The Hill Cipher: A Weakness Studied Through Group Action Theory

Florent Dewez, Valentin Montmirail

The Hill Cipher: A Weakness Studied Through Group Action Theory

Florent Dewez[1] and Valentin Montmirail[2]

[1] Univ. Valenciennes, EA 4015 - LAMAV, FR CNRS 2956,
F-59313 Valenciennes, France
florent.dewez@outlook.com
[2] CRIL, Artois University and CNRS, F62300 Lens, France
valentin.montmirail@cril.fr

Abstract. The Hill cipher is considered as one of the most famous symmetric-key encryption algorithm: based on matrix multiplication, it has some interesting structural features which, for instance, can be exploited for teaching both cryptology and linear algebra. On the other hand, these features have rendered it vulnerable to some kinds of attack, such as the known-plaintext attack, and hence inapplicable in cases of real application. Despite this weakness, it does not stop the community proposing different upgrades for application purposes. In the present paper, we show that the Hill cipher preserves an algebraic structure of a given text and we use group action theory to study in a convenient setting some consequences of this fact, which turns out to be a potentially exploitable weakness. Indeed, our study might lead to a ciphertext-only attack requiring only that the alphabet has a prime number of characters. The main feature of this potential attack is the fact that it is not based on a search over all possible keys but rather over an explicit set of texts associated with the considered ciphertext. Group action theory guarantees that there will be, at worst, as much texts to test as keys, implying especially a better complexity.

Keywords: Symmetric Encryption, Hill Cipher, Mathematical Analysis, Cryptanalysis, Group Action Theory

1 Introduction

The Hill cipher is a relatively old polygraphic substitution cipher based on linear algebra and invented by Lester S. Hill in 1929 [1,2]. For a plaintext of M characters composed of m blocks of n characters in an alphabet with p elements, the Hill cipher considers each block as an element of the vector space $(\mathbb{Z}_p)^n$ and multiplies each block by the same $n \times n$ invertible matrix, which is actually the secret key, to compute the whole ciphertext. As explained in the abstract, the Hill cipher is proved to be vulnerable to cryptanalysis attacks. Because of its linear nature, it suffers from the known-plaintext attack, *i.e.* attacker can obtain one or more plaintexts and their corresponding ciphertexts, as stated in [3]. This weakness has lead to many modifications of the original version of this

cipher to correct it [4,5,6,7,8,9]. Let us mention that some of these papers try to modify the Hill cipher by combining what is done in AES (Advanced Encryption Standard) [10] with an interlacing approach at each iteration [11].

We mention also that the most famous versions of the Hill cipher are probably the two Toorani-Falahati-Hill ciphers [8,9]. These two versions have already been applied in many applications such as Cloud Storage [12], Image Encryption in Steganography [13], Biometric-based Authentication [14] or Software Copy Protection [15]. Nevertheless even such clever modifications, which are aimed at being applied in real situations, may be vulnerable to attacks [16,17]: this makes the research for a robust Hill cipher version interesting. We refer to [18] for a recent detailed review of the existing modifications of the Hill cipher.

In order to perform ciphertext-only attacks, *i.e.* attacker can obtain one or more ciphertexts, approaches based on smart combinations between linear algebra, arithmetical and statistical arguments have been developed under the strong assumption that "the text consists of meaningful English words" with an alphabet having 26 letters [19,20,21,22]. Roughly speaking, these methods consist mainly in recovering the key matrix row by row or column by column by exploiting statistical tools together with data on frequencies of occurrence of n-grams in the English language.

However, in the case of no restrictions on the considered language or alphabet, "the best publicly known ciphertext-only attack on Hill cipher requires full search over all possible secret keys", as it is recently stated in [22]. In the case where p is a prime number, this brute-force tests all the p^{n^2} matrices since the ratio of $n \times n$ matrices that are invertible is very close to 1 in this case [23, Lemma 4.3]. Thus without considering any fast algorithm for matrix multiplication, such as Strassen's method [24] that would not lead to a significant improvement, the complexity to perform a ciphertext-only attack is $\mathcal{O}(n^3 \times p^{n^2})$.

In view of this, we propose in the present paper to analyse an intrinsic property of the Hill cipher, which does not seem to be treated or exploited in the literature, to the best of our knowledge. We study also some of its consequences which, in particular, might create a new ciphertext-only attack or might improve existing ones. More precisely the property we focus on is the fact that the Hill cipher preserves the linear combinations of blocks of a given text. This has strong impacts on the set of ciphertexts (resp. plaintexts) which can be obtained from a given plaintext (resp. ciphertext) via the Hill encryption (resp. decryption) function, as we will show in this paper. To describe that in a explicit and rigorous way, we will employ results from group action theory. Let us also emphasise that our method requires only that the size of the alphabet is a prime number. As mentioned above, this work might lead for instance to a new ciphertext-only attack where the attacker would make an elegant search in the text-space to perform a brute-force instead of in the usual key-space, because group action theory assures that the number of plaintexts to test is smaller than the number of keys.

2 Preliminaries

There exist two types of encryption, namely symmetric-key and asymmetric-key encryptions. Here we will discuss exclusively about symmetric-key encryption and we redirect you to [25] for more information on the differences between symmetric and asymmetric-key encryptions.

2.1 Symmetric-key encryption and Hill cipher

We talk about symmetric encryption when both Alice and Bob use the same key k to encrypt and decrypt a text. They are supposed to keep their shared key secret. Alice encrypts her plaintext X with an encryption algorithm $\mathcal{E}$ which uses the shared key k. She then obtains a ciphertext $Y = \mathcal{E}(X, k)$ and sends Y to Bob. At the reception, Bob uses a decryption algorithm $\mathcal{D}$ and the same key k to recover the plaintext $X = \mathcal{D}(Y, k)$.

Definition 1 (Symmetric-key encryption schema). *A schema $\mathcal{E} : \mathcal{K} \times \mathbb{PT} \to \mathbb{CT}$ is called a symmetric-key encryption schema, where $\mathbb{PT}$ is the set of plaintexts and $\mathbb{CT}$ is the set of ciphertexts, if it has the property that for each key k in the key-space $\mathcal{K}$, the encryption function $\mathcal{E}_k : \mathbb{PT} \to \mathbb{CT}, X \to \mathcal{E}(k, X)$ is invertible. The inverse of $\mathcal{E}_k$ is called the decryption function and is noted $\mathcal{D}_k$.*

A security requirement for $\mathcal{E}$ in Def. 1 is that it should be impossible[3] to successfully execute the good decryption function $\mathcal{D}_k$ without owning the key k. The Hill cipher is one example of a Symmetric-key encryption schema. The definition of this cipher we propose here is slightly different from the original version [1], but the schema stays the same.

Definition 2 (The Hill cipher). *A plaintext string X of size M over an alphabet having p characters is defined as a vector of size M over $\mathbb{Z}_p$ using an arbitrary bijection between the elements of the alphabet and the elements of $\mathbb{Z}_p$. The plaintext X is splitted into m blocs of size n such that $X = X_1 X_2 \dots X_m$. An invertible $n \times n$ matrix K over $\mathbb{Z}_p$, called the key-matrix, is then chosen. Afterwards we construct a block diagonal matrix A whose main diagonal submatrices are equal to K. The encryption is finally performed by considering each X_i as a vector of $(\mathbb{Z}_p)^n$ and by computing the ciphertext $Y = Y_1 Y_2 \dots Y_m$ as follows:*

$$Y = A\ X\ (mod\ p)\ ,$$

which is equivalent to $Y_i = K \times X_i\ (mod\ p)$, for all $i \in \{1, \dots, m\}$. Thanks to the invertible nature of K, A is invertible as well and the decryption is performed by computing:

$$X = A^{-1}\ Y\ (mod\ p)\ .$$

In the case of a key $K = (k_{ij})$ of size 3×3, the matrix A introduced in the preceding definition is a 9×9 block diagonal matrix whose blocks are given by

[3] At least computationally impossible

$$A = \begin{pmatrix} \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} & \mathbf{0_3} & \mathbf{0_3} \\ \mathbf{0_3} & \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} & \mathbf{0_3} \\ \mathbf{0_3} & \mathbf{0_3} & \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \end{pmatrix}$$

Fig. 1. Value of A with $n = 3$

the key K; see Fig.1 for an illustration of such a matrix A. We precise that each "$\mathbf{0_3}$" appearing in this figure is the null matrix of size 3×3. The Hill cipher being now defined, let us now formalise it by using the frame of Def. 1. Before that, let us precise that, for the sake of simplicity, we choose p as a prime number throughout the rest of the present paper. This implies in particular that the set $\mathbb{Z}_p$ is the field of p elements in this case. Because of the nature of the Hill cipher, $\mathbb{PT}$ and $\mathbb{CT}$ are given by the same set $(\mathbb{Z}_p)^M$. Now we introduce the following set of matrices $\mathcal{G}_{M,n}$ in order to define properly the key-space $\mathcal{K}$:

Definition 3. *Let $\mathcal{G}_{M,n} \subset GL_M(\mathbb{Z}_p)$, where $GL_M(\mathbb{Z}_p)$ is the space of invertible matrices of size $M \times M$ over $\mathbb{Z}_p$, be the set defined as follows*

$$A \in \mathcal{G}_{M,n} \qquad \Longleftrightarrow \qquad \exists\, K \in GL_n(\mathbb{Z}_p) \quad A = \begin{pmatrix} K & & & \\ & K & & \\ & & \ddots & \\ & & & K \end{pmatrix} .$$

Since the sets $GL_n(\mathbb{Z}_p)$ and $\mathcal{G}_{M,n}$ are clearly in bijection, we identify the key-space $\mathcal{K}$ to $GL_n(\mathbb{Z}_p)$. Putting everything together, we are in position to define the "Hill cipher map" (or "Hill cipher schema") which will be proved to be a group action in the following section.

Definition 4 (Hill cipher map). *Let $\mathcal{H} : \mathcal{G}_{M,n} \times (\mathbb{Z}_p)^M \longrightarrow (\mathbb{Z}_p)^M$ be the map defined by*

$$\forall\, (A, X) \in \mathcal{G}_{M,n} \times (\mathbb{Z}_p)^M \qquad \mathcal{H}(A, X) := AX \ .$$

2.2 Existing results on group action theory

In this short section, we state some results from group action theory which will furnish a convenient setting in the next section to study the Hill cipher. For the sake of clarity, we provide only the statements of the results and not their proofs, which can be found for instance in [26, Chapter 10]. The results presented here will be interpreted in Sec. 3 in the frame of the Hill cipher.

In the rest of the present section, the notation G will refer to a group whose group law and identity element are respectively represented by $\cdot$ and e.

We start by recalling the notion of a (left) group action on a set.

Definition 5 (Group action). *Let G be a group and S a set. A map $\varphi : G \times S \longrightarrow S$ is said to be a group action of G on S if and only if it satisfies the two following properties:*

- Identity: $\forall\, s \in S \quad \varphi(e, s) = s$
- Compatibility: $\forall\, g, h \in G \quad \forall\, s \in S \quad \varphi(g \cdot h, s) = \varphi\big(g, \varphi(h, s)\big)$

We define now the orbit and the stabiliser of an element $s \in S$: the orbit of s is actually the set of elements of S to which s can be sent by the elements of G while the stabiliser of s is the set of elements of the group G which do not make move s. Let us emphasise that an element s of S can not be sent outside its orbit by definition.

Definition 6 (Orbit and stabiliser). *Let $\varphi : G \times S \longrightarrow S$ be a group action of a group G on a set S and let $s \in S$.*

1. *The orbit $Orb_\varphi(s)$ of s is defined as follows:*
$$Orb_\varphi(s) = \big\{ y \in S \;\big|\; \exists\, g \in G \quad y = \varphi(g, s) \big\} \; .$$
2. *The stabiliser $Stab_\varphi(s)$ of s is defined as follows:*
$$Stab_\varphi(s) = \big\{ g \in G \;\big|\; \varphi(g, s) = s \big\} \; .$$

These two notions are closely related as shown in the following result:

Theorem 1. *Let $\varphi : G \times S \longrightarrow S$ be a group action of a group G on a set S and let $s \in S$. Then the orbit of s is isomorph to the quotient of the group G by the stabiliser of s,* i.e.
$$Orb_\varphi(s) \simeq G / Stab_\varphi(s) \; .$$

Roughly speaking, this theorem claims that it is sufficient to make move s by all the elements of the group G which do not fix it to recover all the elements of the orbit of s.

A direct consequence of the preceding result in the case of finite groups, namely the cardinal of the group is finite, is the equality of the cardinal of the orbit of a given element $s \in S$ with the quotient of the cardinals of the group G and of the stabiliser of s.

Corollary 1. *Let $\varphi : G \times S \longrightarrow S$ be a group action of a finite group G on a set S and let $s \in S$. Then we have*
$$\big|Orb_\varphi(s)\big| = \frac{\big|G\big|}{\big|Stab_\varphi(s)\big|} \; ,$$
where $|Z|$ denotes the cardinal of a given set Z.

To conclude this subsection, we mention that an action of a group G on a set S defines an equivalence relation on S whose equivalence classes are given by the orbits. Since two equivalence classes are either equal or disjoint, the set of the orbits under the action of G forms a partition of S; this is recalled in the following result:

Theorem 2. *Let $\varphi : G \times S \longrightarrow S$ be a group action of a group G on a set S.*

1. *Let $s, t \in S$. Then we have either $Orb_\varphi(s) = Orb_\varphi(t)$ or $Orb_\varphi(s) \cap Orb_\varphi(t) = \emptyset$.*
2. *Let $\mathcal{R} \subseteq S$ be a set of orbit representatives, in other words a subset of S which contains exactly one element from each orbit. Then the family $\left\{Orb_\varphi(s)\right\}_{s\in\mathcal{R}}$ forms a partition of S.*

An illustration of the Theo. 2 is given in Fig. 2.

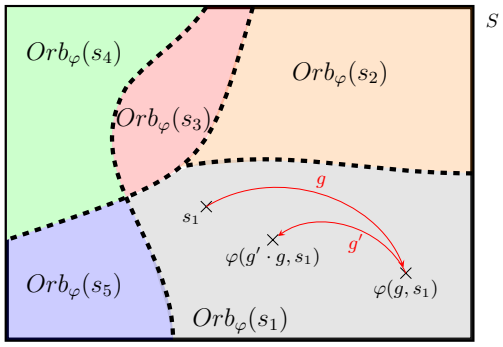

Fig. 2. Illustration of the partition of S created by the group action φ

3 Applications of group action theory to Hill cipher

As explained in the introduction, the Hill cipher preserves the linear combinations of a given plaintext. We state this result in the following proposition:

Proposition 1. *Let $X = X_1 \dots X_m \in (\mathbb{Z}_p)^M$ be a plaintext. Suppose that the block X_i is a linear combination of q other blocks $X_{i_1}, \dots, X_{i_q}$,* i.e.

$$X_i = \sum_{k=1}^{q} \lambda_k^{(i)} X_{i_k} \ , \tag{1}$$

where $\lambda_k^{(i)} \in \mathbb{Z}_p$. Then the i-th block of the ciphertext $Y = \mathcal{H}(A, X)$, with A an element of $\mathcal{G}_{M,n}$ associated with a key-matrix $K \in GL_n(\mathbb{Z}_p)$, satisfies

$$Y_i = \sum_{k=1}^{q} \lambda_k^{(i)} Y_{i_k} \ .$$

Proof. Since we have $Y_i = KX_i$ for all $i \in \{1, \dots, m\}$, it sufficient to multiply equality (1) by K to obtain the result.

Our goal in the present section is to study some consequences of this property. Especially, we shall exhibit an algebraic structure of the text-space $(\mathbb{Z}_p)^M$ inherited from the Hill cipher: this is actually a theoretical weakness which might be exploited to improve some attacks. In order to structure our argument, we will employ results from group action theory which have been recalled in Subsec. 2.2.

It is important to note that, the Hill cipher being a symmetric-key encryption, the results presented here can be interpreted in two ways: the relation $Y = \mathcal{H}(A, X)$ can describe either the encryption of the plaintext X leading to the ciphertext Y, or the decryption of a ciphertext X leading to the plaintext Y. For the sake of clarity, we will define an input text X that can be a plaintext (resp. ciphertext) and the output text Y that can be a ciphertext (resp. plaintext) if we consider an encryption (resp. decryption).

We start this section by showing that the Hill cipher map given in Def. 4 is actually a group action. This is a direct consequence of the basic properties of matrix multiplication.

Theorem 3. *The Hill cipher map given in Def. 4 is a group action.*

Proof. First of all, it is easy to show that the set $\mathcal{G}_{M,n}$ is actually a subgroup of $GL_M(\mathbb{Z}_p)$, so it is itself a group. Now let us prove that the map $\mathcal{H} : \mathcal{G}_{M,n} \times (\mathbb{Z}_p)^M \longrightarrow (\mathbb{Z}_p)^M$ satisfies the two points of Def. 5:

- *Identity.* This point is clear since:
$$\forall\, X \in (\mathbb{Z}_p)^M \qquad \mathcal{H}(I_M, X) = I_M X = X \ ,$$
where I_M is the identity matrix of $GL_M(\mathbb{Z}_p)$.
- *Compatibility.* Let $A, B \in \mathcal{G}_{M,n}$ and $X \in (\mathbb{Z}_p)^M$. Then, by the associativity of matrix multiplication, we have
$$\mathcal{H}(AB, X) = (AB)X = A(BX) = \mathcal{H}\big(A, \mathcal{H}(B, X)\big) \ .$$

The proof is now complete. □

Thanks to the preceding theorem, we are in position to apply Theo. 2 and Cor. 1 to the Hill cipher map $\mathcal{H}$. As a first result, the text-space is split into orbits which are stable under the Hill cipher map; in other words, if we choose an input text and we apply the Hill cipher map to it, then the resulting output text is again in the orbit of the input text. The second result we provide gives a theoretical formula for the number of elements of a given orbit.

Corollary 2. *1. Let $X, X' \in (\mathbb{Z}_p)^M$. Then we have either $Orb_{\mathcal{H}}(X) = Orb_{\mathcal{H}}(X')$ or $Orb_{\mathcal{H}}(X) \cap Orb_{\mathcal{H}}(X') = \emptyset$.*

2. Let $\mathcal{X} \subseteq (\mathbb{Z}_p)^M$ be a set of orbit representatives, in other words a subset of texts which contains exactly one text from each orbit. Then the family $\big\{Orb_{\mathcal{H}}(X)\big\}_{X \in \mathcal{X}}$ forms a partition of $(\mathbb{Z}_p)^M$.

3. For all $X \in (\mathbb{Z}_p)^M$, we have
$$\big|Orb_{\mathcal{H}}(X)\big| = \frac{\big|GL_n(\mathbb{Z}_p)\big|}{\big|Stab_{\mathcal{H}}(X)\big|} \ .$$

Proof. Simple application of Theo. 2 and Cor. 1. □

What is important to notice here is that a given input text will stay in its orbit after being encrypted (resp. decrypted) by the Hill cipher: it can not be sent to any element of the text-space, as illustrated in Fig. 2 in an abstract setting.

According to Cor. 2, the number of elements of an orbit given by an input text X depends on the cardinal of the stabiliser of X. In the following proposition, we describe explicitly the stabiliser of any input text X by exploiting the property that the Hill cipher preserves linear combinations (see Prop. 1); in particular, this will permit to derive the cardinal of the orbit of X in Cor. 3.

In favour of readability, we divide the statement of the following proposition into two cases: the case of n linearly independent blocks in the input text and the case of q linearly independent blocks, where $1 \leqslant q < n$. In the first case, the existence of n linearly independent blocks implies that the only matrix in $\mathcal{G}_{M,n}$ which does not change the input text is the identity matrix. In the second case, a matrix in the stabiliser of the input text is defined through the key-matrix K which have to be equal to the identity on the subspace generated by the q linearly independent blocks but which may be equal to anything on the complement of this subspace. Finally let us mention that we do not treat the case of the input text given by $0_{(\mathbb{Z}_p)^M}$ since any matrix belonging to $\mathcal{G}_{M,n}$ is in its stabiliser.

Proposition 2. *Let $X = X_1 \dots X_m \in (\mathbb{Z}_p)^M \setminus \left\{0_{(\mathbb{Z}_p)^M}\right\}$.*

1. *Suppose that there exist $i_1, \dots, i_n \in \{1, \dots, m\}$ such that $X_{i_1}, \dots, X_{i_n}$ are linearly independent. Then we have*
$$Stab_{\mathcal{H}}(X) = \{I_M\} .$$
2. *Suppose that there exist $q \in \{1, \dots, n-1\}$ and $i_1, \dots, i_q \in \{1, \dots, m\}$ such that $X_{i_1}, \dots, X_{i_q}$ are linearly independent and, for each $i \notin \{i_1, \dots, i_q\}$, X_i is a linear combination of $X_{i_1}, \dots, X_{i_q}$. Then we have*
$$A \in Stab_{\mathcal{H}}(X) \quad \Longleftrightarrow \quad A = \begin{pmatrix} P\widetilde{K}P^{-1} & & & \\ & P\widetilde{K}P^{-1} & & \\ & & \ddots & \\ & & & P\widetilde{K}P^{-1} \end{pmatrix},$$
with
   - *$P = \left(X_{i_1} \middle| \dots \middle| X_{i_q} \middle| V_{q+1} \middle| \dots \middle| V_n\right)$ where $V_{q+1}, \dots, V_n$ are vectors of $(\mathbb{Z}_p)^n$ such that $\left\{X_{i_1}, \dots, X_{i_q}, V_{q+1}, \dots, V_n\right\}$ is a basis of $(\mathbb{Z}_p)^n$;*
   - *$\widetilde{K} \in GL_n(\mathbb{Z}_p)$ is of the form*
$$\begin{pmatrix} 1 & 0 & \dots & 0 & \tilde{k}_{1,q+1} & \dots & \tilde{k}_{1,n} \\ 0 & 1 & \ddots & 0 & \tilde{k}_{2,q+1} & \dots & \tilde{k}_{2,n} \\ \vdots & \ddots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 1 & \tilde{k}_{q,q+1} & \dots & \tilde{k}_{q,n} \\ 0 & \dots & \dots & 0 & \tilde{k}_{q+1,q+1} & \dots & \tilde{k}_{q+1,n} \\ \vdots & & & \vdots & \vdots & & \vdots \\ 0 & \dots & \dots & 0 & \tilde{k}_{n,q+1} & \dots & \tilde{k}_{n,n} \end{pmatrix}. \tag{2}$$

Proof. Choose $X = X_1 \dots X_m \in (\mathbb{Z}_p)^M \setminus \{0_{(\mathbb{Z}_p)^M}\}$.

1. Suppose that $X_{i_1}, \dots, X_{i_n}$ are linearly independent, where $i_1, \dots, i_n \in \{1, \dots, m\}$.
   $\boxed{\supseteq}$ This point is clear since $I_M X = X$.
   $\boxed{\subseteq}$ Let A be an element of $Stab_{\mathcal{H}}(X)$; in particular, A belongs to $\mathcal{G}_{M,n}$ and hence
   $$AX = X \qquad \Longleftrightarrow \qquad \forall\, i \in \{1, \dots, m\} \quad KX_i = X_i \ ,$$
   where $K \in GL_n(\mathbb{Z}_p)$ is the key-matrix. Since the vectors $X_{i_1}, \dots, X_{i_n}$ are linearly independent, the family $\{X_{i_1}, \dots, X_{i_n}\}$ is a basis of $(\mathbb{Z}_p)^n$. Hence the linear application associated with the matrix K is equal to the application identity on a basis of $(\mathbb{Z}_p)^n$. Therefore we have $K = I_M$, implying finally $A = I_M$.
2. Assume that $X_{i_1}, \dots, X_{i_q}$ are linearly independent, where $1 \leqslant q < n$ and $i_1, \dots, i_q \in \{1, \dots, m\}$, and that
   $$\forall\, i \notin \{i_1, \dots, i_q\} \quad \exists\, \lambda_1^{(i)}, \dots, \lambda_q^{(i)} \in \mathbb{Z}_p \qquad X_i = \sum_{k=1}^{q} \lambda_k^{(i)}\, X_{i_k} \ .$$
   Now choose $V_{q+1}, \dots, V_n \in (\mathbb{Z}_p)^n$ such that the family $\{X_{i_1}, \dots, X_{i_q}, V_{q+1}, \dots, V_n\}$ is a basis of $(\mathbb{Z}_p)^n$; let us mention that such vectors exist according to the incomplete basis theorem [27, Proposition 3.15]. Hence the matrix P defined in the statement of Prop. 2 is invertible and satisfies for all $k \in \{1, \dots, q\}$,
   $$PE_k = X_{i_k} \qquad \Longleftrightarrow \qquad P^{-1} X_{i_k} = E_k \ , \tag{3}$$
   where E_k is the k-th vector of the canonical basis of $(\mathbb{Z}_p)^n$. Furthermore, for a given matrix $\widetilde{K}$ of the form (2), the following relation is true for each $k \in \{1, \dots, q\}$,
   $$P\widetilde{K}P^{-1} X_{i_k} = P\widetilde{K}E_k = PE_k = X_{i_k} \ . \tag{4}$$
   Then we deduce that, for all $i \notin \{i_1, \dots, i_q\}$,
   $$P\widetilde{K}P^{-1} X_i = P\widetilde{K}P^{-1} \left(\sum_{k=1}^{q} \lambda_k^{(i)}\, X_{i_k} \right) = \sum_{k=1}^{q} \lambda_k^{(i)} P\widetilde{K}P^{-1} X_{i_k} = \sum_{k=1}^{q} \lambda_k^{(i)}\, X_{i_k} = X_i \ . \tag{5}$$
   We are now in position to prove the equivalence stated in Prop. 2.2.
   $\boxed{\Leftarrow}$ If a matrix $A \in \mathcal{G}_{M,n}$ is given by
   $$A = \begin{pmatrix} P\widetilde{K}P^{-1} & & & \\ & P\widetilde{K}P^{-1} & & \\ & & \ddots & \\ & & & P\widetilde{K}P^{-1} \end{pmatrix} ,$$
   where $\widetilde{K}$ is an invertible matrix of the form (2), then A satisfies
   $$AX = \begin{pmatrix} P\widetilde{K}P^{-1} & & & \\ & P\widetilde{K}P^{-1} & & \\ & & \ddots & \\ & & & P\widetilde{K}P^{-1} \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_m \end{pmatrix} = \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_m \end{pmatrix} = X \ ,$$

according to the relations (4) and (5). This proves that $A \in Stab_{\mathcal{H}}(X)$.

$\boxed{\Rightarrow}$ Let $A \in \mathcal{G}_{M,n}$ be an element of the stabiliser of X. It follows

$$\forall\, k \in \{1, \ldots, q\} \qquad KX_{i_k} = X_{i_k} \ ,$$

where $K \in GL_n(\mathbb{Z}_p)$ is the key-matrix. Hence, by using relation (3), we obtain

$$\forall\, k \in \{1, \ldots, q\} \qquad P^{-1}KPE_k = E_k \ .$$

We observe then that the matrix $\widetilde{K} := P^{-1}KP$ is of the form (2) and is invertible since $K \in GL_n(\mathbb{Z}_p)$. This finally proves that

$$A = \begin{pmatrix} P\widetilde{K}P^{-1} & & & \\ & P\widetilde{K}P^{-1} & & \\ & & \ddots & \\ & & & P\widetilde{K}P^{-1} \end{pmatrix} \ .$$

□

As a consequence of the preceding result, we are able to give the cardinal of the orbit of any input text, *i.e.* the number of texts which can be attained from this input. We note that this cardinal depends actually only on the number of linearly independent blocks of the input text according to Prop. 2.

The proof of the following corollary consists in a combination of the preceding result, which permits to determine the cardinal of the stabiliser of a given input text, with Cor. 2.

Corollary 3. *Let* $X = X_1 \ldots X_m \in (\mathbb{Z}_p)^M \setminus \left\{0_{(\mathbb{Z}_p)^M}\right\}$.

1. *Suppose that there exist* $i_1, \ldots, i_n \in \{1, \ldots, n\}$ *such that* $X_{i_1}, \ldots, X_{i_n}$ *are linearly independent. Then we have*

$$\left|Orb_{\mathcal{H}}(X)\right| = \prod_{k=0}^{n-1} \left(p^n - p^k\right) \ .$$

2. *Suppose that there exist* $q \in \{1, \ldots, n-1\}$ *and* $i_1, \ldots, i_q \in \{1, \ldots, m\}$ *such that* $X_{i_1}, \ldots, X_{i_q}$ *are linearly independent and, for each* $i \notin \{i_1, \ldots, i_q\}$, X_i *is a linear combination of* $X_{i_1}, \ldots, X_{i_q}$. *Then we have*

$$\left|Orb_{\mathcal{H}}(X)\right| = \prod_{k=0}^{q-1} \left(p^n - p^k\right) \ .$$

Proof. First of all, let us recall that the cardinal of $GL_n(\mathbb{Z}_p)$ is given by

$$\left|GL_n(\mathbb{Z}_p)\right| = \prod_{k=0}^{n-1} \left(p^n - p^k\right) \ .$$

1. According to Prop. 2.1, we have in the present case

$$Stab_{\mathcal{H}}(X) = \{I_M\} \ .$$

Hence $\left|Stab_{\mathcal{H}}(X)\right| = 1$ and, by employing Cor. 2.2, we obtain

$$\left|Orb_{\mathcal{H}}(X)\right| = \frac{\left|GL_n(\mathbb{Z}_p)\right|}{\left|Stab_{\mathcal{H}}(X)\right|} = \frac{\displaystyle\prod_{k=0}^{n-1}\left(p^n - p^k\right)}{1} = \prod_{k=0}^{n-1}\left(p^n - p^k\right) \ .$$

2. As above, we determine first the cardinal of $Stab_{\mathcal{H}}(X)$ in the present case, which is actually equal to the number of invertible matrices of the form (2), namely

$$\begin{pmatrix} 1 & 0 & \dots & 0 & \tilde{k}_{1,q+1} & \dots & \tilde{k}_{1,n} \\ 0 & 1 & \ddots & 0 & \tilde{k}_{2,q+1} & \dots & \tilde{k}_{2,n} \\ \vdots & \ddots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 1 & \tilde{k}_{q,q+1} & \dots & \tilde{k}_{q,n} \\ 0 & \dots & \dots & 0 & \tilde{k}_{q+1,q+1} & \dots & \tilde{k}_{q+1,n} \\ \vdots & & & \vdots & \vdots & & \vdots \\ 0 & \dots & \dots & 0 & \tilde{k}_{n,q+1} & \dots & \tilde{k}_{n,n} \end{pmatrix} = \left(\begin{array}{c|c} I_q & \widetilde{K}_{1,2} \\ \hline 0 & \widetilde{K}_{2,2} \end{array}\right) \ .$$

Such a matrix being invertible, the sub-matrix $\widetilde{K}_{2,2}$ is invertible as well; hence we have

$$\prod_{k=0}^{n-q-1}\left(p^{n-q} - p^k\right)$$

choices for the sub-matrix $\widetilde{K}_{2,2}$. Once this sub-matrix is fixed, it remains to choose $\widetilde{K}_{1,2}$, which does not have any restriction: thus there are $p^{q(n-q)}$ choices for the sub-matrix $\widetilde{K}_{1,2}$. Consequently, we obtain

$$\left|Stab_{\mathcal{H}}(X)\right| = p^{q(n-q)} \prod_{k=0}^{n-q-1}\left(p^{n-q} - p^k\right) = \prod_{k=0}^{n-q-1}\left(p^n - p^{k+q}\right) \ .$$

Finally, by using Cor. 2.2, it follows

$$\left|Orb_{\mathcal{H}}(X)\right| = \frac{\displaystyle\prod_{k=0}^{n-1}\left(p^n - p^k\right)}{\displaystyle\prod_{k=0}^{n-q-1}\left(p^n - p^{k+q}\right)} = \frac{\displaystyle\prod_{k=0}^{n-1}\left(p^n - p^k\right)}{\displaystyle\prod_{k=q}^{n-1}\left(p^n - p^k\right)} = \prod_{k=0}^{q-1}\left(p^n - p^k\right) \ .$$

□

The preceding corollary shows that the number of elements of an orbit given by an input text is always smaller than the number of elements in the key-space $GL_n(\mathbb{Z}_p)$. Theoretically this means that if we consider an oracle able to answer in $\mathcal{O}(1)$ whether a matrix is the key or whether a text is the corresponding plaintext of the considered ciphertext, then performing an exhaustive search on the key-space would be in $\mathcal{O}\big(\prod_{k=0}^{n-1}(p^n - p^k)\big)$ whereas performing an exhaustive search on the text-space would be in $\mathcal{O}\big(\prod_{k=0}^{q-1}(p^n - p^k)\big)$ with $q \leq n$ (q being the number of linearly independent blocks in the ciphertext).

In the last result of this paper, we provide an explicit description of the orbit of a given input text which might help to improve some attacks. To do so, we use once again the fact the Hill cipher preserves linear combinations; see Prop. 1.

Let us mention that we use Cor. 3 to prove the following theorem. Nevertheless it seems to be possible to prove this theorem without employing the preceding results and group action theory. We emphasize that we have chosen to study the Hill cipher via group action theory to obtain a convenient setting which makes clear the effects of this cipher on texts. We hope that our approach may be exploited for educational purposes.

As previously, we distinguish two cases for the sake of readability and we do not treat the case of the input text given by $0_{(\mathbb{Z}_p)^M}$ since its orbit is equal to the singleton $\{0_{(\mathbb{Z}_p)^M}\}$.

Theorem 4. *Let $X = X_1 \dots X_m \in (\mathbb{Z}_p)^M \setminus \{0_{(\mathbb{Z}_p)^M}\}$.*

1. *Suppose that there exist $i_1, \dots, i_n \in \{1, \dots, m\}$ such that $X_{i_1}, \dots, X_{i_n}$ are linearly independent; in particular, we have*

$$\forall\, i \notin \{i_1, \dots, i_n\} \quad \exists\, \lambda_1^{(i)}, \dots, \lambda_n^{(i)} \in \mathbb{Z}_p \qquad X_i = \sum_{k=1}^{n} \lambda_k^{(i)}\, X_{i_k}\ .$$

   Then $Y = Y_1 \dots Y_m \in (\mathbb{Z}_p)^M$ belongs to $Orb_{\mathcal{H}}(X)$ if and only if $Y_{i_1}, \dots, Y_{i_n}$ are linearly independent and

$$\forall\, i \notin \{i_1, \dots, i_n\} \qquad Y_i = \sum_{k=1}^{n} \lambda_k^{(i)}\, Y_{i_k}\ .$$

2. *Suppose that there exist $1 \leqslant q < n$ and $i_1, \dots, i_q \in \{1, \dots, m\}$ such that $X_{i_1}, \dots, X_{i_q}$ are linearly independent and*

$$\forall\, i \notin \{i_1, \dots, i_q\} \quad \exists\, \lambda_1^{(i)}, \dots, \lambda_q^{(i)} \in \mathbb{Z}_p \qquad X_i = \sum_{k=1}^{q} \lambda_k^{(i)}\, X_{i_k}\ .$$

   Then $Y = Y_1 \dots Y_m \in (\mathbb{Z}_p)^M$ belongs to $Orb_{\mathcal{H}}(X)$ if and only if $Y_{i_1}, \dots, Y_{i_q}$ are linearly independent and

$$\forall\, i \notin \{i_1, \dots, i_q\} \qquad Y_i = \sum_{k=1}^{q} \lambda_k^{(i)}\, Y_{i_k}\ .$$

Proof. Choose $X = X_1 \dots X_m \in (\mathbb{Z}_p)^M \setminus \left\{0_{(\mathbb{Z}_p)^M}\right\}$ and suppose that there exist $1 \leqslant q \leqslant n$ and $i_1, \dots, i_q \in \{1, \dots, m\}$ such that $X_{i_1}, \dots, X_{i_q}$ are linearly independent and

$$\forall\, i \notin \{i_1, \dots, i_q\} \quad \exists\, \lambda_1^{(i)}, \dots, \lambda_q^{(i)} \in \mathbb{Z}_p \qquad X_i = \sum_{k=1}^{q} \lambda_k^{(i)}\, X_{i_k}\ .$$

For the sake of readability, we define the set

$$E_q(X) := \left\{ Y = Y_1 \dots Y_m \in (\mathbb{Z}_p)^M \;\middle|\; \begin{cases} Y_{i_1}, \dots, Y_{i_q} \text{ are linearly independent} \\ \forall\, i \notin \{i_1, \dots, i_q\} \qquad Y_i = \displaystyle\sum_{k=1}^{q} \lambda_k^{(i)}\, Y_{i_k} \end{cases} \right\}.$$

1. This point is equivalent to $Orb_{\mathcal{H}}(X) = E_n(X)$. To show this equality, we prove an inclusion and the equality between the two cardinals.
   $\boxed{\subseteq}$ Let $Y = Y_1 \dots Y_m \in (\mathbb{Z}_p)^M$ be an element of $Orb_{\mathcal{H}}(X)$. Then, by definition, there exists $A \in \mathcal{G}_{M,n}$ such that

   $$Y = AX \qquad \Longleftrightarrow \qquad \forall\, i \in \{1, \dots, m\} \quad Y_i = KX_i\ ,$$

   where K is the key-matrix. As an immediate consequence of the linear independence of $X_{i_1}, \dots, X_{i_n}$, the vectors $Y_{i_1}, \dots, Y_{i_n}$ are linearly independent, and by Prop. 1, we have

   $$\forall\, i \notin \{i_1, \dots, i_n\} \qquad Y_i = \sum_{k=1}^{n} \lambda_k^{(i)}\, Y_{i_k}\ .$$

   This shows that $Orb_{\mathcal{H}}(X)$ is included in $E_n(X)$.
   $\boxed{=}$ We remark that the cardinal of the set $E_n(X)$ is actually equal to the number of linearly independent families of n vectors belonging to $(\mathbb{Z}_p)^n$, that is to say the number of matrices in $GL_n(\mathbb{Z}_p)$. Hence

   $$\left|E_n(X)\right| = \left|GL_n(\mathbb{Z}_p)\right| = \prod_{k=0}^{n-1} \left(p^n - p^k\right)\ .$$

   And according to Cor. 3.1, we have

   $$\left|Orb_{\mathcal{H}}(X)\right| = \prod_{k=0}^{n-1} \left(p^n - p^k\right)\ ,$$

   showing that $\left|Orb_{\mathcal{H}}(X)\right| = \left|E_n(X)\right|$ and so $Orb_{\mathcal{H}}(X) = E_n(X)$.
2. In the present case, we prove $Orb_{\mathcal{H}}(X) = E_q(X)$, with $1 \leqslant q < n$. To do so, we proceed as previously.
   $\boxed{\subseteq}$ It is sufficient to follow the same arguments as those employed in the preceding point.

$\boxed{=}$ The cardinal of the set $E_q(X)$ is given by the number of linearly independent families of q vectors belonging to $(\mathbb{Z}_p)^n$: this number is equal to

$$\prod_{k=0}^{q-1} \left(p^n - p^k\right) .$$

We employ then Cor. 3.2 to show that $Orb_{\mathcal{H}}(X)$ and $E_q(X)$ have the same cardinal, proving that $Orb_{\mathcal{H}}(X) = E_q(X)$.

□

4 Conclusion

In this paper, we exhibit the property that the Hill cipher preserves linear combinations of blocks in a text, implying a potential weakness. We employ the convenient framework of group action theory to study the consequences of this weakness, such a work being eventually exploitable for educational purposes.

Thanks to the partition of the text-space caused by the Hill cipher, we show that the set of accessible output texts (orbit) of a given input text has at worst the same size as the one of all invertible matrices. We show also that, for a given text, there exists a set of matrices that make the text unchanged (stabiliser) via the Hill cipher. Consequently, in certain cases, there are redundant computations when one performs an exhaustive search in the key-space.

To finish, let us talk briefly about the outlook. To remove the only condition that we need in our study, we would like to generalise our approach to an alphabet whose size is not necessarily a prime number, similarly to what was done for the key-space in [23]. Moreover, it could be interesting to use our knowledge of the orbits to improve the security of the Hill cipher. For instance, one may think that making permutations in the key-matrix would create a new partition of the text-space whose orbits would be bigger than the original ones. On the other hand, we hope that our results might improve some existing attacks, even lead to a ciphertext-only attack performing an elegant search of the orbit of a ciphertext. Finally a last idea would be to adapt our approach to the latest modified versions of the Hill cipher, such as the two Toorani-Falahati-Hill ciphers [8,9], to bring better understanding of these versions, even some improvements.

References

1. Hill, L.S.: Cryptography in an Algebraic Alphabet. The American Mathematical Monthly **36**(6) (1929) 306–312
2. Hill, L.S.: Concerning Certain Linear Transformation Apparatus of Cryptography. The American Mathematical Monthly **38** (1931) 135–154
3. Stinson, D.: Cryptography: Theory and Practice. Second edn. CRC/C&H (2002)
4. Ismail, I.A., Amin, M., Diab, H.: How to Repair the Hill Cipher. Journal of Zhejiang University-Science A **7**(12) (Dec. 2006) 2022–2030
5. Kiele, W.A.: A Tensor-Theoretic Enhancement to the Hill Cipher System. Cryptologia **14**(3) (1990) 225–233

6. Saeednia, S.: How to Make the Hill Cipher Secure. Cryptologia **24**(4) (2000) 353–360
7. Mahmoud, A.Y., Chefranov, A.G.: Hill Cipher Modification Based on Eigenvalues HCM-EE. In: Proc. of SIN'09. (2009) 164–167
8. Toorani, M., Falahati, A.: A Secure Variant of the Hill Cipher. In: Proc. of 14th IEEE Symposium on Computers and Communications (ISCC'09). (2009) 313–316
9. Toorani, M., Falahati, A.: A Secure Cryptosystem Based on Affine Transformation. Security and Communication Networks **4**(2) (2011) 207–215
10. Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Information Security and Cryptography. Springer (2002)
11. Sastry, V., Shankar, N.R.: Modified Hill Cipher with Interlacing and Iteration (2007)
12. Chen, L., Guo, G., Peng, Z.: A Hill Cipher-Based Remote Data Possession Checking in Cloud Storage. Security and Communication Networks **7**(3) (2014) 511–518
13. Karthikeyan, B., Chakravarthy, J., Vaithiyanathan, V.: An Enhanced Hill Cipher Approach for Image Encryption in Steganography. International Journal of Electronic Security and Digital Forensics **5**(3/4) (2013) 178–187
14. Acharya, B., Sharma, M.D., Tiwari, S., Minz, V.K.: Privacy Protection of Biometric Traits Using Modified Hill Cipher with Involutory Key and Robust Cryptosystem. In: Proc. of BIOTEC'10. (2010) 242–247
15. Huang, N.: An Enhanced Hill Cipher and Its Application in Software Copy Protection. JNW **9**(10) (2014) 2582–2590
16. Keliher, L., Thibodeau, S.: Slide Attacks Against Iterated Hill Ciphers. In Thampi, Sabu M. and Atrey, Pradeep K. and Fan, Chun-I and Perez, Gregorio Martinez, ed.: Proc. of SSCC'13, Springer (2013) 179–190
17. Keliher, L., Delaney, A.Z.: Cryptanalysis of the Toorani-Falahati Hill Ciphers. In: Proc. of ISCC'13. (2013) 436–440
18. Parmar, N.B., Bhatt, K.: Hill Cipher Modifications: A Detailed Review. International Journal of Innovative Research in Computer and Communication Engineering **3**(3) (2015) 1467–1474
19. Bauer, C.P., Millward, K.: Cracking Matrix Encryption Row by Row. Cryptologia **31**(1) (2007) 76–83
20. Yum, D.H., Lee, P.J.: Cracking Hill Ciphers with Goodness-of-Fit Statistics. Cryptologia **33**(4) (2009) 335–342
21. Leap, T., McDevitt, T., Novak, K., Siermine, N.: Further Improvements to the Bauer-Millward Attack On the Hill Cipher. Cryptologia **40**(5) (2016) 452–468
22. Khazaei, S., Ahmadi, S.: Ciphertext-only Attack on d × d Hill in $\mathcal{O}(d \times 13^d)$. Inf. Process. Lett. **118** (2017) 25–29
23. Overbey, J., Traves, W., Wojdylo, J.: On the Keyspace of the Hill Cipher. Cryptologia **29**(1) (2005) 59–72
24. Strassen, V.: Gaussian Elimination is Not Optimal. Numer. Math. **13**(4) (Aug. 1969) 354–356
25. Delfs, H., Knebl, H.: Introduction to Cryptography - Principles and Applications, Third Edition. Information Security and Cryptography. Springer (2015)
26. Smith, J.D.: Introduction to Abstract Algebra. Textbooks in Mathematics. Chapman and Hall/CRC (2008)
27. Artin, M.: Algebra. Advanced Mathematics Series edn. Volume 2. Pearson Prentice Hall (2011)