Palestine Journal of Mathematics

Vol. 9(2)(2020) , 639–657

AN APPLICATION OF YOUNG TABLEAUX TO CRYPTOGRAPHY

Kolo F. SORO, Eric D. AKEKE and Konan M. KOUAKOU

Communicated by Ayman Badawi

MSC 2010 Classifications: Primary 05A17; Secondary 94A60.

Keywords and phrases: Partitions, Young tableaux, Schensted algorithm, RSA Cryptosystem, Python programming.

Abstract: Modern cryptography is developing methods naturally for giving data confidently, and also for preserving integrity, authenticity, security with non-repudiation and signature. In this paper, we will show how Young tableaux can be used as a modern cryptosystem by its principles of row-insertion (Schensted algorithm) and the inverse of that operation.

To decrypt a given cipher text following a key K, many semi-standard Young tableaux are used, and for that, we found a remarkable upper bound on number of semi-standard Young tableaux one must not go over.

1 Introduction

Alfred Young introduced the Young tableau in 1900, thing whereby he became well-known. F. G. Frobenius used Young tableaux for the first time in representations of the symmetric group in 1903 and H. Weil also used them in his book *"Theory of groups and quantum mechanics"*.

In this paper, we explore a connection between Young tableaux and cryptography.

After the first section and the second which are dedicated to introduction and presentation of Young diagrams and Young tableaux, we tackle in the third section the main problem of this paper. We define the word (column word) associated to a given semi-standard Young tableau (SSYT) and present the insertion and expelling operations on semi-standard Young tableaux.

In the fourth section, we recall the basic property in cryptography and describe RSA cryptosystem principle.

Finally, in the fifth section, we introduce the use of semi-standard Young tableaux as cryptosystem. We show how any word from an alphabet $S = \{s_1, s_2, \ldots, s_n\}$ containing n letters, can be written in one and only one sequence of semi-standard Young tableaux $T_1, T_2, \ldots, T_k$ by constructing a bijective application between that alphabet and the sub-set $\{1, 2, \ldots, n\}$ of integers. Indeed, for a given clear text $\mathcal{M}$ of p letters, we used its associated sequence of semi-standard Young tableaux $T_1, T_2, \ldots, T_k$ and do the product $T = T_1.T_2 \ldots T_k$, using Schensted algorithm in [6]. Therefore, the cipher text is given by $\mathcal{C} = w(T)$ where T has shape λ, a partition of p and $w(T)$ is the word of T (cf. Definition 3.1). The decryption key is generated by the ciphering and that decryption uses expelling routes (the opposite of bumping routes) to obtain $\mathcal{M}$, the clear text. The key obtained during ciphering is tranferred by using RSA cryptosystem. But, for encryption, there is one and only one bumping route for a given non-zero positive integer x in a $SSYT$. For decryption, there can be many expelling routes for that inserted x. So, many $SSYT$ would be used for decryption, but how many?

Nearly, we found a bound N_λ for the number of $SSYT$ used to decrypt $\mathcal{C} = w(T)$ and gave an algorithm computing this N_λ.

For our future works, we expect to get a better bound or even the accurate number and also we will try to measure the security of that cryptosystem.

2 Young diagrams and Young tableaux

2.1 Partition of an integer

Definition 2.1. Let n be a non-zero positive integer. A partition of n is a sequence $\lambda = (\lambda_1, \lambda_2, ..., \lambda_s)$ of integers such that

$$\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_s > 0 \text{ and } \lambda_1 + \lambda_2 + ... + \lambda_s = n.$$

For a partition $\lambda = (\lambda_1, \lambda_2, ..., \lambda_s)$, we defined its length by : $l(\lambda) = card\{\lambda_i : i \in \overline{1, s}\}$.
The λ_i's are the parts of the partition λ.

Notation 2.2. If λ is a partition of n, it's denoted by $\lambda \vdash n$. The multiplicity of the i^{th} part of λ is $m_i = card\{j : \lambda_j = i\}$. λ is often denoted as: $\lambda = (\lambda_1^{m_1}, \lambda_2^{m_2}, \lambda_3^{m_3}, ...)$.

Let P_n be the number of partitions of the integer n, with convention $P_0 = 1$ and $P_k = 0$ for all $k < 0$. By the Hardy-Ramanujan asymptotic partition formula, the value of P_n is given asymptotically by

$$P_n \sim \frac{1}{4n\sqrt{3}} exp\{\pi\sqrt{(\frac{2n}{3})}\}.$$

Theorem 2.3. ([3], *page* 15)
The P_n's satisfy the following recurrence formula:

$$\forall\, n \geq 1,\ P_n = \sum_{k>0} (-1)^{k-1} (P_{n - \frac{k(3k-1)}{2}} + P_{n - \frac{k(3k+1)}{2}}).$$

Example 2.4. The first twenty non-zero P_n's are :

n	0	1	2	3	4	5	6	7	8	9	10	11
P_n	1	1	2	3	5	7	11	15	22	30	42	56

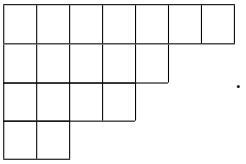
n	12	13	14	15	16	17	18	19
P_n	77	101	135	176	231	297	385	490

2.2 Young diagrams

Definition 2.5. A Young diagram Y is a collection of boxes, or cells, arranged in left-justified rows, with weakly decreasing number of boxes from top to bottom. The number of cells in Y denoted $|Y|$, is the weight of Y.

Remark 2.6. Every partition of n corresponds to one and only one Young diagram which weight is n.

Example 2.7. The partition $\lambda = (7, 5, 4, 2)$ of 18 corresponds to the following Young diagram

$Y(\lambda) =$  .

Definition 2.8. Let $Y(\lambda)$ be a Young diagram. An outside corner is a box in $Y(\lambda)$ such that neither box below or to the right is in $Y(\lambda)$.

2.3 Young tableaux

Definition 2.9. A **Young tableau** (or simply tableau) is a Young diagram filled with non-zero positives integers.

A **semi-standard Young tableau** (SSYT) is a tableau in which the numbers used are weakly increasing in rows from left to right, and strictly increasing in columns from top to bottom.

Example 2.10. Let $\lambda \vdash 18$, with $\lambda = (7, 5, 4, 2)$.

11	5	37	25	4	17	5
2	1	15	5	7		
14	6	19	1			
5	8					

Young tableau

1	2	3	3	4	5	5
2	3	5	5	7		
4	6	9	9			
5	8					

Semi-standard Young tableau

3 Some operations on tableaux

3.1 Word of a tableau

Definition 3.1. Let T be a SSYT with k columns $c_1, c_2, ..., c_k$ such that, on each column c_j, we have the numbers $a_{1,j}, a_{2,j}, ..., a_{n_j,j}$ from top to bottom, where n_j is the number of boxes in the column c_j, for all $j = 1, \ldots, k$. The word (column word) of T denoted $w(T)$ is given by

$$w(T) = a_{1,k}a_{2,k}...a_{n_k,k}a_{1,k-1}...a_{n_{k-1},k-1}...a_{1,1}a_{2,1}...a_{n_1,1}.$$

Example 3.2. For $T =$ $\begin{array}{|c|c|c|c|}\hline 1 & 1 & 2 & 3 \\ \hline 2 & 3 & 3 \\ \cline{1-3} 4 \\ \cline{1-1}\end{array}$ we have $w(T) = 32313124$.

Remark 3.3. It is possible to find T when we have $w(T)$ by subdividing the word into blocks as follows:

$a)$ From left to right, when an entry is greater than the next, then we have the end of a block (a column);

$b)$ With the next entry (the least one) we continue the process and so on.

3.2 Row-insertion principle

Let T be a SSYT. To insert a non-zero positive integer x in T, we construct a new SSYT, denoted $T \leftarrow x$, using the following principle:

$i)$ Starting to the first row of T, if x is at least as large as all the entries, add x in a new box to the end of the row;

$ii)$ If there exists an entry on the first row that is strictly larger than x, then put x in the box of the smaller entry that is strictly larger than x and continue the process as previously with this entry removed (bumped), starting to the second row;

$iii)$ Continue the process with the bumped entries and so on;

$iv)$ Keep going until the bumped entry can be put at the end of the row below, it is bumped into, or until it is bumped out at the bottom. In the last case it forms a new row with one entry.

The bumping route of x is the set of boxes used to insert x in T. Its cardinal is denoted by $l(T \leftarrow x)$.

Example 3.4. Consider $\lambda = (5, 4, 3, 2)$ and let insert 2 in $T(\lambda) =$ $\begin{array}{|c|c|c|c|c|}\hline 1 & 2 & 2 & 3 & 4 \\ \hline 2 & 3 & 4 & 4 \\ \cline{1-4} 4 & 5 & 7 \\ \cline{1-3} 5 & 6 \\ \cline{1-2}\end{array}$.

We have

$\begin{array}{|c|c|c|c|c|}\hline 1 & 2 & 2 & 3 & 4 \\ \hline 2 & 3 & 4 & 4 \\ \cline{1-4} 4 & 5 & 7 \\ \cline{1-3} 5 & 6 \\ \cline{1-2}\end{array}$ $\leftarrow 2$ $\begin{array}{|c|c|c|c|c|}\hline 1 & 2 & 2 & 2 & 4 \\ \hline 2 & 3 & 4 & 4 \\ \cline{1-4} 4 & 5 & 7 \\ \cline{1-3} 5 & 6 \\ \cline{1-2}\end{array}$ $\leftarrow 3$ $\begin{array}{|c|c|c|c|c|}\hline 1 & 2 & 2 & 2 & 4 \\ \hline 2 & 3 & 3 & 4 \\ \cline{1-4} 4 & 5 & 7 \\ \cline{1-3} 5 & 6 \\ \cline{1-2}\end{array}$ $\leftarrow 4$

1	2	2	2	4
2	3	3	4	
4	4	7		
5	6			

$\leftarrow 5$

1	2	2	2	4
2	3	3	4	
4	4	7		
5	5			
6				

$\leftarrow 6.$

The bumping route of 2 is a set of five boxes as shown in the following tableau.

1	2	2	2	4
2	3	3	4	
4	4	7		
5	6			
6				

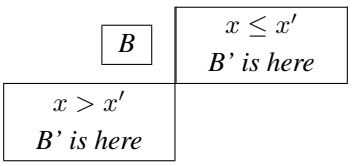
$l(T \leftarrow 2) = 5.$

Remark 3.5. Given $T \leftarrow x$, it's easy to obtain T knowing x and its bumping route.
For row-insertion of an integer x in T there exists one and only one bumping route.

Theorem 3.6. ([6], *Row Bumping Lemma*)
Let T be a SSYT, x and x' two integers. Consider R the bumping route of x in T and R' that of x' in $T \leftarrow x$. For this two successive row- insertions, we obtain two new cells B and B' respectively for x and x'.

(i) If $x \leq x'$, then R is strictly left of $R'$and B is strictly left of and weakly below B'.

(ii) If $x > x'$, then R' is weakly left of R and B' is weakly left of and strictly below B.



Corollary 3.7. *Let T be a SSYT, x and x' two integers. Then we have:*

i) if $x \leq x'$, then $l(T \leftarrow x) \geq l(T \leftarrow x')$,

ii) if $x > x'$, then $l(T \leftarrow x) < l(T \leftarrow x')$.

Remark 3.8. Let T be a $SSYT$ of shape $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_m)$ and x be a non-zero positive integer.

a) For row-insertion of x in T, we have: $1 \leq l(T \leftarrow x) \leq m + 1$.

b) Suppose $l(T \leftarrow x) = n$. The semi-standard Young tableau $T \leftarrow x$ have the shape μ such that:

(1) if $n < m$, then $\mu = (\lambda_1, \lambda_2, \ldots, \lambda_{n-1}, \lambda_n + 1, \lambda_{n+1}, \ldots, \lambda_m)$,
(2) if $n = m$, then $\mu = (\lambda_1, \lambda_2, \ldots, \lambda_{m-1}, \lambda_m + 1)$,
(3) if $n = m + 1$, then $\mu = (\lambda_1, \lambda_2, \ldots, \lambda_m, 1)$.

3.3 An algorithm using in python

- An algorithm to insert a positive integer in a SSYT

```
m = int(input("The number of rows is : "))
N = [ ]
for i in range (0, m) :
    n = int(input("The number of cells in the next row is : "))
    N.append (n)
print("The corresponded partition is : ", N)
Tablo = [ ]
```

```
print("Enter the tableau")
for i in range (0, m) :
    lists = [ ]
    for j in range (0, N[i]) :
        Num = int(input("Enter the next integer in the row : "))
        lists.append (Num)
    print (lists)
    Tablo.append(lists)
print ("The tableau is : ")
for i in range (0, m):
    print (Tablo[i])
Tab = int(input("The integer to be inserted : "))
if Tablo[0][N[0] − 1] <= Tab :
    Tablo[0] = Tablo[0] + [Tab]
    c = N[0] + 1
elif Tab < Tablo [0][0] :
    for i in range (0, m) :
        Tab, Tablo[i][0] = Tablo[i][0], Tab
    Tablo = Tablo + [[Tab]]
    c = 1
else :
    k = 1
    b = 0
    j = 1
    while k < N[0] and Tablo[0][k] <= Tab :
        k = k + 1
    Tablo[0][k], Tab = Tab, Tablo[0][k]
    c = k + 1
    for j in range (1, m):
      while b == 0 :
          if Tablo[j][N[j] − 1] <= Tab :
              Tablo[j] = Tablo[j] + [Tab]
              b = 1
          elif Tab < Tablo[j][0] :
                Tab, Tablo[j][0] = Tablo[j][0], Tab
                if j! = m − 1:
                    b = 0
                    j = j + 1
                else :
                    Tablo = Tablo + [[Tab]]
                    b = 1
           else :
                p = 1
                while p < N[j] and Tablo[j][p] <= Tab :
                    p = p + 1
                Tablo[j][p], Tab = Tab, Tablo[j][p]
                if j! = m − 1 :
                    b = 0
                    j = j + 1
                else :
                    Tablo = Tablo + [[Tab]]
                    b = 1
print("The obtain tableau is : ")
for i in range (0, len(Tablo)) :
    print(Tablo[i])
print("The component of the key is : ", c)
```

3.4 Product of semi-standard Young tableaux

Definition 3.9. Let T and U be two SSYT. The product of T by U, denoted $T.U$, is defined by row inserting the elements (entries) of U in T starting from bottom to top and left to right.

Example 3.10. Consider $T =$ $\begin{array}{|c|c|c|c|c|c|}\hline 1&1&2&2&2&3\\\hline 2&2&3&4&4\\\cline{1-5} 4&4&5\\\cline{1-3} 6&7\\\cline{1-2}\end{array}$ and $U =$ $\begin{array}{|c|c|c|}\hline 1&2&2\\\hline 2&3\\\cline{1-2}\end{array}$. We obtain:

$$T.U = ((((T \leftarrow 2) \leftarrow 3) \leftarrow 1) \leftarrow 2) \leftarrow 2 = \begin{array}{|c|c|c|c|c|c|c|c|}\hline 1&1&1&2&2&2&2&2\\\hline 2&2&2&3&3\\\cline{1-5} 3&4&4&4\\\cline{1-4} 4&7\\\cline{1-2} 5\\\cline{1-1} 6\\\cline{1-1}\end{array}.$$

It follows from [6] Claim 1, page 12, that for all semi-standard Young tableaux T, U and V, we have $(T.U).V = T.(U.V)$.

4 Basic principle in cryptography

Modern cryptography is based on public key algorithms, used either directly for encryption or to encrypt the key in a conventional system. The security of such systems is based on computational problems.

Let $\mathcal{M}$ be the clear text, $\mathcal{C}$ the cipher text and $\mathcal{K}$ the keys' space (for encryption and decryption). Let denote $E_{\mathcal{K}}$ the encryption function and $D_{\mathcal{K}}$ the decryption function. Thus, the basic property in cryptography is

$$\mathcal{M} = D_{\mathcal{K}}(\mathcal{C}) \Leftrightarrow \mathcal{C} = E_{\mathcal{K}}(\mathcal{M}).$$

RSA cryptosystem (Rivest – Shamir – Adleman)
Principle

- Choose p and q two big prime numbers and compute $n = pq$;
- Choose an integer "e", coprime with $\varphi(n) = (p-1)(q-1)$. The public key is given by $(e; n)$;
- Compute "d" the inverse of "e" modulo $\varphi(n)$, that is

$$d.e \equiv 1 \mod \varphi(n).$$

The secret key is given by $(d; n)$.

The encryption is given by: $\mathcal{C} \equiv \mathcal{M}^e \mod n$
and the decryption by: $\mathcal{M} \equiv \mathcal{C}^d \mod n$.

However, $\mathcal{M}$ must be divided by blocs sometimes (when $\mathcal{M} \geq n$) and each bloc is encrypted (also for the decryption of $\mathcal{C}$) with the same process explained above.

5 Young tableaux in cryptography

5.1 Writing a text in SSYT

We consider a finite alphabet S of n elements: $S = \{s_1, s_2, \ldots, s_n\}$.
A word of S is a finite sequence of elements of S.

Let consider the following bijective correspondence θ:

x	s_1	s_2	...	s_{n-1}	s_n
$\theta(x)$	1	2	...	$n-1$	n

.

For a given clear text $\mathcal{M}$ in S containing p letters $(p \geq 2)$ and for each letter x of $\mathcal{M}$, we use $\theta(x)$.

Let $r_i = \theta(x_i)$ where x_i is the i^{th} letter of $\mathcal{M}$. We construct semi- standard Young Tableaux as follows:

i) There exists an integer k_1 such that $r_1 \leq r_2 \leq ... \leq r_{k_1}$ and $r_{k_1} > r_{k_1+1}$. Then we put

$$T_1 = \begin{array}{|c|c|c|c|} \hline r_1 & r_2 & ... & r_{k_1} \\ \hline \end{array};$$

ii) If $k_1 = p$, then stop the process;

iii) If $k_1 \neq p$, then there exist an integer k_2 such that $r_{k_1+1} \leq r_{k_1+2} \leq ... \leq r_{k_2}$ and $r_{k_2} > r_{k_2+1}$. We put

$$T_2 = \begin{array}{|c|c|c|c|} \hline r_{k_1+1} & r_{k_1+2} & ... & r_{k_2} \\ \hline \end{array};$$

- if $k_2 = p$, then stop the process;
- if $k_2 \neq p$, continue the process.

So, we obtain a sequence $T_1, T_2, \ldots, T_k$ of $SSYT$ such that, for all i from 1 to k, T_i has one row. The sequence $T_1, T_2, \ldots, T_k$ of $SSYT$ obtained is called the sequence of tableaux associated with $\mathcal{M}$.

NB : *For all the examples in this paper, we will use the following alphabet*

$$S = \{A, B, \ldots, Z, 0, 1, \ldots, 9\}$$

and the bijective function f from S to $\{1, 2, \ldots, 36\}$ respecting this table below:

x	A	B	...	Y	Z	0	1	...	8	9
$f(x)$	01	02	...	25	26	27	28	...	35	36

.

By abuse, we will sometimes write

x	A	B	...	I	J	...	Z	...	8	9
$f(x)$	1	2	...	9	10	...	26	...	35	36

.

Example 5.1. Consider the following clear text: $\mathcal{M}$ =**YOUNG TABLEAUX.**

Its associated sequence of tableaux is:

25		15	21		14		7	20		1	2	12		5		1	21	24

.

Remark 5.2. Each clear text corresponds to one and only one finite sequence of semi-standard Young tableaux (all with one row).

5.2 Encryption principle

Let $T_1, T_2, \ldots, T_k$ be the sequence of tableaux associated with a clear text $\mathcal{M}$. To encrypt $\mathcal{M}$, we proceed like this:

- find the product: $T = T_1.T_2 \ldots T_k$;
- write $w(T)$ the word of T (cf. Definition 3.1).

The cipher text is $\mathcal{C} = w(T)$.

5.3 Decryption key

Let p be the number of cells in $T = T_1.T_2 \dots T_k$ and q be that of cells in T_1. Let put $r = p-q$, then r is the number of integers which have been inserted to obtain T. Let us call them $x_1, x_2, \dots, x_r$ and suppose that they are inserted in this order.

(a) If $T = T_1$, then $r = 0$ and no ciphering has been done.

(b) If $T \neq T_1$, for i from 1 to r, let denote k_i the position of the cell that contain x_i on the first row, from left to right, in the semi-standard Young tableau $(\dots(T_1 \leftarrow x_1) \leftarrow \cdots) \leftarrow x_i$.

By definition, the $r - tuple\ K = (k_r, k_{r-1}, \dots, k_1)$ is the key for decryption and r its length.

Example 5.3. Let's concider the following message: **STREET 12 DOOR 8.**
Its associated sequence of tableaux is:

19	20		18		5	5	20	28	29		4	15	15	18	35	.			

The encryption gives $T =$

4	5	15	15	18	35
5	20	20	28	29	
18					
19					

and the key is $K = (6, 5, 4, 3, 1, 5, 4, 3, 2, 1, 1)$.

The encrypted text is therefore

$$\mathcal{C} = 35182915281520052004051819 \text{ or } \mathcal{C} = \text{8R2O1OTETDERS},$$

using the correspondence table (cf. Subsection 5.1).

Remark 5.4. If the shape of the semi-standard Young tableau T is $\lambda = (\lambda_1, \lambda_2, ..., \lambda_m)$, then

$$\sum_{i=2}^{m} \lambda_i \leq r < \sum_{i=1}^{m} \lambda_i.$$

5.4 Decryption algorithm

In this section, we give an algorithm for decryption of a message knowing the key K.

Let $K = (k_r, k_{r-1}, \dots, k_1)$ be the key to decrypt the cipher text $\mathcal{C} = w(T)$. Then the procedure is as follows:

- Construct T ;
- Remove in T the k_r^{th} entry n_1 on the first row, always from left to right. We obtain $SSYT$ of type $U_1 = T \rightarrow n_1$. Note that, this kind of tableau is not unique in general. We easily check that $n_1 = x_r$, that is the last integer inserted during ciphering process;
- Remove in all tableaux of type U_1 the k_{r-1} entries on the first rows. We obtain tableaux of type $U_2 = U_1 \rightarrow n_2$. But n_2 is not necessarily the same integer for all tableaux of type U_1 obtain;
- Keep going until the last component k_1 of K.

So the clear text is obtained by its associated sequence of $SSYT$.

Remark 5.5. Some tableaux will not be used in the decryption process. Indeed, for the i^{th} component k_{r-i+1} of the key K, let $a_{i,1}$ be the entry to be expelled and l_k $(k = 1, \dots, m)$ be the row containning the outside corner eliminated. Removing operation (expulsion) is possible if and only if the $SSYT$ of type U_{i-1} (with $U_0 = T$) used satisfy one of the following conditions:

(i) $a_{i,1}$ is in the last cell of the first row and no cell below. That is equivalente to $k = 1$.

(ii) if $k \neq 1$, for j from 2 to k, there exist $a_{i,j}$ on the j^{th} row of U_{i-1} such that

$$a_{i,j-1} < a_{i,j} \leq \beta_{i,j-1},$$

where $\beta_{i,j-1}$ is the entry rigth of $a_{i,j-1}$ or ∞ if there is no cell rigth of $a_{i,j-1}$.

Proposition 5.6. *The previous decryption principle allows to get the clear text in one and only one sequence of $SSYT$, each tableau having one row.*

Proof. Let T be a $SSYT$ of a word to be decrypt and $K = (k_r, k_{r-1}, \ldots, k_1)$ the decryption key. For each component of K, there exists at least one tableau for continuing the expulsion process. Indeed:

- For the first component k_r of K, we expel x_r the last integer inserted during the encryption. The set of the different $SSYT$ obtained necessarily contains the tableau

$$T^{(1)} = (\ldots(T_1 \leftarrow x_1) \leftarrow \cdots) \leftarrow x_{r-1}$$

relatively to the bumping route of x_r.

- For the second component k_{r-1} of K, the integer x_{r-1} is expelled from $T^{(1)}$. Of course there are possibly other $SSYT$ and other integers to be expelled. The set of the different $SSYT$ obtained contains the tableau

$$T^{(2)} = (\ldots(T_1 \leftarrow x_1) \leftarrow \cdots) \leftarrow x_{r-2.}$$

- Thus, for the i^{th} component k_{r-i+1} of K, $i \in \{1, \ldots, r-1\}$, we expel x_{r-i+1} from $T^{(i-1)}$, with $T^{(0)} = T$. The set of the different $SSYT$ obtained contains the tableau

$$T^{(i)} = (\ldots(T_1 \leftarrow x_1) \leftarrow \cdots) \leftarrow x_{r-i}$$

for which it is sure to be able to continue the process relatively to the bumping route of x_{r-i+1} in $T^{(i)}$.

- For the last component k_1 of K, the integer x_1 is expelled from $T^{(r-1)}$. The set of $SSYT$ obtained necessarily contains the tableau

$$T^{(r)} = T_1$$

which is indeed a $SSYT$ with one row.

We obtain the clear text by arrangement of all the expelled integers, ordered from right to left as follows:

T_1	x_1	x_2	...	x_r

We note that we obtain the sequence $(T_i)_{i \in \overline{1,k}}$ of $SSYT$ used for encryption (cf. Subsection 5.2).

Unicity: The uniqueness of the bumping route (Remark 3.5) ensures the uniqueness of the sequence of row $SSYT$ resulting in the clear text. Indeed, let V and U be two $SSYT$ such that $U = V \leftarrow x$. For the expulsion of x in U, there may be several routes in which the bumping route of x in V (which is unique) makes it possible to find V. Necessarily any other route leads to another $SSYT$ different from V. □

Example 5.7. Let's encrypt the message: $\mathcal{M} =$ **AN EXAMPLE**.

The writing in row $SSYT$ is given by:

01	14		05	24		01	13	16		12		05

The ciphering gives: $T =$

1	1	5	16
5	12		
13	24		
14			

The cipher text is thus: $\mathcal{C} = 160501122401051314 =$ PEALXAEMN (Remember that if a cell contains a digit, it is preceded by a zero) and the key is: $K = (3, 3, 4, 3, 2, 3, 2)$.

For the decryption following the key, we construct the semi-standard Young tableau T starting from the cipher text $\mathcal{C}$.

- For $k_7 = 3$, the integer to be expelled from T is 5. We obtain two $SSYT$:

$$V_{1,1} = \begin{array}{|c|c|c|c|}\hline 1 & 1 & 5 & 16 \\ \hline 5 & 13 \\ \cline{1-2} 14 & 24 \\ \cline{1-2}\end{array}, V_{1,2} = \begin{array}{|c|c|c|c|}\hline 1 & 1 & 12 & 16 \\ \hline 5 & 24 \\ \cline{1-2} 13 \\ \cline{1-1} 14 \\ \cline{1-1}\end{array} \quad \text{and } x_7 = 5.$$

- For $k_6 = 3$ the integer to be expelled from $V_{1,1}$ and $V_{1,2}$ is 12.

  - For $V_{1,1}$ there is only one $SSYT$:

$$V_{2,1} = \begin{array}{|c|c|c|c|}\hline 1 & 1 & 13 & 16 \\ \hline 5 & 24 \\ \cline{1-2} 14 \\ \cline{1-1}\end{array} \quad \text{and } x_6 = 12.$$

  - For $V_{1,2}$ the operation is impossible.

- For $k_5 = 4$, the integer to be expelled from $V_{2,1}$ is 16. We obtain two $SSYT$:

$$V_{3,1} = \begin{array}{|c|c|c|}\hline 1 & 1 & 13 \\ \hline 5 & 24 \\ \cline{1-2} 14 \\ \cline{1-1}\end{array}, V_{3,2} = \begin{array}{|c|c|c|c|}\hline 1 & 1 & 13 & 24 \\ \hline 5 \\ \cline{1-1} 14 \\ \cline{1-1}\end{array} \quad \text{and } x_5 = 16.$$

- For $k_4 = 3$, the integer to be expelled from $V_{3,1}$ and $V_{3,2}$ is 13.

  - For $V_{3,1}$ there are two $SSYT$:

$$V_{4,1} = \begin{array}{|c|c|}\hline 1 & 1 \\ \hline 5 & 24 \\ \cline{1-2} 14 \\ \cline{1-1}\end{array}, \quad V_{4,2} = \begin{array}{|c|c|c|}\hline 1 & 1 & 24 \\ \hline 5 \\ \cline{1-1} 14 \\ \cline{1-1}\end{array} \quad \text{and } x_4 = 13.$$

  - For $V_{3,2}$ the operation is impossible.

- For $k_3 = 2$, the integer to be expelled from $V_{4,1}$ and $V_{4,2}$ is 1. We obtain three $SSYT$:

  - For $V_{4,1}$ there are two $SSYT$:

$$V_{5,1} = \begin{array}{|c|c|}\hline 1 & 5 \\ \hline 14 & 24 \\ \cline{1-2}\end{array}, \quad V_{5,2} = \begin{array}{|c|c|}\hline 1 & 24 \\ \hline 5 \\ \cline{1-1} 14 \\ \cline{1-1}\end{array} \quad \text{and } \ x_3 = 1.$$

  - For $V_{4,2}$ there is only one $SSYT$:

$$V_{5,3} = \begin{array}{|c|c|c|}\hline 1 & 5 & 24 \\ \hline 14 \\ \cline{1-1}\end{array} \quad \text{and } x_3 = 1.$$

- For $k_2 = 3$, the integer to be expelled from $V_{5,3}$ is 24 and the operation is impossible for the others. There is only one $SSYT$:

$$V_{6,1} = \begin{array}{|c|c|}\hline 1 & 5 \\ \hline 14 \\ \cline{1-1}\end{array} \quad \text{and } x_2 = 24.$$

- For $k_1 = 2$, the integer to be expelled from $V_{6,1}$ is 5. We obtain two $SSYT$:

$$V_{7,1} = \begin{array}{|c|}\hline 1 \\ \hline 14 \\ \hline \end{array}, \quad V_{7,2} = \begin{array}{|c|c|}\hline 1 & 14 \\ \hline \end{array} \quad \text{and } x_1 = 5.$$

After using the last component of the key, we obtain an unique row $SSYT$. The clear text is read as follows:

$$\begin{array}{|c|c|}\hline 1 & 14 \\ \hline \end{array}\ x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_7.$$

01	14	05	24	01	13	16	12	05
A	N	E	X	A	M	P	L	E

Definition 5.8. The size of a non-zero positive integer is the number of digits that compose it taking into account their multiplicities.

For example, 245002 is an integer of size 6.

5.5 Transferring the key

To transfer the key, the **RSA** system can be used.

Principle
Let $K = (k_r, k_{r-1}, \ldots, k_1)$ be the key to be transferred. The transfer takes place in two steps:
Step 1 :

- If $k_i \in \{1, \ldots, 9\}$ for all $i = 1, \ldots, r$, then the key is arranged as follows $k_r k_{r-1} \ldots k_1$;
- If there exists $k_i > 9$, then we consider $k_\alpha = \sup\limits_{1 \le i \le r} k_i$ and m its size. Now we express all the other components of K with m digits (taking into account their multiplicities) by preceding the number of one or more zero if its size is less than m. Consequently, the components obtained are arranged as above.

Step 2 :

RSA cryptosystem is used to encrypt the obtained text.

Example 5.9. Let us transfer the key $K = (3, 3, 4, 3, 2, 3, 2)$ from **Example** 5.7. Then the clear text is $\mathcal{M}_\mathcal{K} = 3343232$. Let $p = 41$ and $q = 71$. Then $n = pq = 2911$ and $\varphi(n) = 2800$.

Let $e = 13$. We have $gcd(e, \varphi(n)) = 1$ and the public key is $(13; 2911)$. Let us determine "d" the inverse of "e" modulo $\varphi(n)$.

$$d \equiv e^{\varphi(\varphi(n))-1} \mod \varphi(n) \equiv 13^{960} \mod 2800 \equiv 1077.$$

Then $(1077; 2911)$ is the secret key.

For encryption, the clear text is subdivided into blocks of size smaller than n. We have $\mathcal{M}_\mathcal{K} = 3343232 = 003\ \ 343\ \ 232$ and

$$\begin{aligned} 003^{13} &\mod 2911 \equiv 2006, \\ 343^{13} &\mod 2911 \equiv 1646, \\ 232^{13} &\mod 2911 \equiv 1449. \end{aligned}$$

The cipher text is: $\mathcal{C} = 2006\ \ 1646\ \ 1449$.

For decryption, the receiver computes

$$\begin{aligned} 2006^{1077} &\mod 2911 \equiv 003, \\ 1646^{1077} &\mod 2911 \equiv 343, \\ 1449^{1077} &\mod 2911 \equiv 232. \end{aligned}$$

The clear text is therefore $\mathcal{M}_\mathcal{K} = 003343232$ and we have the key $K = (3, 3, 4, 3, 2, 3, 2)$.

Remark 5.10. Let T be a $SSYT$ of shape $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_m)$ and $K = (k_r, k_{r-1}, \ldots, k_1)$ the decryption key. Then there exists $i \in \{1, \ldots, r\}$ such that $k_i \ge \lambda_2$. Indeed, all cells from l_2 to l_m must be deleted and in particular the last cell on l_2.

5.6 An upper bound for decryption

Proposition 5.11. *Let T be a $SSYT$ of shape $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_m)$, $m \geq 1$ and x be a non-zero positive integer to be expelled from T. We suppose that x is in the first row and the j^{th} column of T. Then the number of possible expelling routes (that is of $SSYT$) is less than the following integer M:*

i) *if $m = 1$, then $M = 1$,*

ii) *if $m = 2$, then $M = 2$,*

iii) *if $m \geq 3$, then $M = P_{(\mu;1;m)} - \sum_{k=3}^{m} P_{(\mu;k;m)}(n(\mu_k)+1)(\mu_k - \mu_m - \frac{n(\mu_k)}{2})$, with*

$$\mu_i = min\ (\lambda_i, j), \forall\ i \in \{2; \ldots; m\},$$

$$P_{(\mu;k;m)} = \begin{cases} \prod_{i=k+1}^{m-1} (\mu_i - \mu_m + 1), & \text{if } k \leq m-2, \\ 1 & \text{otherwise} \end{cases}, \text{and}$$

$$n(\mu_k) = \begin{cases} \mu_k - \mu_m - 1, & \text{if } \mu_k \neq \mu_m \\ 0 & \text{otherwise} \end{cases}.$$

Proof.

i) $m = 1$.

- If $j = \lambda_1$, only one outside corner is eliminated, that means there is at most one possible expelling route;
- If $j \neq \lambda_1$, no outside corner can be eliminated (the expulsion of x is impossible): no possible expelling route.

Therefore, $M = 1$.

ii) $m = 2$.

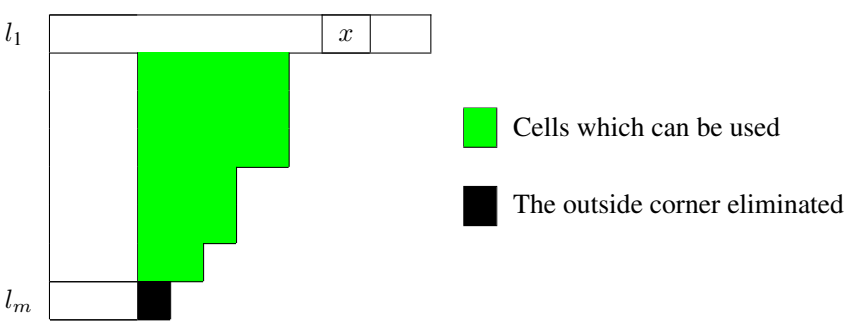
- If $j = \lambda_1$, then two outside corners can be eliminated: the one on the first row l_1 and the one on the second row l_2.
- If $\lambda_2 \leq j < \lambda_1$, only the outside corner on l_2 can be eliminated.
- If $j < \lambda_2$, no outside corner can be eliminated (the expulsion of x is impossible).

Therefore, $M = 2$.

iii) $m \geq 3$. It should be noted that the number of possible expelling routes for expulsion is maximal if the outside corner considered (and therefore eliminated) is on the last row of T.

There are two cases: $\lambda_2 \leq j$ or $\lambda_2 > j$.

- Suppose that $\lambda_2 \leq j$. Then $\mu_i = \lambda_i, \forall\ i \in \{2; \ldots; m\}$.



On each row l_k, $k \in \{2, \ldots, m-1\}$, the maximum number of cells that can be used is

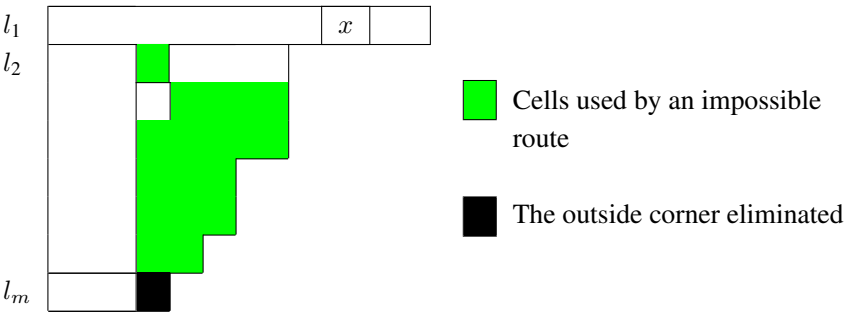
$$\lambda_k - (\lambda_m - 1) = \lambda_k - \lambda_m + 1.$$

Let N be the number of impossible expelling routes for x, for $m \geq 3$. Considering the cells that can be used on l_2 from left to right, we have:

- For the first cell, that is the λ_m^{th} cell on l_2, the number of impossible expelling routes using this cell is

  $$N_{(\lambda_2;1)} = (\lambda_3 - \lambda_m)P_{(\lambda;3;m)}$$

  because movements from left to right are impossible.



- For the 2^{nd} cell : $N_{(\lambda_2;2)} = (\lambda_3 - (\lambda_m + 1))P_{(\lambda;3;m)}$.
- For the j^{th} cell, $j \in \{1, \ldots, \lambda_3 - \lambda_m\}$:

  $$N_{(\lambda_2;j)} = (\lambda_3 - (\lambda_m + j - 1))P_{(\lambda;3;m)}.$$

  It will be noted that the last cell on l_2 for which there are impossible paths is reached for

  $$j = \lambda_2 - (\lambda_m - 1) - (\lambda_2 - \lambda_3 + 1) = \lambda_3 - \lambda_m$$

  because for each of the last $\lambda_2 - \lambda_3 + 1$ cells on l_2, there are no cells on l_3 that is strictly right.

  Let $Q(\mu_k; l) = \begin{cases} (\mu_k - (\mu_m + l))P_{(\mu;k;m)}, & \text{if } 0 \leq l < \mu_k - \mu_m \\ 0 & \text{otherwise} \end{cases}$, where l is an integer. It is checked that $Q(\lambda_3; l) = N_{(\lambda_2;j)}$, for $l = j - 1$ and as $j \in \{1, \ldots, \lambda_3 - \lambda_m\}$, then $l \in \{0, \ldots, n(\lambda_3)\}$.

  More generally, considering the cells liable to be used on l_k from left to right with $k = 2, \ldots, \lambda_{m-1}$, we have for the j^{th} cell, $j \in \{1, \ldots, \lambda_{k+1} - \lambda_m\}$,

  $$N_{(\lambda_k;j)} = Q(\lambda_{k+1}; j - 1).$$

  Therefore

  $$N = \sum_{k=3}^{m} \sum_{l=0}^{n(\lambda_k)} Q(\lambda_k; l) = \sum_{k=3}^{m} \sum_{l=0}^{n(\lambda_k)} (\lambda_k - (\lambda_m + l))P_{(\lambda;k;m)}.$$

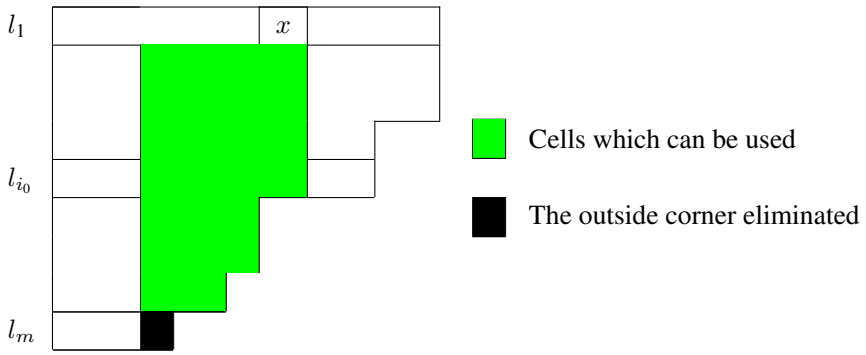
  It is clear that for $m = 3$, we have $N = 0$. So

  $$N = \sum_{k=3}^{m} P_{(\lambda;k;m)} \sum_{l=0}^{n(\lambda_k)} (\lambda_k - \lambda_m - l) = \sum_{k=3}^{m} P_{(\lambda;k;m)}(n(\lambda_k) + 1)(\lambda_k - \lambda_m - \tfrac{n(\lambda_k)}{2}).$$

  Then

  $$M = (\prod_{k=2}^{m-1} (\lambda_k - \lambda_m + 1)) - N = P_{(\lambda;1;m)} - \sum_{k=3}^{m} P_{(\lambda;k;m)}(n(\lambda_k) + 1)(\lambda_k - \lambda_m - \tfrac{n(\lambda_k)}{2}).$$

- Suppose now that $\lambda_2 > j$ and let us put $i_0 = max\{i \in \{2, \ldots, m\} : \lambda_i \geq j\}$.



For each row l_k, with $2 \leq k \leq i_0$, the maximum number of cells that can be used is $j - \lambda_m + 1$. And, for $k > i_0$, this number is equal to $\lambda_k - \lambda_m + 1$. Then considering the tableau U of shape $\mu = (\mu_1, \mu_2, \ldots, \mu_m)$ such that

$$\forall\, i \in \{1, \ldots, i_0\},\ \ \mu_i = j \ \text{ and } \forall\, k \in \{i_0 + 1, \ldots, m\}, \mu_k = \lambda_k,$$

we obtain

$$N = \sum_{k=3}^{m} P_{(\mu;k;m)}(n(\mu_k) + 1)(\mu_k - \mu_m - \tfrac{n(\mu_k)}{2}) \text{ and}$$
$$M = (j - \lambda_m + 1)^{i_0 - 1}(\prod_{k=i_0+1}^{m-1}(\lambda_k - \lambda_m + 1)) - N.$$

Then

$$M = P_{(\mu;1;m)} - \sum_{k=3}^{m} P_{(\mu;k;m)}(n(\mu_k) + 1)(\mu_k - \mu_m - \tfrac{n(\mu_k)}{2}).$$

□

Theorem 5.12. *Let T be a $SSYT$ of shape $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_m)$. We assume that T is the tableau of a cipher text to be decrypted and $K = (k_r, k_{r-1}, \ldots, k_1)$ the decryption key.*

Let $p = (\sum_{i=1}^{m} \lambda_i) - r$, and

$$U_{m,p} = \{(i_1, i_2, \ldots, i_m) \in \mathbb{N}^m : i_m \leq i_{m-1} \leq \cdots \leq i_1, p - 1 \leq i_1 \leq \lambda_1 \text{ and } 0 \leq i_j \leq \lambda_j \text{ for all } j = 2, \ldots, m\}.$$

Then the number of $SSYT$ used for the decryption of the cipher text is less than or equal to the following integer N_λ.

i) For $m = 1$, $N_\lambda = 0$;

ii) For $m \geq 2$,

- *(a) if $p \neq 1$, then $N_\lambda = card\,(U_{m,p}) - 1$;*
- *(b) if $p = 1$, then $N_\lambda = card\,(U_{m,1}) - 2$.*

Proof.

i) If $m = 1$, then $r = 0$ and the cipher text is equal to the clear text. There is no expulsion to do.

ii) Suppose $m \geq 2$. Then for each of the components of K, an outside corner in T is eliminated with $T = T(\lambda)$, $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_m)$ and $K = (k_r, k_{r-1}, \ldots, k_1)$.

It is remembered that: $\sum_{i=2}^{m} \lambda_i \leq r < \sum_{i=1}^{m} \lambda_i$.

At the end of the decryption, we obtain a row $SSYT$ having p cells ($p \geq 1$).

(a) Suppose $p \neq 1$. Then, at each step of the decryption following the key, we obtain $SSYT$ of shape $T_{i_1,\ldots,i_m}$, $(i_1, i_2, ..., i_m)$ being in $U_{m,p}$, where i_j denotes the number of cells on the j^{th} row of the tableau obtained, for all j in $\{1, 2, \ldots, m\}$. Therefore, determining all $SSYT$ for deciphering is equivalent to finding all the $SSYT$ of shape $T_{i_1,\ldots,i_m}$, except of course the case $i_j = \lambda_j$, for all $j = 1, 2, \ldots, m$. Indeed, the process of expulsion is impossible for $SSYT$ of shape $T_{p-1,i_2,\ldots,i_m}$. Now the number of $SSYT$ of shape $T_{i_1,\ldots,i_m}$ is exactly $card\, U_{m,p}$.

Consequently, we obtain: $N_\lambda = card\, U_{m,p} - 1$.

(b) For $p = 1$, let consider the following set: $V_{m,1} = \{(i_1, i_2, ..., i_m) \in U_{m,1} : i_1 \neq 0\}$. By a similar reasoning to the previous one: $N_\lambda = card\, V_{m,1} - 1$.

On the other hand: $card(V_{m,1}) = card(U_{m,1}) - 1$. Then: $N_\lambda = card(U_{m,1}) - 2$.

□

- Algorithm computing N_λ for $T = T(\lambda)$, $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_m)$

```
def Number (b, n_1, n_2, ..., n_m) :
    c = 0
    for i_1 from b to n_1 :
        for j from 2 to m :
            for i_j from 0 to n_j :
                if i_m ≤ i_{m-1} ≤ ··· ≤ i_1 :
                    c = c + 1
                else :
                    c = c
    print(c − 1)
def Number_of_SSYTab (B, λ_1, λ_2, ..., λ_m) :
    Number(B, λ_1, λ_2, ..., λ_m)
#B = p − 1 if p ≠ 1 and B = 1 for p = 1.
```

Example 5.13. Let encrypt the message:
"**The multiplication of Young tableaux is an internal operation**"
The ciphering gives the following tableau:

$T =$

1	1	1	1	1	1	9	14	14	14	15	18	20
2	5	5	5	9	9	12	15	24				
3	6	7	9	14	14	16	20					
5	9	9	12	15	15	18						
8	12	12	14	21								
13	15	19	20									
16	20	20										
20	21											
21	25											

$T = T(\lambda)$ with $\lambda = (13, 9, 8, 7, 5, 4, 3, 2, 2)$ a partition of 53 (the number of letters in the clear text).

The cipher text is

$\mathcal{C} =$ 20181514142414152009121618010914150109141521010509121420010 5070912192 00105060912152021250102030508131620 21.

For the decryption, there is at most $N_\lambda = 56613$ $SSYT$ used. But, to find the message by permutations on the cipher text, we have

$N = \frac{53!}{6!6!6!6!5!4!4!3!2!2!} = 95891321746968382123410869501936632662034022400000 00$

possible results, therefore considerably greater than N_λ.

Corollary 5.14. *Let T be a $SSYT$ of shape $\lambda = (\lambda_1, \lambda_2)$ and K $(K \in \mathbb{N}^{*r})$ the decryption key. Then:*

i) if $p > \lambda_2$, then $N_\lambda = (\lambda_2 + 1)(r - \lambda_2 + 2) - 1$;

ii) if $2 \leq p \leq \lambda_2$, then $N_\lambda = (\lambda_2 + 1)(\lambda_1 - \lambda_2 + 1) - 1 + \frac{(\lambda_2 - p + 1)(\lambda_2 + p)}{2}$;

iii) if $p = 1$, then $N_\lambda = (\lambda_2 + 1)(\lambda_1 - \lambda_2 + 1) - 1 + \frac{(\lambda_2 - 1)(\lambda_2 + 2)}{2}$.

Proof.
We have : $p = \lambda_1 + \lambda_2 - r$ and $U_{2,p} = \{(i,j)/\ p - 1 \leq i \leq \lambda_1, 0 \leq j \leq \lambda_2 \text{ and } j \leq i\}$.

i) For $p > \lambda_2$, the condition $j \leq i$ being verified, then

$$U_{2,p} = \{(i,j)/\ p - 1 \leq i \leq \lambda_1, 0 \leq j \leq \lambda_2\}$$

and $card(U_{2,p}) = card\{p-1, ..., \lambda_1\}.card\{0, ..., \lambda_2\} = (\lambda_1 - p + 2)(\lambda_2 + 1)$
$= (r - \lambda_2 + 2)(\lambda_2 + 1)$.

Then $N_\lambda = (\lambda_2 + 1)(r - \lambda_2 + 2) - 1$.

ii) For $2 \leq p \leq \lambda_2$, $U_{2,p} = A \cup B$ with $A = \{(i,j)/\ p - 1 \leq i \leq \lambda_2 - 1, 0 \leq j \leq i\}$ and $B = \{(i,j)/\ \lambda_2 \leq i \leq \lambda_1, 0 \leq j \leq \lambda_2\}$.

Since $A \cap B = \emptyset$ then $card(U_{2,p}) = card(A) + card(B)$. We have:

$card(A) = \sum_{i=p-1}^{\lambda_2 - 1} (\sum_{j=0}^{i} 1) = \sum_{i=p-1}^{\lambda_2 - 1} (i+1) = \sum_{i=p}^{\lambda_2} i = \frac{(\lambda_2 - p + 1)(\lambda_2 + p)}{2}$ and
$card(B) = card\{\lambda_2, ..., \lambda_1\}.card\{0, ..., \lambda_2\} = (\lambda_1 - \lambda_2 + 1)(\lambda_2 + 1)$.

So $card(U_{2,p}) = (\lambda_2 + 1)(\lambda_1 - \lambda_2 + 1) + \frac{(\lambda_2 - p + 1)(\lambda_2 + p)}{2}$ and then

$N_\lambda = (\lambda_2 + 1)(\lambda_1 - \lambda_2 + 1) - 1 + \frac{(\lambda_2 - p + 1)(\lambda_2 + p)}{2}$.

iii) For $p = 1$, $U_{2,p} = E \cup B$ with $E = \{(i,j)/\ 0 \leq i \leq \lambda_2 - 1, 0 \leq j \leq i\}$ and $B = \{(i,j)/\ \lambda_2 \leq i \leq \lambda_1, 0 \leq j \leq \lambda_2\}$.

Since $E \cap B = \emptyset$ then $card(U_{2,p}) = card(E) + card(B)$. We have:

$card(E) = \sum_{i=0}^{\lambda_2 - 1} (\sum_{j=0}^{i} 1) = \sum_{i=0}^{\lambda_2 - 1} (i+1) = \sum_{i=1}^{\lambda_2} i = \frac{\lambda_2(\lambda_2 + 1)}{2}$,
and $card(U_{2,p}) = (\lambda_2 + 1)(\lambda_1 - \lambda_2 + 1) + \frac{\lambda_2(\lambda_2 + 1)}{2}$.

Hence $N_\lambda = card(U_{2,p}) - 2 = (\lambda_2 + 1)(\lambda_1 - \lambda_2 + 1) - 1 + \frac{(\lambda_2 - 1)(\lambda_2 + 2)}{2}$.

It should be noted that the case $p = 1$ corresponds exactly to the case $p = 2$ in the previous situation ($2 \leq p \leq \lambda_2$). □

Remark 5.15. For $m = 2$, if the components of K are all strictly less than λ_1, then $r = \lambda_2$ and $N_\lambda = 2\lambda_2 + 1$.

More precisely, the number of possible $SSYT$ is exactly λ_2 and $\lambda_2 \leq N_\lambda$. Indeed, no outside corner is eliminated on l_1. Then $T_1 = T(\lambda_1)$. Hence $r = \lambda_2$ and for each of the components of K, one and only one $SSYT$ is obtained.

Corollary 5.16. *Let T be a $SSYT$ of shape $\lambda = (\lambda_1, \lambda_2, \lambda_3)$ and K $(K \in \mathbb{N}^{*r})$ the decryption key. Then:*

(i) if $p > \lambda_2$, then $N_\lambda = \frac{(\lambda_3 + 1)(\lambda_1 - p + 2)(2\lambda_2 - \lambda_3 + 2)}{2} - 1$;

(ii) if $\lambda_3 < p \leq \lambda_2$, then
$N_\lambda = \frac{(\lambda_3 + 1)}{2}[(\lambda_2 - p + 1)(\lambda_2 + p - \lambda_3) + (\lambda_1 - \lambda_2 + 1)(2\lambda_2 - \lambda_3 + 2)] - 1$;

(iii) *if* $1 < p \leq \lambda_3$, *then*
$N_\lambda = \frac{(\lambda_3-p+1)(3\lambda_3+3p-2)}{4} + \frac{\lambda_3(\lambda_3-1)(2\lambda_3-1)-(p-1)(p-2)(2p-3)}{12} + \frac{(\lambda_3+1)}{2}[(\lambda_2+1)(\lambda_2-\lambda_3) + (\lambda_1-\lambda_2+1)(2\lambda_2-\lambda_3+2)] - 1$;

(iv) *if* $p = 1$, *then*
$N_\lambda = \frac{\lambda_3(\lambda_3-1)(2\lambda_3-1)}{12} + \frac{(\lambda_3-1)(3\lambda_3+4)}{4} + \frac{(\lambda_3+1)}{2}[(\lambda_2+1)(\lambda_2-\lambda_3) + (\lambda_1-\lambda_2+1)(2\lambda_2-\lambda_3+2)] - 1$.

Proof. We have : $p = \lambda_1 + \lambda_2 + \lambda_3 - r$ and

$$U_{3,p} = \{(i,j,k) \in \mathbb{N}^3 : p-1 \leq i \leq \lambda_1, 0 \leq j \leq \lambda_2, 0 \leq k \leq \lambda_3 \text{ and } k \leq j \leq i\}.$$

Let $I = \{p-1, \ldots, \lambda_1\}, J = \{0, 1, \ldots, \lambda_2\}$ and $L = \{0, 1, \ldots, \lambda_3\}$.

(i) For $p > \lambda_2, U_{3,p} = V_1 \cup V_2$ with
$V_1 = \{(i,j,k) \in U_{3,p} \,/\, p-1 \leq i \leq \lambda_1, 0 \leq j \leq \lambda_3 - 1, 0 \leq k \leq j\}$
and $V_2 = \{(i,j,k) \in U_{3,p} \,/\, p-1 \leq i \leq \lambda_1, \lambda_3 \leq j \leq \lambda_2, 0 \leq k \leq \lambda_3\}$.
Since $V_1 \cap V_2 = \emptyset$, then $card(U_{3,p}) = card(V_1) + card(V_2)$. We have
$card(V_1) = card(I).\sum_{j=0}^{\lambda_3-1}(\sum_{k=0}^{j}1)$ = $(\lambda_1-p+2)(\sum_{j=0}^{\lambda_3-1}(j+1))$ = $(\lambda_1-p+2)(\sum_{j=1}^{\lambda_3}j)$
$card(V_1) = \frac{1}{2}\lambda_3(\lambda_1-p+2)(\lambda_3+1)$, and
$card(V_2) = card(I).card\{\lambda_3, ..., \lambda_2\}.card(L) = (\lambda_1-p+2)(\lambda_2-\lambda_3+1)(\lambda_3+1)$.
Then $card(U_{3,p}) = \frac{1}{2}(\lambda_1-p+2)(\lambda_3+1)(2\lambda_2-\lambda_3+2)$.
Therefore $N_\lambda = \frac{(\lambda_3+1)(\lambda_1-p+2)(2\lambda_2-\lambda_3+2)}{2} - 1$.

(ii) For $\lambda_3 < p \leq \lambda_2$, $U_{3,p}$ is a disjoint union of four sets below:
$V_3 = \{(i,j,k) \,/\, p-1 \leq i \leq \lambda_2 - 1\}, 0 \leq j \leq \lambda_3 - 1, 0 \leq k \leq j\}$;
$V_4 = \{(i,j,k) \,/\, p-1 \leq i \leq \lambda_2 - 1, \lambda_3 \leq j, k \in L\}$;
$V_5 = \{(i,j,k) \,/\, \lambda_2 \leq i \leq \lambda_1, 0 \leq j \leq \lambda_3 - 1, 0 \leq k \leq j\}$;
$V_6 = \{(i,j,k) \,/\, \lambda_2 \leq i \leq \lambda_1, \lambda_3 \leq j \leq \lambda_2, k \in L\}$.

$card(V_3) = card\{p-1, \ldots, \lambda_2 - 1\}.\sum_{j=0}^{\lambda_3-1}(\sum_{k=0}^{j}1)$ = $\frac{1}{2}\lambda_3(\lambda_3+1)(\lambda_2-p+1)$;
$card(V_4) = card(L).\sum_{i=p-1}^{\lambda_2-1}(\sum_{j=\lambda_3}^{i}1)$ = $(\lambda_3+1)\sum_{i=p-1}^{\lambda_2-1}(i-\lambda_3+1)$ = $(\lambda_3+1)\sum_{i=p-\lambda_3}^{\lambda_2-\lambda_3}i$
$card(V_4) = \frac{1}{2}(\lambda_3+1)(\lambda_2-p+1)(\lambda_2+p-2\lambda_3)$;
$card(V_5) = card\{\lambda_2, \ldots, \lambda_1\}.\sum_{j=0}^{\lambda_3-1}(\sum_{k=0}^{j}1)$ = $\frac{1}{2}\lambda_3(\lambda_3+1)(\lambda_1-\lambda_2+1)$;
$card(V_6) = card\{\lambda_2, \ldots, \lambda_1\}.card\{\lambda_3, \ldots, \lambda_2\}.card(L)$
$card(V_6) = (\lambda_3+1)(\lambda_1-\lambda_2+1)(\lambda_2-\lambda_3+1)$.
Hence we have: $card(U_{3,p}) = \sum_{i=3}^{6}card(V_i)$;
$card(U_{3,p}) = \frac{1}{2}(\lambda_3+1)[(\lambda_2-p+1)(\lambda_2+p-\lambda_3) + (\lambda_1-\lambda_2+1)(2\lambda_2-\lambda_3+2)]$
and then
$N_\lambda = \frac{(\lambda_3+1)}{2}[(\lambda_2-p+1)(\lambda_2+p-\lambda_3) + (\lambda_1-\lambda_2+1)(2\lambda_2-\lambda_3+2)] - 1$.

(iii) For $1 < p \leq \lambda_3$, $U_{3,p}$ is a disjoint union of five sets: V_5, V_6 and
$V_7 = \{(i,j,k) \,/\, p-1 \leq i \leq \lambda_3 - 1, 0 \leq j \leq i, 0 \leq k \leq j\}$;
$V_8 = \{(i,j,k) \,/\, \lambda_3 \leq i \leq \lambda_2 - 1, 0 \leq j \leq \lambda_3 - 1, 0 \leq k \leq j\}$;
$V_9 = \{(i,j,k) \,/\, \lambda_3 \leq i \leq \lambda_2 - 1, \lambda_3 \leq j \leq i, k \in L\}$.

$card(V_7) = \sum_{i=p-1}^{\lambda_3-1}(\sum_{j=0}^{i}(\sum_{k=0}^{j}1)) = \sum_{i=p-1}^{\lambda_3-1}(\sum_{j=0}^{i}(j+1)) = \sum_{i=p-1}^{\lambda_3-1}(\sum_{j=1}^{i+1}j) = \sum_{i=p-1}^{\lambda_3-1}\frac{(i+1)(i+2)}{2}$
$card(V_7) = \frac{1}{2}\sum_{i=p-1}^{\lambda_3-1}(i^2+3i+2) = \frac{1}{2}\sum_{i=p-1}^{\lambda_3-1}i^2 + \frac{3}{2}\sum_{i=p-1}^{\lambda_3-1}i + \sum_{i=p-1}^{\lambda_3-1}1$

$card(V_7) = \frac{\lambda_3(\lambda_3-1)(2\lambda_3-1)-(p-1)(p-2)(2p-3)}{12} + \frac{(\lambda_3-p+1)(3\lambda_3+3p-2)}{4}$.

$card(V_8) = card\{\lambda_3, ..., \lambda_2 - 1\}. \sum_{j=0}^{\lambda_3-1} (\sum_{k=0}^{j} 1) = (\lambda_2 - \lambda_3) \sum_{j=0}^{\lambda_3-1} (j+1);$

$card(V_8) = (\lambda_2 - \lambda_3) \sum_{j=1}^{\lambda_3} j = \frac{1}{2}(\lambda_3 + 1)(\lambda_2 - \lambda_3).$

$card(V_9) = card(L). \sum_{i=\lambda_3}^{\lambda_2-1} (\sum_{j=\lambda_3}^{i} 1) = (\lambda_3 + 1) \sum_{i=\lambda_3}^{\lambda_2-1} (i - \lambda_3 + 1) = (\lambda_3 + 1) \sum_{i=1}^{\lambda_2-\lambda_3} i$

$card(V_9) = \frac{1}{2}(\lambda_3 + 1)(\lambda_2 - \lambda_3)(\lambda_2 + 1).$

Hence we have: $card(U_{3,p}) = \sum_{i=5}^{9} card(V_i)$

$card(U_{3,p}) = \frac{\lambda_3(\lambda_3-1)(2\lambda_3-1)-(p-1)(p-2)(2p-3)}{12} + \frac{(\lambda_3-p+1)(3\lambda_3+3p-2)}{4} +$

$\frac{(\lambda_3+1)}{2}[(\lambda_2 + 1)(\lambda_2 - \lambda_3) + (\lambda_1 - \lambda_2 + 1)(2\lambda_2 - \lambda_3 + 2)]$

and then

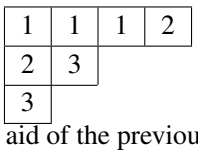
$N_\lambda = \frac{\lambda_3(\lambda_3-1)(2\lambda_3-1)-(p-1)(p-2)(2p-3)}{12} + \frac{(\lambda_3-p+1)(3\lambda_3+3p-2)}{4} +$

$\frac{(\lambda_3+1)}{2}[(\lambda_2 + 1)(\lambda_2 - \lambda_3) + (\lambda_1 - \lambda_2 + 1)(2\lambda_2 - \lambda_3 + 2)] - 1.$

(iv) For $p = 1$, it suffices to replace p by 2 in the relationship obtained for $1 < p \leq \lambda_3$. Then we get:

$N_\lambda = \frac{\lambda_3(\lambda_3-1)(2\lambda_3-1)}{12} + \frac{(\lambda_3-1)(3\lambda_3+4)}{4} + \frac{(\lambda_3+1)}{2}[(\lambda_2+1)(\lambda_2-\lambda_3)+(\lambda_1-\lambda_2+1)(2\lambda_2-\lambda_3+2)] - 1.$

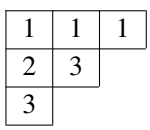
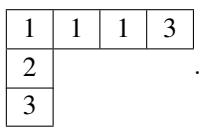
□

Example 5.17. Let $T =$  and $K = (4, 3, 4, 3)$ be the decryption key.

It is verified with the aid of the previous formula that $N_\lambda = 14$.

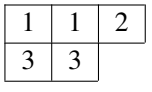
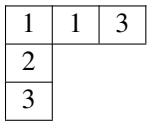
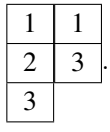
Let decrypt the message.

$a)$ For $k_4 = 4$, we expel 2 from T. Two $SSYT$ are obtained:

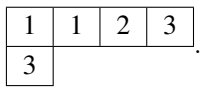
$T_1 =$  and $T_2 =$  .

$b)$ For $k_3 = 3$, we expel 1 from the preceeding tableaux. Four $SSYT$ are obtained:

- For T_1, we have three $SSYT$:

$T_3 =$  , $T_4 =$  and $T_5 =$  .

- For T_2, we have only one $SSYT$:

$T_6 =$  .

$c)$ For $k_2 = 4$, we expel 3 from T_6. A single $SSYT$ is obtained. For the tableaux T_3, T_4 and T_5 the operation is impossible.

$$T_7 = \begin{array}{|c|c|c|}\hline 1 & 1 & 2 \\ \hline 3 \\ \cline{1-1} \end{array}.$$

d) For $k_1 = 3$, we expel 2 from T_7. Two $SSYT$ are obtained:

$$T_8 = \begin{array}{|c|c|c|}\hline 1 & 1 & 3 \\ \hline \end{array} \quad \text{and} \quad T_9 = \begin{array}{|c|c|}\hline 1 & 1 \\ \hline 3 \\ \cline{1-1} \end{array}.$$

We get the clear message after 9 tableaux.

Corollary 5.18. *Let $T = T(\lambda)$, $\lambda = (1^m)$ and $K = (k_r, k_{r-1}, \ldots, k_1)$ the decryption key. Then the number N of $SSYT$ used for decryption is:*

$$N = N_\lambda = m - 1.$$

Proof. $T = T(\lambda)$ with $\lambda = (1^m)$. Then $r = m - 1$ and $K = (1, 1, \ldots, 1)$.

At each step with the key K, exactly one $SSYT$ is obtained because there is only one possible bumping route. So

$$N = \sum_{i=1}^{r} 1 = r \text{ and } N_\lambda = card(U_{m,1}) - 2 = (m + 1) - 2 = m - 1.$$

□

Young tableaux are well used as cryptosystem. They permit to encrypt and decrypt texts. The number N_λ found for the number of semi-standard Young tableaux used for decryption of a given cipher text is just a bound, the aim being to find exactly the number of $SSYT$ used, or a better bound for this number.

References

[1] G. H. Hardy and S. Ramanujan, *Asymptotic formulae in combinatory analysis, Proc London Math Soc,* 2, 17, (1918), 75 − 115

[2] Kenneth H. Rosen, Ph D., *Discrete mathematics and its applications, Cryptography theory and practice, third edition,* 2006

[3] Laurent Chéno, *La lettre de Caml, numéro* 6*, été* 1997, 39 *pages*

[4] Marcel Schützenberger, *Propriétés nouvelles des tableaux de Young, Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome* 19, $n°2$ (1977 − 1978)*, exp.*$n°$26*, p.*1 − 14

[5] Mathieu Mansuy, *Tableau de Young et Bases Cristallines de $U_q(sl_{n+1})$, exposé au séminaire de Jussieu,* 29 *novembre* 2012

[6] William Fulton, *Young tableaux with applications to representation theory and geometry, University of Chicago, Department of Mathematics, Cambridge University Press,* 1997 − 260 *pages.*

Author information

Kolo F. SORO, Eric D. AKEKE and Konan M. KOUAKOU,
Département de Mathématiques et Informatique,
Université Félix Houphouët Boigny,
22 BP 582 Abidjan 22, CÔTE D'IVOIRE.
E-mail: koloetienne180@gmail.com, ericdago@yahoo.fr, makonankouakou@yahoo.fr

Received: August 14, 2018.
Accepted: April 15, 2019.