Part I
Crypting Protocol

We will crypt a simple message containing the word 'salut'.
In a first step we have to compute the weight list of the differents caracters (meaning an approximation of the ASCII code used in the computer code algorithm).

Weigth List

Giving 0 to 'a' to 26 to 'z', we have : *18.0.11.20.19* as the weigth list of the string

Cumulated weigth list

Once done, we have to compute the cumulated weigth list. I mean, the list application can be considered as a suit defined by :

$$u_n \text{ a suit from N to N with the length } n \in \text{N} \quad | \quad u_i{=}u_{i-2}{+}u_{i-1}$$

In our case, the computed list is *18.18.29.49.68* We call it v_i

Key Computing

At this moment we have to compute the public key k_i of the algorithm defined via modulo since the formula :

$$\begin{cases} k_i = [u_i.u_{n-i} \quad mod \quad 26] + 10 & if \quad \exists u_i, u_{n-i} \\ u_j & if \quad !\exists u_j, j = n/2+1 \end{cases}. \tag{1}$$

With our example, it gives :

$$\begin{cases} k_0 = [18.19 \quad mod \quad 26] + 10 = 14 \\ k_1 = [20.0 \quad mod \quad 26] + 10 = 10 \\ k_2 = [11 \quad mod \quad 26] + 10 = 11 \end{cases}. \tag{2}$$

We build the full Length key ξ using the formula :

$$\begin{cases} \xi_i = k_i & if \quad i <= n/2+1 \\ \xi_i = k_{n-i} & if \quad i > n/2+1 \end{cases}. \tag{3}$$

Crypting Process

The crypting process is ruled by a pseudo-convolution with the given symbol $*$ meaning a point by point multiplication. This newer suit is ruled by v_i and u_i
We call it w_i defined by : $v_i * u_i$
In our example, it gives :

$$\begin{cases} w_0 = v_0.u_0 = 324 \\ w_1 = v_1.u_1 = 0 \\ w_2 = v_2.u_2 = 319 \\ w_3 = v_3.u_3 = 980 \\ w_4 = v_5.u_4 = 1292 \end{cases} . \tag{4}$$

We obtain the suit w=*324.0.319.980.1292*

Encryption

At the end we use the Encryption into differents numeric bases to hide the crypting process.
The Base indexes are defined by the key ξ
The list to encrypt is defined by w
The Encryption process will be caled Ξ
Defined by :

$$\Xi_i = (w_i)_{\xi_i} \tag{5}$$

$$\begin{cases} \Xi_0 = (w_0)_{\xi_0} = (324)_{14} = 192 \\ \Xi_1 = (w_1)_{\xi_1} = (0)_{10} = 0 \\ \Xi_2 = (w_2)_{\xi_2} = (319)_{11} = 270 \\ \Xi_3 = (w_3)_{\xi_3} = (980)_{10} = 980 \\ \Xi_4 = (w_4)_{\xi_4} = (1292)_{14} = 684 \end{cases} . \tag{6}$$

The Encrypted suit is Ξ = *192.0.270.980.684*
Its associate key is ξ = *14.10.11.10.14*

Part II

Decrypting Protocol

Initialisation

In this demonstration, we will use a Encrypted list using the Raptor cryptographic algorithm. The terms list is given by :

!018kh"05a3c#8064$12vj%2gai&0605a(67500)0ba30*277a4+25376,2a5db-581336u7!146367"27706#1j68c

The associated key is given as a public key :

2116103428141013

We consider in a first time differents type of caracters set used in the crypting and Encrypting processes.

§= [!,",#,$,%,&,(,),*,+,-,]

Using this informations, we could get a first Terms list to treat called Ξ.

018kh.05a3c.8064.12vj.2gai.0605a.67500.0ba30.277a4.25376.2a5db.5813.36u7.146367.27706.1j68c

A list with length 16 is highlighting We will use the Set X = [a-z] $\cup$ [0-9]
With χ the length of the Terms list.
Here χ = 16, we could observ than length of key $\rho \mid \rho = \chi$.
Ξ_i will represent the respectives terms of the list.
We start the decrypting process by exctracting the key's Bases index from the c_n number suit contained in key. with c_i, $\forall$ i $\in$ [0,ρ], $c_i \leq 9$

We obtain : ξ = *21.16.10.34.28.14.10.13*

Successive Base Transpositions - Step 1

Highlighted ξ_j , Bases index are consistent with the Terms of the suit Ξ Thereby, with the Correspondance between ξ_0 and Ξ_0 , we obtain the following chained system resolution.

0.1 Ξ_0 = 018kh, ξ_0 = 21

By drawing up the 21 Base Table, we find :

$$\begin{cases} 0 = 0 \\ 1 = 1 \\ 8 = 8 \\ k = 20 \\ h = 17 \end{cases} . \tag{7}$$

Or by performing a Base transposition since the 21 Base Table, we obtain :

$$(018kh)_{21} = (0.21^4 + 1.21^3 + 8.21^2 + 20.21 + 17)_{10} = 13226 \tag{8}$$

0.2 Ξ_1 = 05a3c, ξ_1 = 16

By drawing up the 16 Base Table, we find :

$$\begin{cases} 0 = 0 \\ 5 = 5 \\ a = 10 \\ 3 = 3 \\ c = 12 \end{cases} . \tag{9}$$

Or by performing a Base transposition since the 16 Base Table, we obtain :

$$(05a3c)_{16} = (5.16^3 + 10.16^2 + 3.16 + 12)_{10} = 23100 \tag{10}$$

0.3 Ξ_2 = 8064, ξ_2 = 10

The specified base index $\xi_2 = 10$, so any conversion is superfluous.

0.4 Ξ_3 = 12vj, ξ_3 = 34

By drawing up the 34 Base Table, we find :

$$\begin{cases} 1 = 1 \\ 2 = 2 \\ v = 31 \\ j = 19 \end{cases} . \tag{11}$$

Or by performing a Base transposition since the 34 Base Table, we obtain :

$$(12vj)_{34} = (1.34^3 + 2.34^2 + 31.34 + 19)_{10} = 42689 \tag{12}$$

0.5 Ξ_4 = 2gai, ξ_4 = 28

By drawing up the 28 Base Table, we find :

$$\begin{cases} 2 = 2 \\ g = 16 \\ a = 10 \\ i = 18 \end{cases} . \tag{13}$$

Or by performing a Base transposition since the 28 Base Table, we obtain :

$$(2gai)_{28} = (2.28^3 + 16.28^2 + 10.28 + 18)_{10} = 56746 \tag{14}$$

0.6 Ξ_5 = 0605a, ξ_5 = 14

By drawing up the 14 Base Table, we find :

$$\begin{cases} 0 = 0 \\ 6 = 6 \\ 5 = 5 \\ a = 10 \end{cases} . \tag{15}$$

Or by performing a Base transposition since the 14 Base Table, we obtain :

$$(0605a)_{14} = (6.14^3 + 5.14 + 10)_{10} = 16544 \tag{16}$$

0.7 Ξ_6 = 67500, ξ_6 = 10

The specified base index $\xi_6 = 10$, so any conversion is superfluous.

0.8 Ξ_7 = 0ba30, ξ_7 = 13

By drawing up the 13 Base Table, we find :

$$\begin{cases} b = 11 \\ a = 10 \\ 3 = 3 \\ 0 = 0 \end{cases} . \tag{17}$$

Or by performing a Base transposition since the 13 Base Table, we obtain :

$$(0ba30)_{13} = (11.13^3 + 10.13^2 + 3.13 + 13)_{10} = 25886 \tag{18}$$

The Base transposition done, we could reverse the key to obtain the rest of the list.

Key build

We can use the following definition :
ρ is the length of the key ξ since Initialisation Section.
We go to compare the ρ length of ξ with χ the length of Ξ.We have χ=2.ρ
We will use the following terms :

- $\tilde{\xi}$: the mirror of ξ
- $\tilde{\xi}_{/n}$: the mirror of ξ bereft of ξ_n
- $\mathring{\xi}$: the rebuilded key
- $\frown$: the concatenation operator

To rebuild the missing half key, we go to reverse ξ with the following syntax

$$\begin{cases} \mathring{\xi} = \xi \frown \tilde{\xi} & if \quad \chi \quad mod \quad 2 = 0 \\ \mathring{\xi} = \xi \frown \tilde{\xi}_{/n} & if \quad \chi \quad mod \quad 2 = 1 \end{cases}. \tag{19}$$

Successive Base Transpositions - Step 2

Once the full key rebuilded from ξ, we could transpose again the rest of the list as step 1.

0.9 Ξ_8 = 277a4, ξ_8 = 13

By drawing up the 13 Base Table, we find :

$$\begin{cases} 2 = 2 \\ 4 = 4 \\ 7 = 7 \\ a = 10 \end{cases}. \tag{20}$$

Or by performing a Base transposition since the 13 Base Table, we obtain :

$$(277a4)_{13} = (2.134 + 7.13^3 + 7.13^2 + 10.13 + 4)_{10} = 73818 \tag{21}$$

0.10 Ξ_9 = 25376, ξ_9 = 10

The specified base index $\xi_9 = 10$, so any conversion is superfluous.

0.11 Ξ_{10} = 2a5db, ξ_{10} = 14

By drawing up the 14 Base Table, we find :

$$\begin{cases} 2 = 2 \\ 5 = 5 \\ a = 10 \\ b = 11 \\ d = 13 \end{cases} . \tag{22}$$

Or by performing a Base transposition since the 14 Base Table, we obtain :

$$(2a5db)_{14} = (2.144 + 10.14^3 + 5.14^2 + 13.14 + 11)_{10} = 105445 \tag{23}$$

0.12 Ξ_{11} = 5813, ξ_{11} = 28

By drawing up the 28 Base Table, we find :

$$\begin{cases} 1 = 1 \\ 3 = 3 \\ 5 = 5 \\ 8 = 8 \end{cases} . \tag{24}$$

Or by performing a Base transposition since the 28 Base Table, we obtain :

$$(5813)_{28} = (5.28^3 + 8.28^2 + 1.28 + 3)_{10} = 116063 \tag{25}$$

0.13 Ξ_{12} = 36u7, ξ_{12} = 34

By drawing up the 34 Base Table, we find :

$$\begin{cases} 3 = 3 \\ 6 = 6 \\ 7 = 7 \\ u = 30 \end{cases} . \tag{26}$$

Or by performing a Base transposition since the 34 Base Table, we obtain :

$$(36u7)_{34} = (3.34^3 + 6.34^2 + 30.34 + 7)_{10} = 125875 \tag{27}$$

0.14 Ξ_{13} = 146367, ξ_{13} = 10

The specified base index $\xi_{13} = 10$, so any conversion is superfluous.

0.15 Ξ_{14} = 27706, ξ_{14} = 16

Or by performing a Base transposition since the 16 Base Table, we obtain :

$$(27706)_{16} = (2.164 + 7.16^3 + 7.16^2 + 6)_{10} = 161542 \tag{28}$$

0.16 Ξ_{15} = 1j68c, ξ_{15} = 21

By drawing up the 21 Base Table, we find :

$$\begin{cases} 1 = 1 \\ 6 = 6 \\ 8 = 8 \\ c = 12 \\ j = 19 \end{cases} . \tag{29}$$

Or by performing a Base transposition since the 21 Base Table, we obtain :

$$(1j68c)_{21} = (1.214 + 19.21^3 + 6.21^2 + 8.21 + 12)_{10} = 373266 \tag{30}$$

We finnaly obtain the following numeric suit :
13226.23100.42689.56746.16544.67500.25886.73818.25376.105445.116063.125875.161542.373266

Chain Polynom Resolution

To continue the decrypting process, we know the suit increasing by recurrence. We can resolve the polynom using logic, we call it Ch.

$$Ch_n = y^2 + (y'^2 + (y''^2 + ... + y^{(n)2})).\text{y} + \text{c} = 0$$

The recursive injection of a polynome is resolvable uniquely using positive real roots.

With this definition, we will not keep cases with $\triangle \leq 0$

In the last part of the demonstration, we will use the Chain Polynoms resolution algorithm defined by :

- Solve $y^2 + b.y - \Xi_i = 0$
- $x = (root > 0) - b$
- $b = root$
- Add x to the solved list R.

We gonna initialize the procedure with :

- $y^2 = \Xi_0 \iff y = \sqrt{13226} = 115$
  $R_0 = 115$
- $y^2 - 115.y - 23100 = 0$
  $x = 220 - 115 = 105$
  $R_1 = 105$
- $y^2 - 220.y - 8064 = 0$
  $R_2 = 252 - 220 = 32$
- $y^2 - 252.y - 42688 = 0$
  $R_3 = 368 - 252 = 116$
- $y^2 - 368.y - 56745 = 0$
  $R_4 = 485 - 368 = 117$
- $y^2 - 485.y - 16544 = 0$
  $R_5 = 517 - 485 = 32$
- $y^2 - 517.y - 67500 = 0$
  $R_6 = 625 - 517 = 108$
- $y^2 - 625.y - 25896 = 0$
  $R_7 = 664 - 625 = 39$
- $y^2 - 664.y - 73817 = 0$
  $R_8 = 761 - 664 = 97$
- $y^2 - 761.y - 25376 = 0$
  $R_9 = 793 - 761 = 32$
- $y^2 - 793.y - 105444 = 0$
  $R_{10} = 909 - 793 = 116$
- $y^2 - 909.y - 116622 = 0$
  $R_{11} = 1023 - 909 = 114$
- $y^2 - 1023.y - 125874 = 0$
  $R_{12} = 1134 - 1023 = 111$
- $y^2 - 1134.y - 146367 = 0$
  $R_{13} = 1251 - 1134 = 117$

- $y^2 - 1251.y - 161542 = 0$
  $R_{14} = 1369 - 1251 = 118$
- $y^2 - 1369.y - 373266 = 0$
  $R_{15} = 1602 - 1369 = 118$

Conclusion

we can conclude using a simple ASCII table and get letters from the obtained numeric suit.
R={115,105,32,116,117,32,108,39,97,92,116,114,11,117,118,233}
$ASCII_R$={s,i, ,t,u, ,l,',a, ,t,r,o,u,v,é }

We can get the final decrypted string : "si tu l'a trouvé"