# Uruguayan cryptographic carpet

**Juan José Cabezas**
Instituto de Computación
Facultad de Ingeniería
Universidad de la República
Montevideo, Uruguay
jcabezas@fing.edu.uy

**Joachim von zur Gathen**
B-IT, Universität Bonn
Germany
gathen@
bit.uni-bonn.de

**Jorge Tiscornia**
Presidencia Uruguay
Montevideo, Uruguay
jtiscornia@
presidencia.gub.uy

## Abstract

We present a unique item in the history of cryptography: a woollen carpet woven in a Uruguayan penitentiary in 1980 during the dictatorship in that country. The colors of a pair of horizontally adjacent knots encrypt a single letter. The carpet is in moderately good shape, with loss of colors and some damage by moths. We had obtained the original code and here report on the deciphering. The plaintext is a political message destined to comrades outside, with a description of the political situation and directives for actions.

The cryptosystem is a simple substitution. Breaking such codes is trivial. The real task here is to translate the knots into a machine-readable representation of their colors, in the presence of unclear colors and damage to parts of the carpet.

The encrypted carpet is an important document from the dark times of the Uruguayan dictatorship, manufactured by prisoners from the guerrilla movement *Tupamaros*. Two of the present authors (JJC and JT) were active members of this group. Their personal memories were essential for our successful reconstruction of the plaintext.

## 1 Introduction

Uruguay (*República Oriental del Uruguay*) borders on Brazil, Argentina, and the Atlantic Ocean with the estuary of the Río de la Plata. It was known as the *Switzerland of South America* because of its wealth, safety, and democratic governance. An economic downturn started in the 1960s. In its wake, militant groups arose.

On the extreme right side, the JUP (*Juventud Uruguaya de Pie*, Uruguayan youth standing up) aimed at the unions and other leftists, and their death squads killed some of their enemies.

On the left side was the MLN (*Movimiento de Liberación Nacional*, Movement for national liberation). Its members were known as the *Tupamaros*, after the leader Túpac Amaru II of an anticolonial uprising in Perú around 1780.

By 1973, the Tupamaros were essentially defeated by the government forces, their leaders killed, imprisoned, or refugees abroad. Many of them were held at a penitentiary with the unlikely name of *penal de Libertad*. The town of Libertad (Liberty) is located 51 km from Montevideo, the capital of Uruguay, and was founded by European refugees in the 19th century, happy to find their religious liberty. *Penal* is prison or penitentiary.

The Tupamaro inmates composed, in discussions over three years, a lengthy text to their companions outside, still in liberty (with small l). How to get it out of prison?

They were allowed to produce handicraft articles, receiving the materials at 8 am and handing them back at 4.30 pm. Ricardo García wove the carpet in several months' work in 1980. The carpet successfully left the prison.

A relative of Ricardo García received the carpet but it never reached its destination, an MLN group in Sweden. When the relative went into exile in Germany, he had the cipher table (Table 2), but lost it and remembered it only years later. The carpet was never decrypted in its time.

Uruguay regained democracy in 1985 and the prisoners of Libertad were freed. 29 years later, Jorge Tiscornia found the carpet in Ricardo García's home, and he was also given the cipher table. At the end of 2014, he told Juan José Cabezas about the carpet (Figure 1) who then set out to decipher it.

The carpet is unique in several aspects; it shows an imaginative use of simple cryptography under the dire circumstances of prison, and it is a unique

*Proceedings of the 1st Conference on Historical Cryptology*, pages 21– 27,
Uppsala, Sweden, 18-20 June, 2018

Figure 1: The carpet.

testimony of its type concerning this historic period.

The only other encryption methods by weaving or knotting that we are aware of are the Inca quipus and the encrypted quilts on the underground railway for black slaves fleeing from the USA to Canada in the 19th century (see Tobin (1999)).

The Tupamaros were inspired by Dickens' *Tale of Two Cities* (Dickens, 1859). It distills the atmosphere in pre-revolutionary France around 1789. A tough tavern owner, a central character in the book, works as the eyes and ears of the pre-revolution. She knits diligently accounts into her knitware, of evil persons, their deeds, and of spies, dreaming of future vengeance. "Knitted, in her own stitches and her own symbols, it will always be as plain to her as the sun." For any malefactor, it would be easier "to erase himself from existence, than to erase one letter of his name or crimes from the knitted register of Madame Defarge." Dickens says nothing about her encryption method, but these words were enough to fire the penitentiary inmates' imagination and inspire the idea of their carpet. Dickens' poetic introductory sentence refers to the French Revolution, but it describes the Tupamaros' situation as well: "It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness, it was the epoch of belief, it was the epoch of incredulity, it was the season of Light, it was the season of Darkness, it was the spring of hope, it was the winter of despair, we had everything before us, we had nothing before us, we were all going direct to Heaven, we were all going direct the other way.".

## 2 The encryption method

In the following, we distinguish typographically between `ciphertext` and *plaintext*.

The coding method, communicated by Ricardo García to us, uses a simple substitution on 18 letters. Each letter is encoded by a pair of horizontally adjacent colors, allowing six colors for the first item and three for the second one.

The encoding goes as follows:

| O | G | B | L | W | P | color |
|---|---|---|---|---|---|---|
| *M* | *A* | *R* | *K* | *O* | *S* | O |
| *D* | *I* | *N* | *T* | *E* | *L* | G |
| *J* | *U* | *P* | *V* | *H* | *F* | B |

Table 1: The code.

using the following six colors:

| color | abbr |
|---|---|
| orange, yellow | O |
| dark green | G |
| beige, pink, ochre | B |
| light green | L |
| white, light gray | W |
| purple | P |

Table 2: The colors.

The lines stand for Marcos, (door) lintel, and JUP (see above). VHF presumably is a filler with the remaining letters and unlikely to refer to *very high frequency*. The system thus employs a reduced alphabet of 18 letters: *A, D, E, F, H, I, J, K, L, M, N, O, P, R, S, T, U, V*. Taking into account the phonetics and orthography of the Latin American Spanish language, some of them represent more than one letter:

- *K* represents the letter k, and qu, and also c when pronounced like k.
- *V* represents v and b.
- *S* represents s, and also c when pronounced like s.
- *J* represents j and g.
- *I* represents i and y.

It was not meant as a simplified orthography of Spanish, but can be taken as such. (In today's text messages in Spanish, K is often used for qu.) For example, the list of color pairs

```
(W,O),(P,G),(G,O),(L,O),
(W,G),(L,G),(G,O),(P,G)
```

encrypts the text *OLAKETAL*. Interword spaces, the (silent) initial H, and punctuation marks are not present, and the list represents the phrase *Hola que tal* (Hi, how are you?).

The absence of spaces, accents, and punctuation marks means that a string of colors may represent more than one grammatically and semantically valid text. In our decipherment, such ambiguities were an obstacle, and this might be worse if this method was used elsewhere without the a priori knowledge we had about the context.

## 3 The current state of the carpet

The carpet measures $55.3 \times 36.8$ cm and contains almost 13 000 knots for about 6400 encrypted letters, arranged in a matrix of 67 rows and 96 columns. Moths have totally or partially damaged about 10% of the color pairs, and the borders are frayed, as is visible in the figures.

We distilled from a high-resolution digital image of the carpet a machine-readable matrix of colors. Our software then transformed the resulting RGB values to one of the six colors. This had to be done in a robust way so that similar colors were transformed to the same value, but distinct colors were properly distinguished. Then adjacent pairs of knots were deciphered as individual letters, proper word separations introduced, and the final decipherment produced. This was less than straightforward, and we encountered the following problems.

1. Damage to the carpet.
2. About 5% of the colors ran into adjacent knots, affecting their (automatic) legibility.
3. After 35 years, colors have degraded. In some parts, it is difficult to distinguish between white and ochre, and between light and dark green.
4. The reading ambiguities mentioned above sometimes make interpretation difficult. For example, the string *AKNTPERONOA* is to be read as *a CNT pero no a* ... (to CNT but not to ...) where CNT is the *Convención Nacional de Trabajadores* (National Convention of Workers).

## 4 Decryption

The digitized image is presented in Postscript, which is then converted to plaintext. We illustrate the process on the carpet's second line, magnified in Figures 3 through 5 and its decryption in Figure 6.

Each dot of color is given as an RGB (Newman and Sprouil, 1983) triple of red, green, and blue values, each ranging from 0 to 25.

We took samples from various sections of the carpet and determined the range of RGB values for each color, and also the fractions of these values, in order to be able to account for dark or light sections. That is, 6 7 8 and 7 8 9 represent the same hue, the latter slightly lighter than the former. Overlap of these values and fractions occurred mainly for G (dark green) and L (light green), and for B (beige) and W (white). Since G and B occur more frequently in the carpet than L

Figure 2: The bottom left shows moth damage and lost material on the fringes.

Figure 3: The second line, left part. It starts at top left and ends at bottom right.

Figure 4: The second line, middle part.

Figure 5: The second line, right part.

| GO | BO | GO | PB | GO | PG | WG | BO | WO | PG | GB | WG | OB | WO | GG | OG |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *a* | *r* | *a* | *f* | *a* | *l* | *e* | *r* | *o* | *l* | *u* | *e* | *j* | *o* | *i* | *d* |
| GO | LB | GG | WG | OB | WO | PO | PO | WG | BB | BO | WO | OG | GB | PO | WG |
| *a* | *v* | *i* | *e* | *j* | *o* | *s* | *s* | *e* | *p* | *r* | *o* | *d* | *u* | *s* | *e* |
| GO | BG | G? | ?? | LO | GG | GO | OG | GB | BO | GO | BG | LG | WG | | |
| *a* | *n* | *a* | *r* | *k* | *i* | *a* | *d* | *u* | *r* | *a* | *n* | *t* | e | | |

Figure 6: Part of the second line transcribed (upper line) and decrypted (lower line).

and W, respectively, we opted to use the former in ambiguous cases.

The next step was to convert these color values into text. We covered each knot in the carpet by small horizontal rectangles, whose width was about that of the whole knot. Our matrix algorithm (James D. Foley and Hughes, 1990) scanned each rectangle and looked for a dominant color among the rectangles of each knot. If a dominant color was found, it was considered the color of the knot. In a pair of adjacent knots starting in an "even" position, there are six possible colors for its first member and three for its second one. Invalid dominant colors, damaged areas, and the absence of a dominant color are also reported.

In cases of doubt, we also employed a vector search using vertical vectors in the middle of the knot. If two or more occurrences of a valid color were detected, then four vertical vectors determined its dominance in the knot.

In the end, we obtained a sequence of knot colors, with numerous unresolved cases.

Bypassing the intermediate steps explained below, we take the carpet's second line as an example in Figures 3 through 6.

## 5 Recovering the plaintext

In another example, from the carpet's third line, we illustrate some of the steps from the raw identification of letters, with many unclear positions, into plaintext. This was no easy task and required substantial manual intervention. We first discovered some obvious plaintext snippets, then searched for valid words before and after such pieces, and in the case of damaged knots, had to visually inspect the carpet.

Letters without parenthesis or bracket are considered correct by the software. * is an unrecognized letter, *(MARKOS)*, *(DINTEL)*, and *(JUPVHF)* show six possible choices, and similarly *(MDJ)*, *(AIU)*, *(RNJ)*, *(KTV)*, *(OEH)*, and *(SLF)* correspond to three possibilities. These indicate that the first or second color of a pair, respectively, may be damaged. $[c1|c2$ means that letter c1 seems more likely than letter c2 in this place, and $< c >$ indicates the letter c, but with low probability.

So here are the steps from the original letters to plaintext. Lower case letters in the fourth text present guessed corrections of the automatic color readings.

*N[U|*L(SLF)ARD(DINTEL)SARROLLOIDAR*
*ESPLIKASION[I|*K[D|*EP*OTA*
*TRESTENDENSIAAN<I>TIM<D>*
*LN[a|*(KTV)J[N|*FALSO**

*N[U|*L(SLF)AR DESARROLLO I DAR*
*ESPLIKASION [I|*K[D|*EP*OTA*
*TRES TENDENSIA AN<I>TIM<D>LN[a|*
*(KTV)J[N|* FALSO*

*N[U|*L(SLF)AR DESARROLLO I DAR*
*ESPLIKASION [I|*K[D|*EP*OTA*
*TRES TENDENSIA ANTI MLN [a|*
*(KTV)J[N|* FALSO*

*pULSAR DESARROLLO I DAR*
*ESPLIKASION DErrOTA*
*TRES TENDENSIA ANTI MLN*
*KoN FALSO*

*... pulsar desarrollo y dar explicación derrota. Tres - tendencia anti-MLN con falso ...* (... further the development and give an explanation of [our] defeat. Third—anti-MLN tendency with false...)

A translation into plaintext would have been hard without the personal acquaintance of Tiscornia with the situation and political context of the MLN and the penitentiary at Libertad around 1980.

## 6 Conclusions

We have recovered the plaintext of about 95% of the carpet; only small parts of it are damaged beyond recognition. The carpet is now becoming a valuable testimony of Uruguayan and Latin American history.

From a cryptographical point of view, the following aspects are particularly interesting:

- The inmates have succeeded in encrypting a substantial amount of information by means of material accessible to prisoners in the penitentiary.
- The construction of the carpet presumably involved a large number of hours, but then, time is the one thing that is abundant in prison.
- The prisoners used a simple coding mechanism in a clever way which even fooled the exit checks at the prison.

In terms of cryptanalytic techniques, our task was trivial once the sequence of colors was established. However, given just that sequence with its many errors and ambiguities, it is not clear how easy this task would have been without the knowledge of the encryption in Table 2.

In synthesis, we have an original piece of cryptography, well conceived and well implemented. It was secure, efficient, and economic under the dire circumstances of the penitentiary. The fact that we could decipher it 35 years later shows the success of their method.

## 7 The first lines of the computer generated transcription.

The first four lines of the transcription read as follows:

*(DINTEL)MD[A|*FA(DINTEL)*E*OLUEJO*
*IDAVIEJO(MARKOS)SP<M>RODUSE*
*ANUJKIAD(AIU)RA(DINTEL)TETRESA(RNP)*
*(DINTEL)OSPORKAUSASUNO(SLF)*

*[*|*E(MARKOS)II<*>DI(KTV)*
*(JUPVHF)(DINTEL)FIATS*
*APO<*>LITIKAI<P>UER*
*SONA(DINTEL)AT(JUPVHF)*
*DONI(KTV)E(DINTEL)*
*I[I|*O<*>SINKANASDI<A>RIJE<*
*T>ITESN<*>EIM(SLF)*

*N[U|*L(SLF)ARD(DINTEL)SARROLLOIDAR*
*ESPLIKASION[I|*K[D|*EP*OTATR*
*ESTENDENSIAAN<I>TIM<D>L*
*N[a|*(KTV)J[N|*FALSO**

*DP[R|*SLE<I>NINDESTRUIENDO*
*ENVE(MARKOS)*
*DEELEV[N|*V[R|*T<*>ODOESTOK*
*ON(JUPVHF)OKAKOM<*>UNIA<I>D*
*[A|*SIONITE(DINTEL)SIO**

Distilling cleartext from this is not always obvious.

## 8 Parts of the carpet's cleartext.

We present the initial part of the cleartext. The opinions and political points of view expressed in this document do not, in any way, reflect necessarily those of the authors or their institutions. Comments between brackets are the authors'.

A complete version of the cleartext (in Spanish) can be found at `https://www.fing.edu.uy/~jcabezas/papers/ElTapizMLN2015.pdf`.

**[First line.]** *...ona: sólo tu debe conocer vía y forma. Traduce esto, al final te aclaro. Hazlo llevar ...ama Falero.*

**[Introduction.]** *Luego ida viejos se produce anarquía durante tres años por causas:*

1. *pérdida confianza política y personal a todo nivel,*
2. *incapacidad dirigentes de impulsar desarrollo y dar explicación derrota y*
3. *tendencia anti-MLN con falso marxismo-leninismo, destruyendo en vez de elevar, todo esto con poca comunicación y tensión represiva.*

*Arriba hay confianza y crece, fierreros y divisionistas retroceden.*

*El correcto marxismo-leninismo va mas lento, dirección autocrítica MLN, un paso necesario y defectuoso.*

**[Previous events.]** *Luego del año 55, la izquierda marxista será determinada por dos hechos:*

1. *lucha de clases desatada por crisis económica*
2. *discusión ideológica internacional entre vía violenta o pacífica al socialismo.*[1]


### Acknowledgements

Alfredo "Tuba" Viola brought the authors together during a course given by the second author in Montevideo. Without his support, this paper would not have come into being, and we thank him for it.



**About the authors.** JJC is a professor of computer science at the Instituto de Computación in the Universidad de la República, Uruguay. He was


[1] [M]ona: only you must know the method and form. Translate this, at the end I explain it. Take it [... ama] Falero.
After the older leaders left, we had anarchy during three years for various reasons: 1. loss of political and personal confidence at all levels, 2. inability of the leaders to further development and explain our defeat, 3. anti-MLN tendency with false marxism-leninism, destroying rather than elevating, all this with little communication and repressive tension.
On the higher floors [where the leaders were housed, floors 3 to 5] we have growing confidence, [but] warriors [who want to continue the armed struggle] and divisionists [who prefer a political party for the struggle] retreat. The correct marxism-leninism goes more slowly, in the direction of MLN self-criticism, a necessary step that is missing.
Since 1955, the marxist left has been determined by two facts: 1. class struggle unleashed by the economic crisis, 2. international ideological discussion between violent and peaceful road to socialism.

severely injured in 1970 while manufacturing a bomb in his workshop and fled the country, hidden in the trunk of a car. JvzG is an emeritus professor of computer science at the Universität Bonn, Germany, and has no experience in building bombs. JT (Jorge Carlos Tiscornia Bazzi) is an Uruguayan writer and was a member of the Tupamaro *Colona 15*, together with JJC. He now works at the Presidencia Uruguay. During his 4646 days in the penitentiary of Libertad, from 1972 to 1985, he kept a secret diary on small slips of paper, normally used to roll cigarettes. He hid them in wooden clogs that he used in the shower. They are now published (Tiscornia (2012)) and provide moving insights into the (in)human conditions in prison, see also Tiscornia (2014). They were turned into a documentary movie (Charlo (2014)).

## References


José Pedro Charlo. 2014. *El almanaque. Documentary movie.* Argentina, Spain, Uruguay.

Charles Dickens. 1859. *A Tale of Two Cities*. Chapman & Hall, London.

Steven K. Feiner James D. Foley, Andries van Dam and John F. Hughes. 1990. *Computer Graphics Principles and Practice*. Adisson Wesley.

William M. Newman and Robert F. Sprouil. 1983. *Principles of Interactive Computer Graphics*. Mc Graw Hill.

Jorge Tiscornia. 2012. *El almanaque*. Yaugurú, Montevideo, Uruguay.

Jorge Tiscornia. 2014. *Nunca en domingo. Relatos. Penal de Libertad 1972-1985*. Ediciones de la Banda Oriental, Montevideo, Uruguay.

Jacqueline Tobin. 1999. *Hidden in Plain View. A secret story of quilts and the underground railway*. Anchor Books, New York.