assuming that the attacker already knows the four coefficients of the matrix $\boldsymbol{K}_1$ in Eq.(4), then the above two equations are sufficient for finding the two unknown $\boldsymbol{IV}$ coefficients as

$$e=\frac{c_3-c_4}{ap_3+bp_4-c_3} \bmod n,$$

$$f=\frac{ap_3c_4+bp_4c_4-c_3^2}{acp_3^2+adp_3p_4+bcp_3p_4-cp_3c_3-dp_4c_3+bdp_4^2} \bmod n.$$

A second attack can be launched if the HillMRIV scheme is utilized for encrypting images. As it was already mentioned, Ismail *et al*.(2006) proposed to use their scheme for encrypting grayscale images in an alphabet of 256 symbols.

However, let us recall that according to the HillMRIV algorithm of Fig.2, if all the characters in a plaintext block are zeroes, then $\boldsymbol{P}^{(i)}=\boldsymbol{C}^{(i)}=\boldsymbol{0}$. Since in the standard grayscale, black pixels are mapped to zero, the suggested application may become problematic for those images having significant portions of pixels in black. This situation is illustrated in Fig.3.



(a) (b)

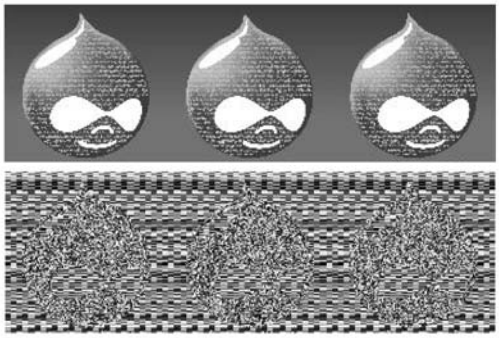
Fig.3 Encrypting a black background image. (a) Original image; (b) Encrypted image

Yet another weakness of the HillMRIV scheme lies in the selection of the initial vector ***IV***. In (Ismail *et al*., 2006), it was stated that ***IV*** could be chosen at random. Nevertheless, this is not the case. If this vector is not chosen carefully, some of the new keys to be generated by algorithm of Fig.1 may not be invertible over Z_n, which will make them useless for encryption/decryption purposes. More specifically, the algorithm shown in Fig.1 defines a cyclic group of finite order, i.e., sooner or later we will return to the original key matrix $\boldsymbol{K}_1$. The order of the cyclic group depends on the selection of both $\boldsymbol{K}_1$ and ***IV***. In particular, given a fixed key matrix $\boldsymbol{K}_1$, bad selections of ***IV*** will cause shorter periods. For example if m=2, the choice

$$\boldsymbol{K}_1=\begin{bmatrix}2 & 3\\ 5 & 7\end{bmatrix},\quad \boldsymbol{IV}=[5\ \ 7] \tag{5}$$

would define a cyclic group that will produce just 384 different key matrices. This limited number of key matrices can be exploited by an attacker when a relatively large plaintext image is being encrypted, even if the image has not all-zero plaintext blocks.

In order to illustrate this scenario, we encrypted the image shown in Fig.4a using the parameters given in Eq.(5). We obtained the encrypted image shown in Fig.4b. Clearly, the resulting encrypted image keeps many characteristics of the plaintext image.



(a)

(b)

Fig.4 (a) A plaintext image; (b) Encryption of the image in (a) using the parameters given in Eq.(5)

CONCLUSION

We have shown that the modified Hill cryptosystem HillMRIV has severe security flaws by describing three different attacks. Firstly, we show that when encrypting several images, the HillMRIV scheme should not repeat the same Hill key matrix $\boldsymbol{K}_1$. Otherwise, the scheme can be easily attacked using a standard known-plaintext attack identical to the one utilized against the original Hill cipher. Second, those plaintexts with many all-zero blocks will not be protected by the HillMRIV scheme. Finally, any wrong choice of $\boldsymbol{K}_1$ and the initial vector ***IV*** could lead to disastrous situations. Other potential attacks can be mounted observing that if ***IV*** is somehow compromised, then the HillMRIV scheme reverts to a standard Hill cipher. Hence, a determined attacker can launch a combination of chosen-plaintext and brute force attack by trying all possible values of ***IV***. In the case of m=2, n=256, there exist at most 2^{16} different ***IV***'s, implying a protection of only 16 bits, which is insufficient for modern cryptographic applications.

References

Hill, L.S., 1929. Cryptography in an algebraic alphabet. *The American Mathematical Monthly*, **36**:306-312. [doi:10.2307/2298294]

Hill, L.S., 1931. Concerning certain linear transformation apparatus of cryptography. *The American Mathematical Monthly*, **38**:135-154. [doi:10.2307/2300969]

Ismail, I.A., Amin, M., Diab, H., 2006. How to repair the Hill cipher. *J. Zhejiang Univ. Sci. A*, **7**(12):2022-2030. [doi:10.1631/jzus.2006.A2022]

Overbey, J., Traves, W., Wojdylo, J., 2005. On the keyspace of the Hill cipher. *Cryptologia*, **29**(1):59-72. [doi:10.1080/0161-110591893771]

Saeednia, S., 2000. How to make the Hill cipher secure? *Cryptologia*, **24**(4):353-360. [doi:10.1080/01611190008984253]

Trappe, W., Washington, L.C., 2006. Introduction to Cryptography with Coding Theory (2nd Ed.). Prentice Hall.