

TX 4820 - Réalisation de démonstrateurs pédagogiques d'algorithmes de cryptographie - Documentation utilisateur

[1. Lancement de l'application](#)

[1.1. Sur Windows](#)

[1.2. Sur Linux/Unix](#)

[1.3. Sur MacOS](#)

[1.4. Remarque](#)

[2. Menus](#)

[3. Algorithme RC4](#)

[3.1. Cryptage](#)

[3.2. Décryptage](#)

[4. Algorithme RSA](#)

[4.1 Cryptage](#)

[4.2. Décryptage](#)

[5. Exemple d'utilisation](#)

[5.1. RC4](#)

[5.1.1. Cryptage](#)

[5.1.2. Décryptage](#)

[5.2. RSA](#)

[5.2.1. Cryptage](#)

[5.2.2. Décryptage](#)

1. Lancement de l'application

1.1. Sur Windows

Extraire le contenu de l'archive "TX_portage_Windows.tar.gz" contenant toutes les dll nécessaires à l'exécution de l'application, et dans le dossier TX_portage_Windows, lancer l'exécutable "TX.exe"

1.2. Sur Linux/Unix

Extraire le contenu de l'archive "TX_portage_Linux.tar.gz" et lancer l'exécutable "TX" via la commande :

```
$ ./TX
```

1.3. Sur MacOS

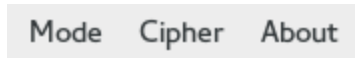
Extraire le contenu de l'archive "TX_portage_MacOS.tar.gz".

1.4. Remarque

Lors du lancement de l'application, celle-ci est réglée sur l'algorithme RC4 en mode cryptage.

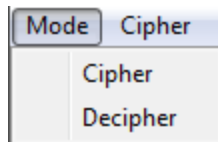
2. Menus

L'application se compose de 3 menus, tels qu'affichés sur la capture d'écran ci-dessous.



Barre de menu de l'application

Le menu *Mode* permet de définir le mode de l'application : Cryptage (*Cipher*) ou Décryptage (*Decipher*).



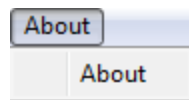
Menu "Mode" permettant de basculer entre le mode "Cipher" et le mode "Decipher"

Le menu *Cipher* permet de choisir quel algorithme utiliser : RC4 ou RSA.

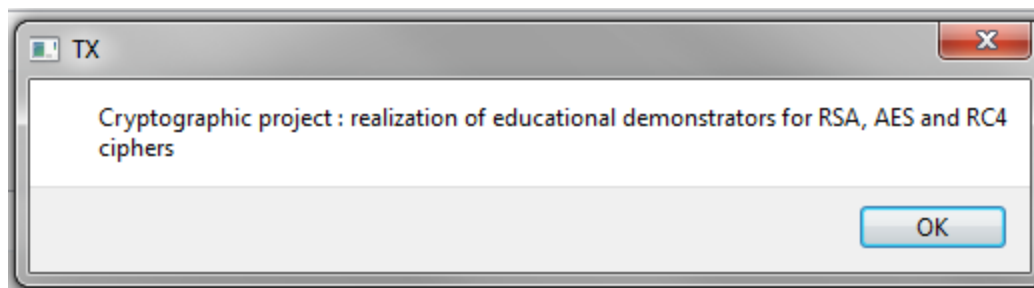


Menu "Cipher" permettant de basculer entre l'algorithme RC4 et l'algorithme RSA

Le menu *About* ouvre une fenêtre contextuelle donnant des informations sur l'application.



Menu "About"

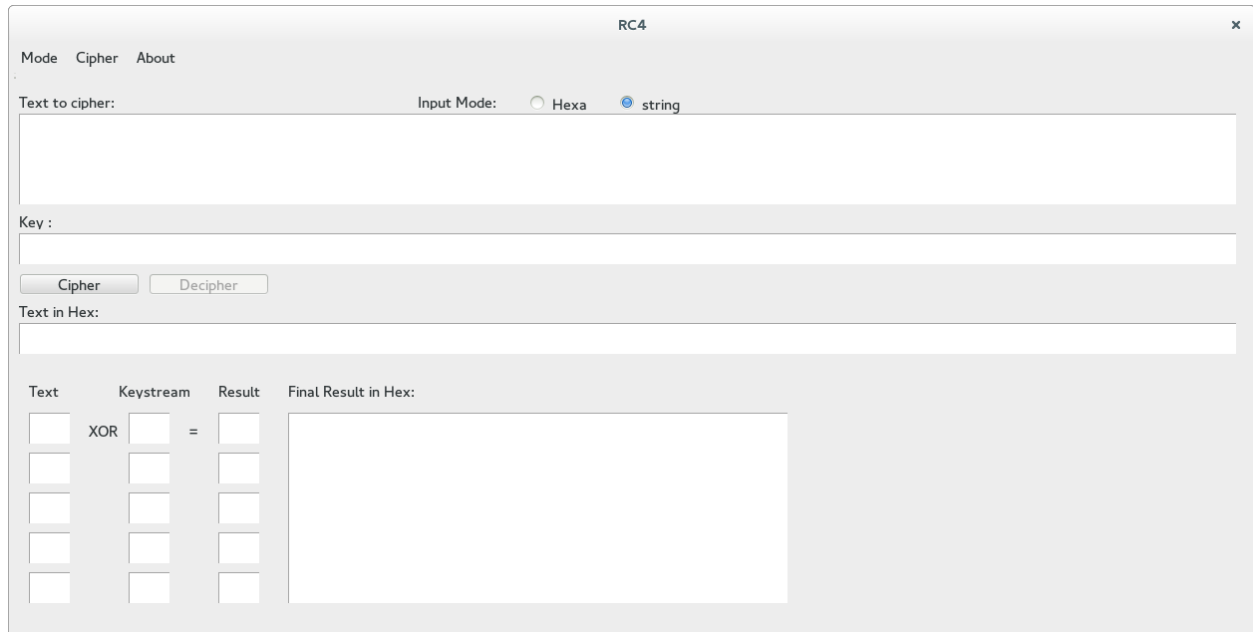


Fenêtre contextuelle donnant des informations sur l'application

3. Algorithme RC4

3.1. Cryptage

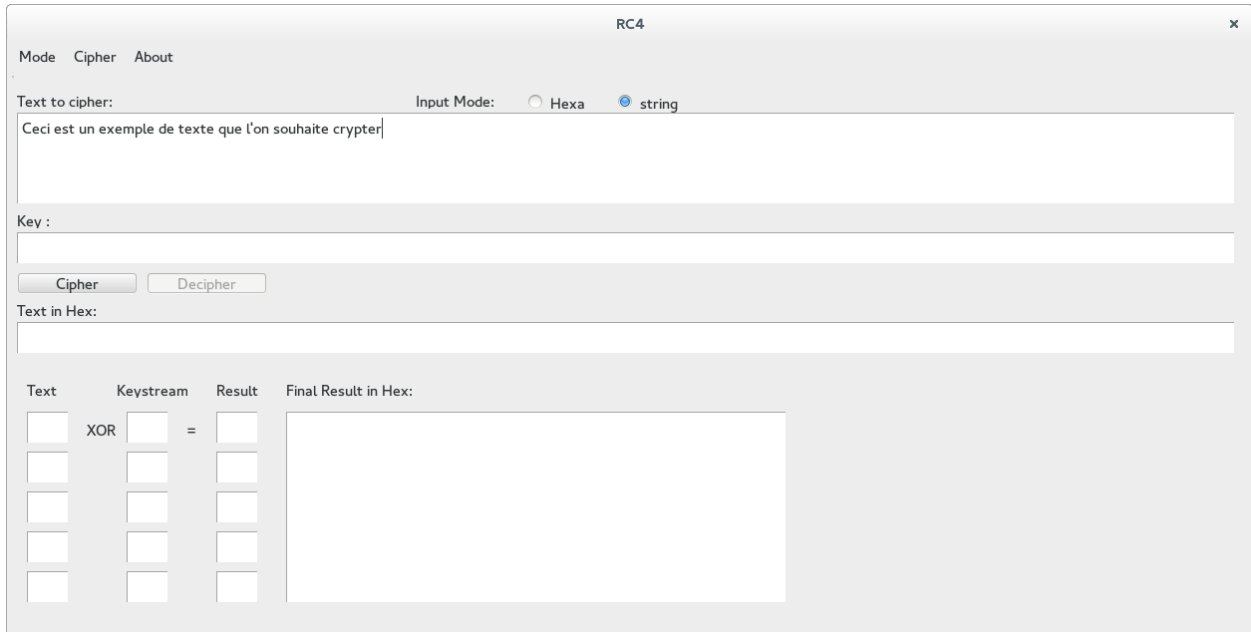
Le mode cryptage se décompose en 2 parties distinctes : la partie supérieure, contenant les zones de saisie de texte, et la zone inférieure contenant les zones d’affichage des résultats du cryptage.



The screenshot shows the RC4 application window with the title bar "RC4". The menu bar includes "Mode", "Cipher", and "About". The "Input Mode" section has two radio buttons: "Hexa" and "string", with "string" selected. Below this is a large text area labeled "Text to cipher:". A "Key:" label is followed by a text input field. Two buttons, "Cipher" and "Decipher", are positioned below the key field. Another text area labeled "Text in Hex:" is located below the buttons. The bottom section displays the XOR operation: "Text", "Keystream", "Result", and "Final Result in Hex:". It features five rows of input boxes for "Text" and "Keystream", followed by an equals sign and a box for "Result". To the right of these is a large text area for the "Final Result in Hex:".

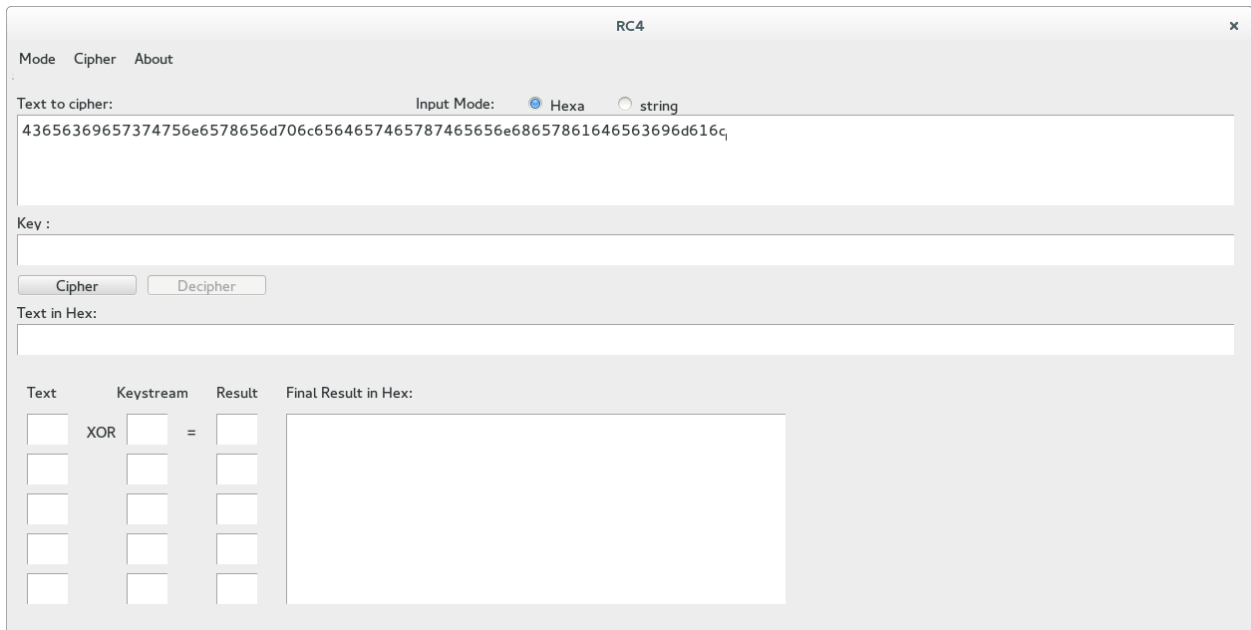
Ecran principal de l’algorithme RC4 en mode Cryptage (Cipher)

La zone “*Text to cipher*” permet de saisir le texte à crypter. Il est possible de choisir si l’on souhaite entrer un texte clair, ou un texte en hexadécimal. Ce choix se fait via les boutons radios *Hexa* et *String* dans l’encart *Input Mode*.



The screenshot shows the RC4 application window with the title bar 'RC4'. The menu bar contains 'Mode', 'Cipher', and 'About'. The 'Text to cipher:' field contains the text 'Ceci est un exemple de texte que l'on souhaite crypter'. The 'Input Mode:' section has two radio buttons: 'Hexa' (unselected) and 'string' (selected). Below this is a 'Key :' field. There are two buttons: 'Cipher' and 'Decipher'. The 'Text in Hex:' field is empty. At the bottom, there is a table with four columns: 'Text', 'Keystream', 'Result', and 'Final Result in Hex:'. The 'Text' column has five empty input boxes. The 'Keystream' column has the text 'XOR' and five empty input boxes. The 'Result' column has five empty input boxes. The 'Final Result in Hex:' column has a large empty text area.

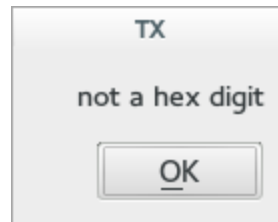
Utilisation de l'option "String" pour le texte à crypter



The screenshot shows the RC4 application window with the title bar 'RC4'. The menu bar contains 'Mode', 'Cipher', and 'About'. The 'Text to cipher:' field contains the hexadecimal string '43656369657374756e6578656d706c6564657465787465656e68657861646563696d616c'. The 'Input Mode:' section has two radio buttons: 'Hexa' (selected) and 'string' (unselected). Below this is a 'Key :' field. There are two buttons: 'Cipher' and 'Decipher'. The 'Text in Hex:' field is empty. At the bottom, there is a table with four columns: 'Text', 'Keystream', 'Result', and 'Final Result in Hex:'. The 'Text' column has five empty input boxes. The 'Keystream' column has the text 'XOR' and five empty input boxes. The 'Result' column has five empty input boxes. The 'Final Result in Hex:' column has a large empty text area.

Utilisation de l'option "Hexa" pour le texte à crypter

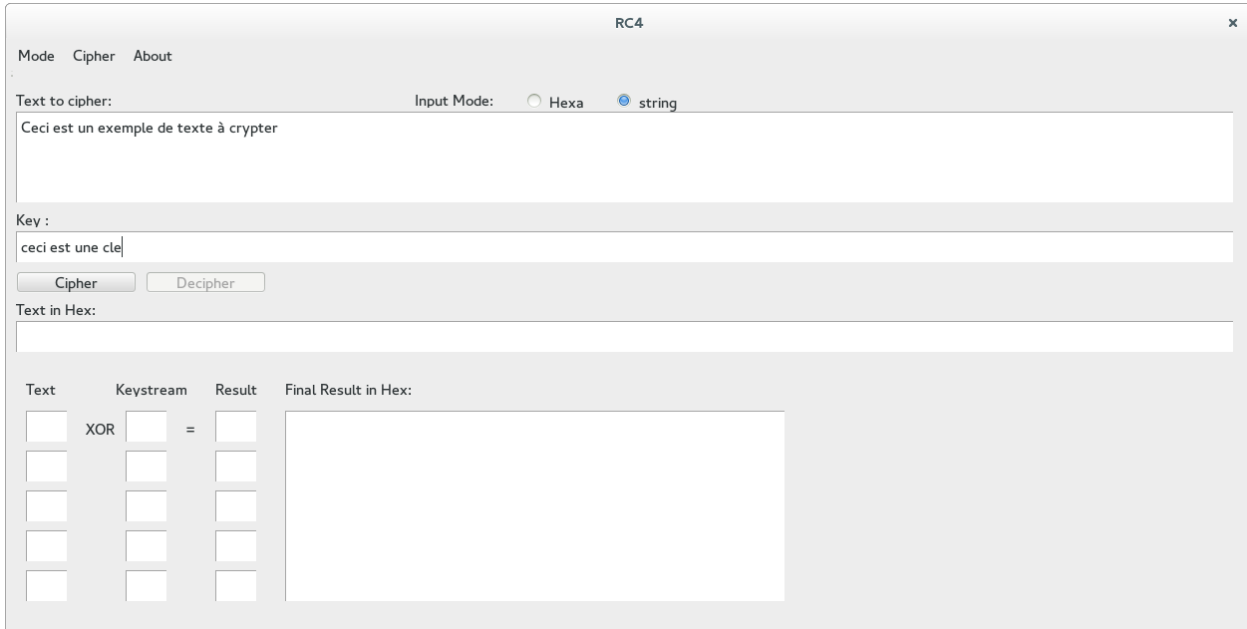
Si le texte renseigné n'est pas au format hexadécimal, un message d'erreur est affiché.



*Message d'erreur affiché lorsque le
texte entré n'est pas en hexadécimal*

Le texte en clair peut contenir des accents et des espaces, l'application se charge des les supprimer avant tout traitement. De même, les minuscules seront remplacées par des majuscules avant tout traitement.

Le champ *Key* permet d'entrer la clé de cyptage que l'on souhaite utiliser. Elle peut également être renseignée avec des espaces, qui seront retirés avant tout traitement.

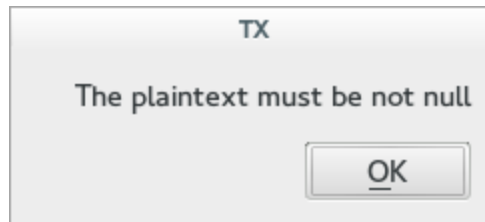


The screenshot shows the 'RC4' application window. At the top, there are tabs for 'Mode', 'Cipher', and 'About'. Below the tabs, there's a section for 'Text to cipher:' with an 'Input Mode:' selector set to 'string'. The text input field contains 'Ceci est un exemple de texte à crypter'. Below this is the 'Key :' section, where the text input field contains 'ceci est une cle'. There are 'Cipher' and 'Decipher' buttons. Below the key field is a 'Text in Hex:' section. At the bottom, there's a table with columns: 'Text', 'Keystream', 'Result', and 'Final Result in Hex:'. The 'Text' column has five empty input boxes. The 'Keystream' column has the label 'XOR'. The 'Result' column has an '=' sign and four empty input boxes. The 'Final Result in Hex:' column has a large empty text area.

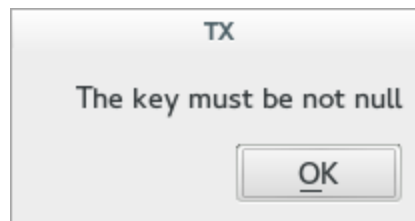
Renseignement du champ "Key"

Une fois les deux champs renseignés, le cryptage peut être lancé en cliquant sur le bouton *Cipher*.

NB : Si un des champs n'est pas complété (*Text to Cipher* ou *Key*), un message d'erreur va s'afficher à l'écran, indiquant que les deux champs doivent être remplis.

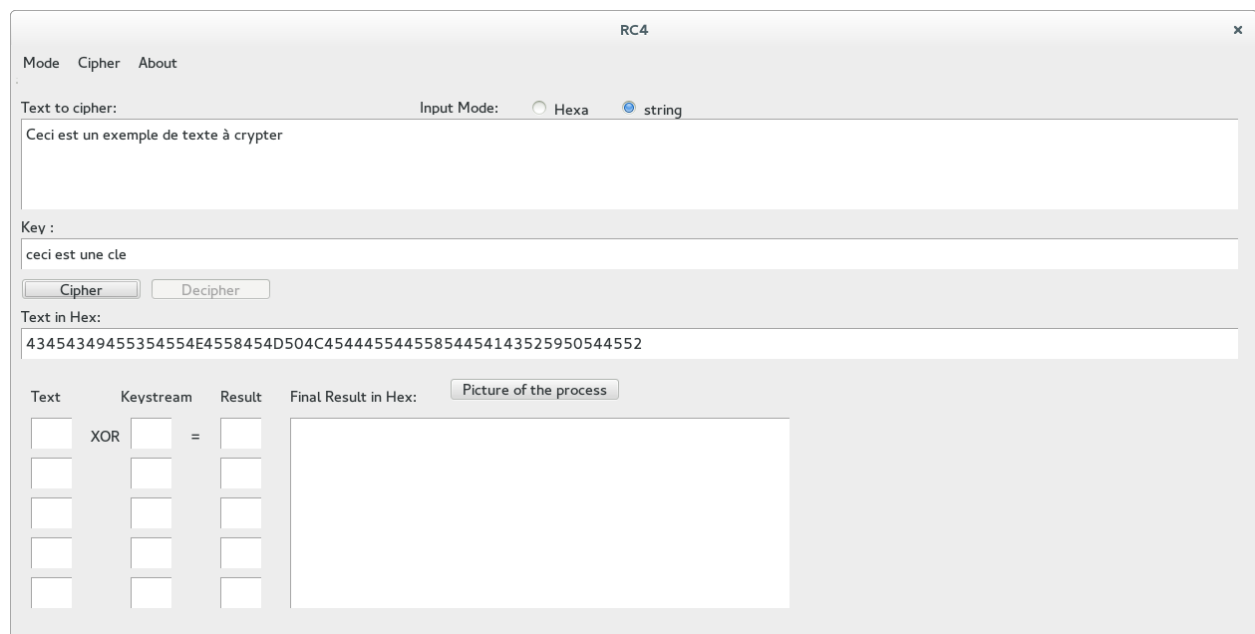


*Message d'erreur lorsque le champ
Text to cipher n'est pas renseigné*



*Message d'erreur lorsque la
clé n'est pas renseignée*

Si tous les champs sont renseignés, lorsque l'on clique sur le bouton *Cipher*, le texte donné est converti en hexadécimal et affiché, et un nouveau bouton fait son apparition : *Picture of the process*.



Affichage du texte à crypter en hexadécimal, et bouton Picture of the process

Lorsque l'on clique sur le bouton *Picture of the process*, une nouvelle fenêtre s'affiche permettant de décrire la génération du Keystream utilisé dans l'algorithme RC4.

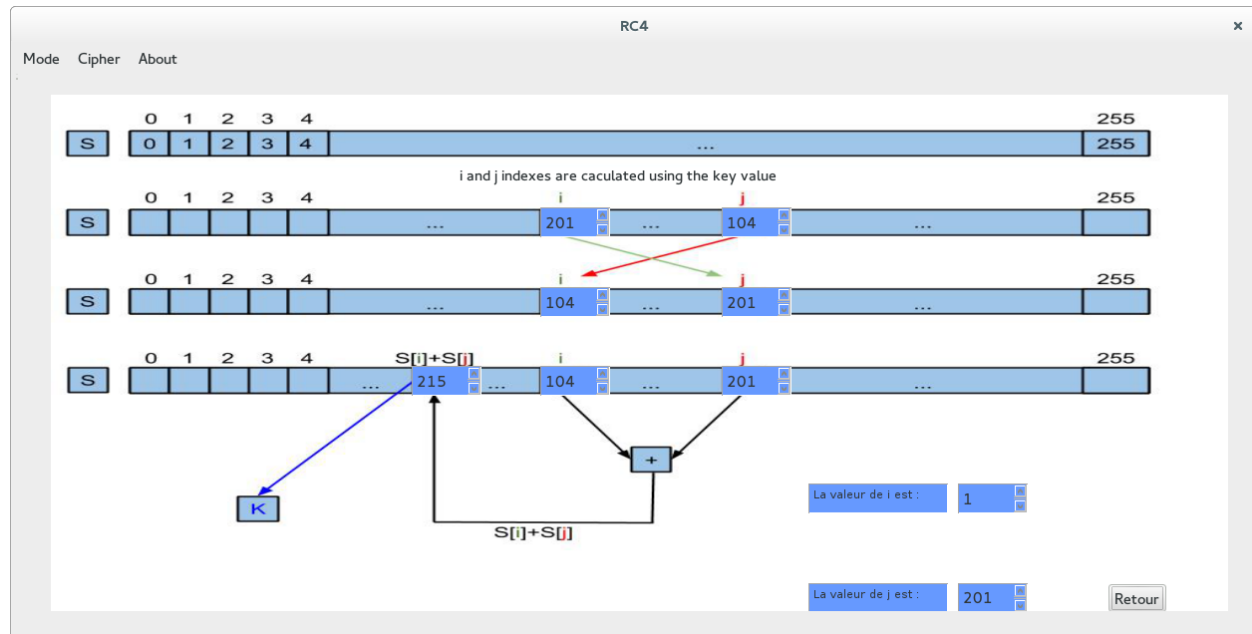


Schéma expliquant la génération du Keystream, affiché lors du clique sur le bouton "Picture of the process"

Il est possible de revenir à la fenêtre précédente en cliquant sur le bouton *Retour*.

Sur la fenêtre principale, un clic droit permet d'afficher le calcul entre le premier caractère du texte à crypter et du premier caractère du Keystream. En cliquant une nouvelle fois sur le clic droit, on affiche le 2ème calcul et son résultat dans l'encart *Final result in Hex*, et ainsi de suite jusqu'au remplissage des 5 premiers calculs. Chaque clic rajoute le nouveau caractère calculé au *Final result in Hex*. Un dernier clic droit permet d'afficher le résultat final, à savoir l'intégralité du texte crypté.

RC4

Mode Cipher About

Text to cipher: Input Mode: ☐ Hexa ☒ string

Ceci est un exemple de texte à crypter

Key :
ceci est une cle

Text in Hex:
43454349455354554E4558454D504C45444554455854454143525950544552

Text Keystream Result Final Result in Hex:

43	XOR	D7	=	94	94
<input type="text"/>		<input type="text"/>		<input type="text"/>	
<input type="text"/>		<input type="text"/>		<input type="text"/>	
<input type="text"/>		<input type="text"/>		<input type="text"/>	
<input type="text"/>		<input type="text"/>		<input type="text"/>	

Affichage après un clic droit

RC4

Mode Cipher About

Text to cipher: Input Mode: ☐ Hexa ☒ string

Ceci est un exemple de texte à crypter

Key :
ceci est une cle

Text in Hex:
43454349455354554E4558454D504C45444554455854454143525950544552

Text Keystream Result Final Result in Hex:

43		D7		94	9490
45	XOR	D5	=	90	
<input type="text"/>		<input type="text"/>		<input type="text"/>	
<input type="text"/>		<input type="text"/>		<input type="text"/>	
<input type="text"/>		<input type="text"/>		<input type="text"/>	

Affichage après un second clic droit

RC4 x

Mode Cipher About

Text to cipher: Input Mode: ☐ Hexa ☒ string

Ceci est un exemple de texte à crypter

Key :
ceci est une cle

Text in Hex:
43454349455354554E4558454D504C45444554455854454143525950544552

Text	Keystream	Result	Final Result in Hex:
43	D7	94	<input type="button" value="Picture of the process"/>
45	D5	90	
43 XOR 69	=	2A	

Affichage après un 3ème clic droit

RC4 x

Mode Cipher About

Text to cipher: Input Mode: ☐ Hexa ☒ string

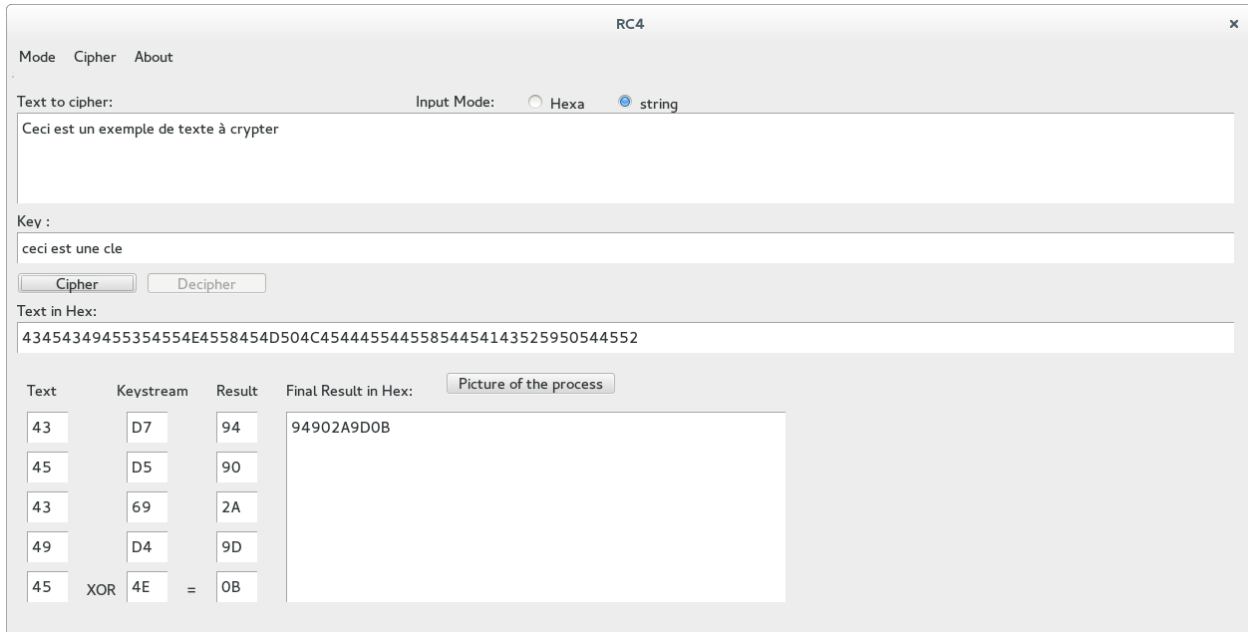
Ceci est un exemple de texte à crypter

Key :
ceci est une cle

Text in Hex:
43454349455354554E4558454D504C45444554455854454143525950544552

Text	Keystream	Result	Final Result in Hex:
43	D7	94	<input type="button" value="Picture of the process"/>
45	D5	90	
43	69	2A	
49 XOR D4	=	9D	

Affichage après un 4ème clic droit



Mode Cipher About

Text to cipher: Input Mode: ☐ Hexa ☒ string

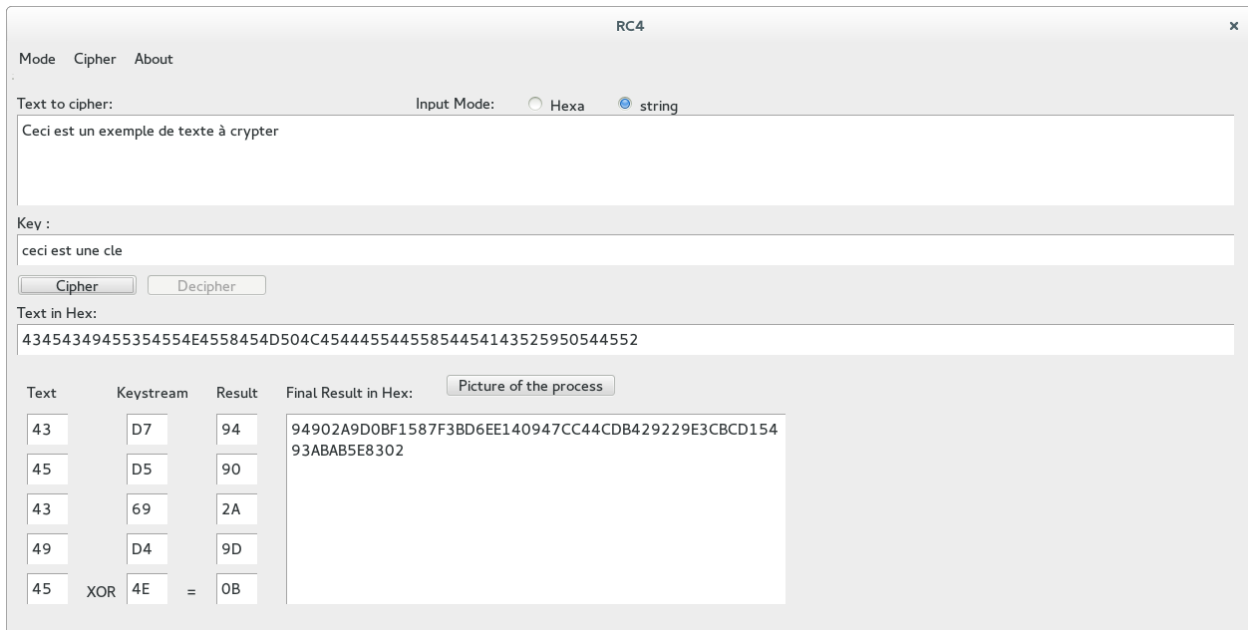
Ceci est un exemple de texte à crypter

Key :
ceci est une cle

Text in Hex:
43454349455354554E4558454D504C45444554455854454143525950544552

Text	Keystream	Result	Final Result in Hex:
43	D7	94	94902A9D0B
45	D5	90	
43	69	2A	
49	D4	9D	
45 XOR 4E =	0B		

Affichage après un 5ème clic droit



Mode Cipher About

Text to cipher: Input Mode: ☐ Hexa ☒ string

Ceci est un exemple de texte à crypter

Key :
ceci est une cle

Text in Hex:
43454349455354554E4558454D504C45444554455854454143525950544552

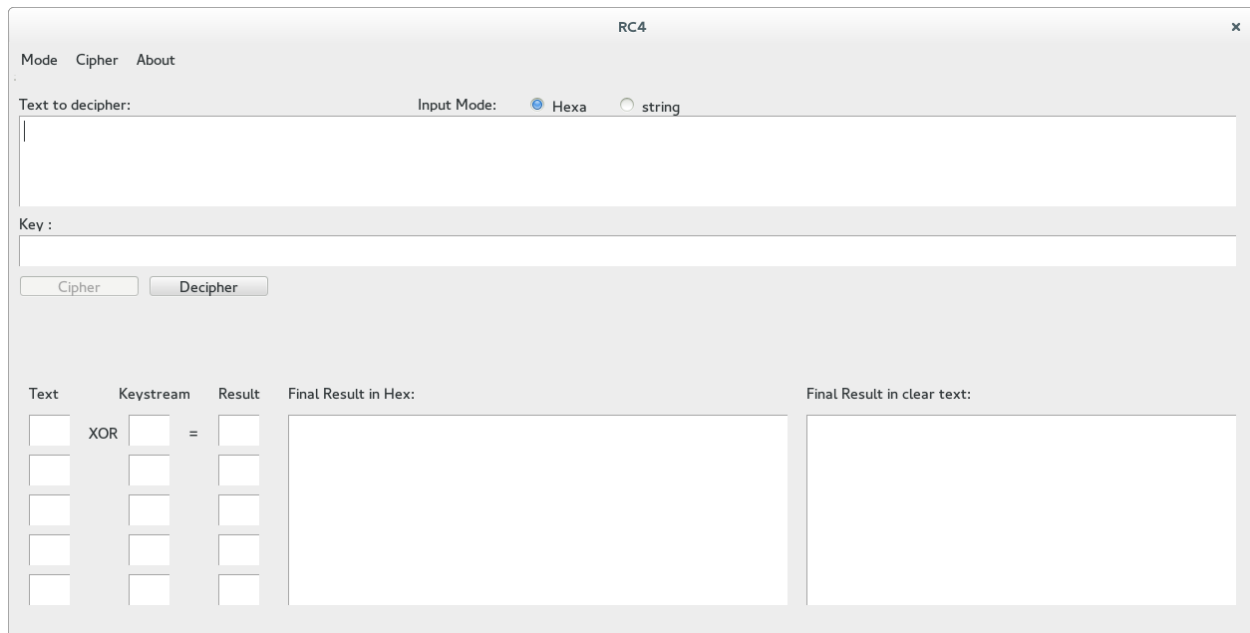
Text	Keystream	Result	Final Result in Hex:
43	D7	94	94902A9D0BF1587F3BD6EE140947CC44CDB429229E3CBCD15493ABAB5E8302
45	D5	90	
43	69	2A	
49	D4	9D	
45 XOR 4E =	0B		

Affichage du résultat final après un 6ème clic droit

3.2. Décryptage

Pour réaliser le décryptage, il est d'abord nécessaire de passer l'application en mode Décryptage, via l'option *Decipher* du menu *Mode*. Le bouton *Cipher* devient grisé, tandis que le bouton *Decipher* devient actionnable. De plus, une nouvelle zone *Final Result in clear text* permet

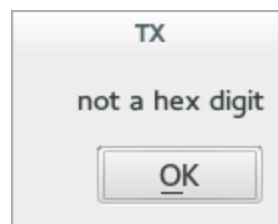
d'afficher le résultat du décryptage en texte clair, en plus de l'afficher en hexadécimal dans l'encart *Final Result in Hex*.



The screenshot shows the 'RC4' application window. At the top, there are tabs for 'Mode', 'Cipher', and 'About'. The 'Mode' tab is selected. Below the tabs, there is a 'Text to decipher:' label and a large text input field. To the right of the input field, there is an 'Input Mode:' section with two radio buttons: 'Hexa' (selected) and 'string'. Below the input field, there is a 'Key:' label and a smaller text input field. Below the key field, there are two buttons: 'Cipher' and 'Decipher'. The 'Decipher' button is highlighted. At the bottom of the window, there are five columns: 'Text', 'Keystream', 'Result', 'Final Result in Hex:', and 'Final Result in clear text:'. The 'Text' column has five input boxes, the 'Keystream' column has five input boxes, and the 'Result' column has five input boxes. Between the 'Keystream' and 'Result' columns, there is an 'XOR' label and an '=' sign. The 'Final Result in Hex:' and 'Final Result in clear text:' columns are empty.

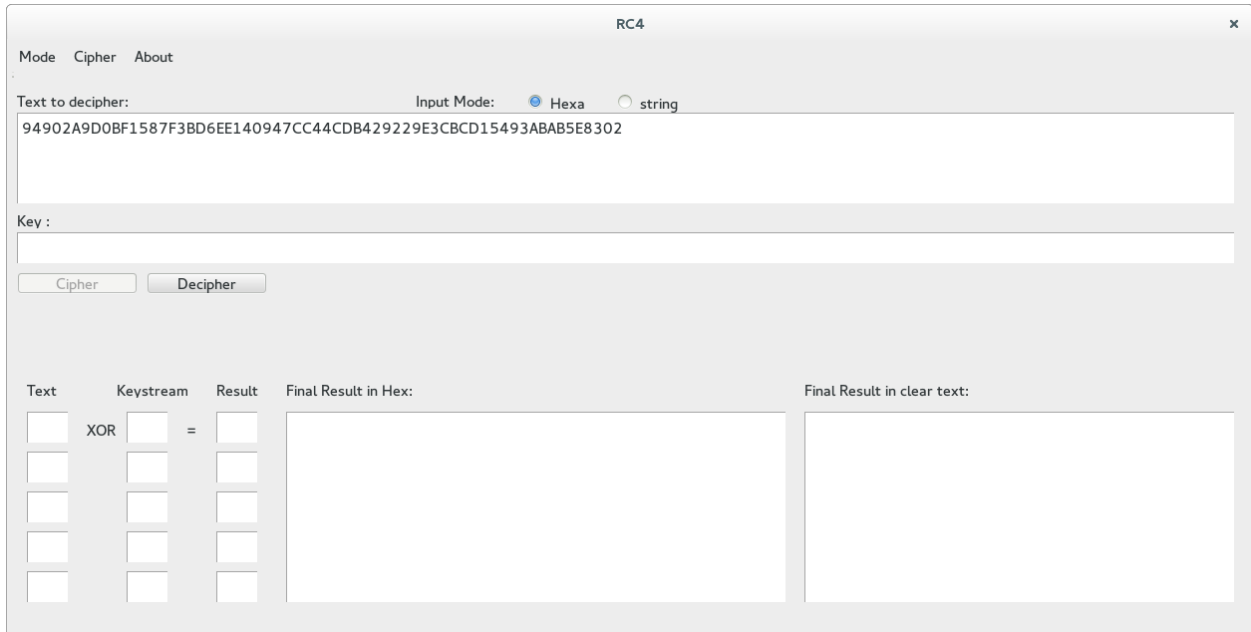
Ecran principal en mode Décryptage

Lorsque l'on choisit le mode Décryptage, le mode de saisie passe automatiquement en hexadécimal. Il n'est possible d'entrer un texte qu'en hexadécimal. Si le texte entré n'est pas en hexadécimal, un message d'erreur est affiché.



*Message d'erreur lorsque le texte
n'est pas en hexadécimal*

Une fois le mode de l'application réglé sur *Decipher*, il suffit d'entrer le texte crypté au format hexadécimal.



Mode Cipher About

Text to decipher: Input Mode: ☒ Hexa ☐ string

94902A9D0BF1587F3BD6EE140947CC44CDB429229E3CBCD15493ABAB5E8302

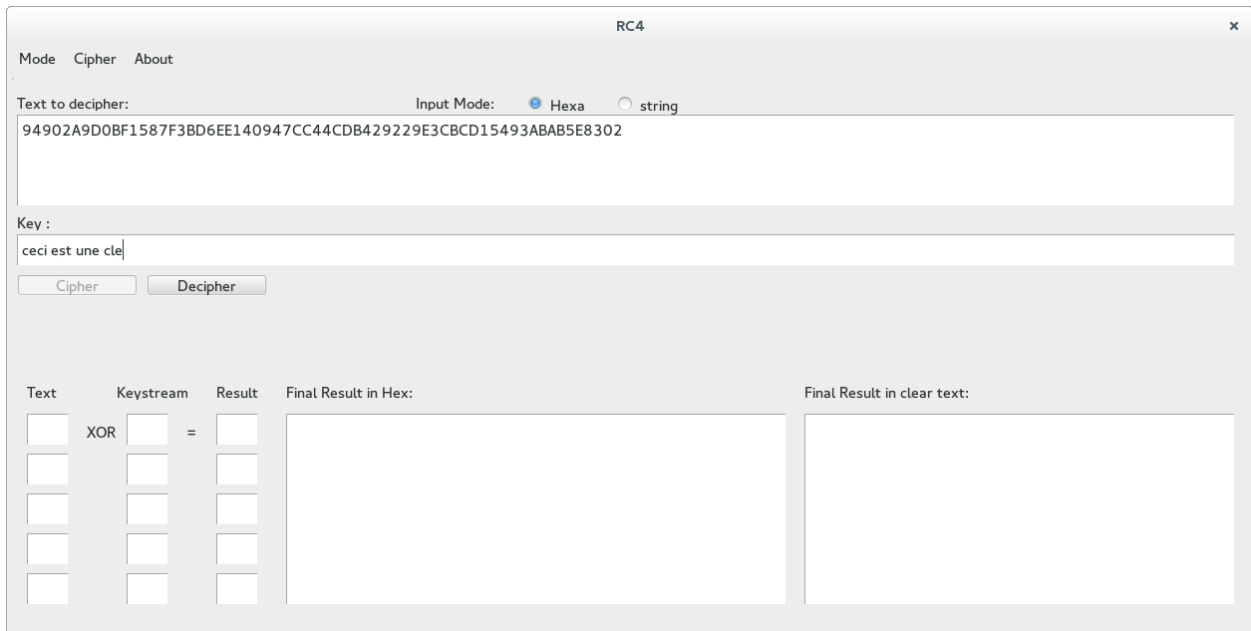
Key :

Cipher Decipher

Text	Keystream	Result	Final Result in Hex:	Final Result in clear text:
<input type="checkbox"/>	XOR <input type="checkbox"/>	= <input type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		

Affichage de l'application après avoir renseigné le texte crypté.

Il ne reste plus qu'à renseigner le champ Key afin de lancer le décryptage.



Mode Cipher About

Text to decipher: Input Mode: ☒ Hexa ☐ string

94902A9D0BF1587F3BD6EE140947CC44CDB429229E3CBCD15493ABAB5E8302

Key :
ceci est une cle

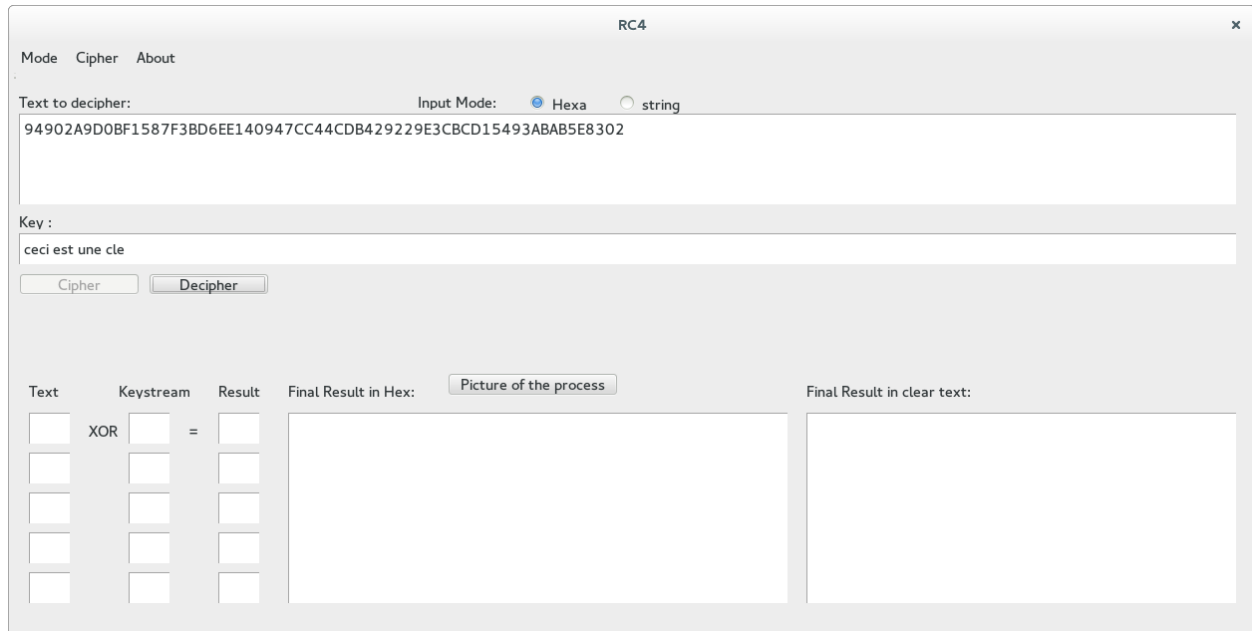
Cipher Decipher

Text	Keystream	Result	Final Result in Hex:	Final Result in clear text:
<input type="checkbox"/>	XOR <input type="checkbox"/>	= <input type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		

Affichage après que la clé a été renseigné

Si les champs ne sont pas renseignés, les mêmes messages d'erreurs que pour le cryptage sont affichés.

Lorsque le bouton *Decipher* est actionné, un nouveau bouton fait son apparition, le bouton *Picture of the process*. Comme pour le cryptage, il permet d'afficher la construction du Keystream.



The screenshot shows the 'RC4' application window with the 'Decipher' mode selected. The 'Text to decipher' field contains a long hexadecimal string. The 'Key' field contains the text 'ceci est une cle'. Below these fields are 'Cipher' and 'Decipher' buttons. At the bottom, there is a section for visualizing the keystream construction. It includes a table with columns 'Text', 'Keystream', and 'Result', followed by an equals sign and a 'Final Result in Hex' field. A 'Picture of the process' button is located above the 'Final Result in Hex' field. To the right of the 'Final Result in Hex' field is a 'Final Result in clear text' field. The table has five rows, each with input boxes for 'Text' and 'Keystream' and a 'Result' box. The first row is pre-filled with 'XOR' in the 'Text' box.

Text	Keystream	Result
XOR		

Affichage après clic sur le bouton “Decipher”

Comme pour le cryptage, il est possible, via 5 clics droits, d'afficher les 5 premiers calculs du décryptage. Dans les encarts *Final Result in Hex* et *Final Result in clear text*, les 5 premiers caractères s'affichent après chaque clic droit. Un dernier clic permet d'afficher le résultat final.

RC4

Mode Cipher About

Text to decipher: Input Mode: ☒ Hexa ☐ string

94902A9D0BF1587F3BD6EE140947CC44CDB429229E3CBCD15493ABAB5E8302

Key :
ceci est une cle

Cipher Decipher

Text	Keystream	Result	Final Result in Hex:	Picture of the process	Final Result in clear text:
94	XOR D7	= 43	43		C

Après le premier clic droit

RC4

Mode Cipher About

Text to decipher: Input Mode: ☒ Hexa ☐ string

94902A9D0BF1587F3BD6EE140947CC44CDB429229E3CBCD15493ABAB5E8302

Key :
ceci est une cle

Cipher Decipher

Text	Keystream	Result	Final Result in Hex:	Picture of the process	Final Result in clear text:
94	D7	43	4345		CE
90	XOR D5	= 45			

Après le second clic droit

RC4


Mode Cipher About

Text to decipher: Input Mode: ☒ Hexa ☐ string

94902A9D0BF1587F3BD6EE140947CC44CDB429229E3CBCD15493ABAB5E8302

Key :
ceci est une cle

Cipher Decipher

Text	Keystream	Result	Final Result in Hex:	Picture of the process	Final Result in clear text:
94	D7	43	434543		CEC
90	D5	45			
2A	XOR 69	= 43			

Après le 3ème clic droit

RC4


Mode Cipher About

Text to decipher: Input Mode: ☒ Hexa ☐ string

94902A9D0BF1587F3BD6EE140947CC44CDB429229E3CBCD15493ABAB5E8302

Key :
ceci est une cle

Cipher Decipher

Text	Keystream	Result	Final Result in Hex:	Picture of the process	Final Result in clear text:
94	D7	43	43454349		CECI
90	D5	45			
2A	69	43			
9D	XOR D4	= 4D			

Après le 4ème clic droit

RC4

Mode Cipher About

Text to decipher: Input Mode: ☒ Hexa ☐ string

94902A9D0BF1587F3BD6EE140947CC44CDB429229E3CB CD15493ABAB5E8302

Key :
ceci est une cle

Cipher Decipher

Text	Keystream	Result	Final Result in Hex:	Picture of the process	Final Result in clear text:
94	D7	43	4345434945		CECIE
90	D5	45			
2A	69	43			
9D	D4	4D			
0B	XOR 4E	= 45			

Après le 5ème clic droit

RC4

Mode Cipher About

Text to decipher: Input Mode: ☒ Hexa ☐ string

94902A9D0BF1587F3BD6EE140947CC44CDB429229E3CB CD15493ABAB5E8302

Key :
ceci est une cle

Cipher Decipher

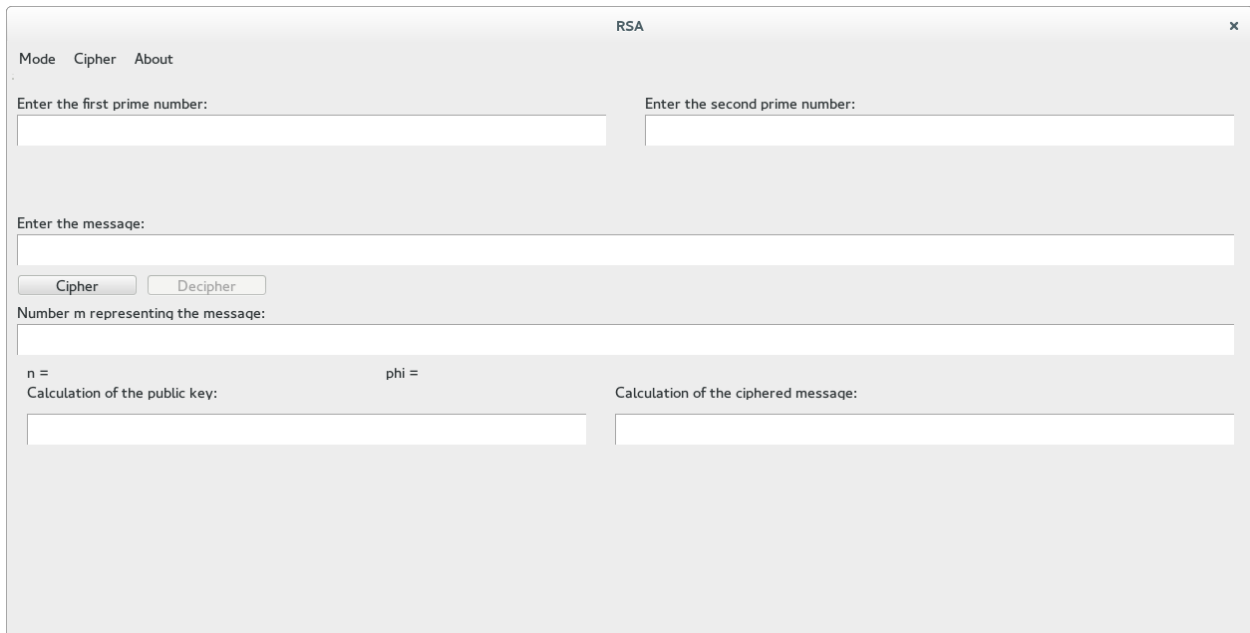
Text	Keystream	Result	Final Result in Hex:	Picture of the process	Final Result in clear text:
94	D7	43	43454349455354554E4558454D504C45444554455854454143525950544552		CECIESTUNEXEMPLEDETETEAECRYPTER
90	D5	45			
2A	69	43			
9D	D4	4D			
0B	XOR 4E	= 45			

Affichage du texte décrypter après le 6ème clic droit

4. Algorithme RSA

4.1 Cryptage

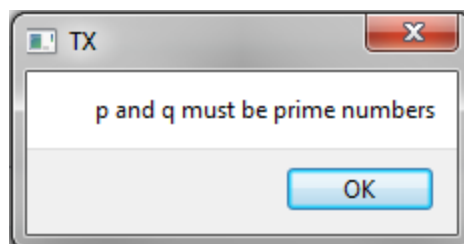
L'application RSA fonctionne de façon similaire à l'application RC4. Pour se placer en mode RSA, il suffit de cliquer sur le menu *Cipher* et de choisir l'option *RSA*. Une nouvelle fenêtre s'affiche alors.



Fenêtre principale pour l'algorithme RSA

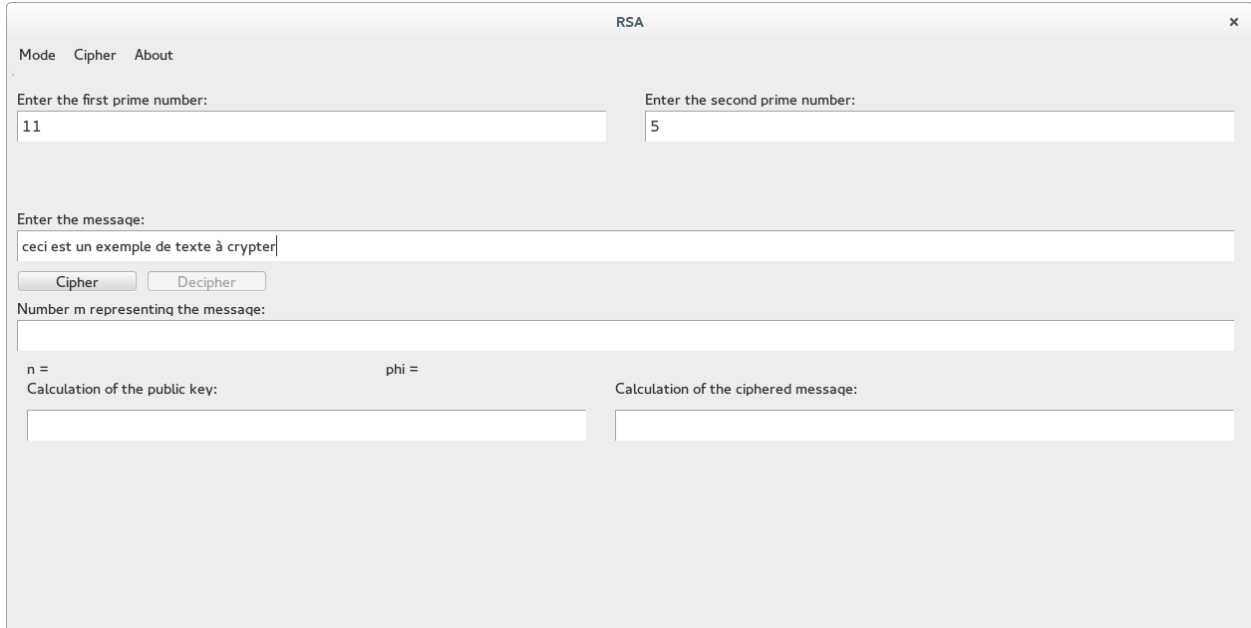
Sur cette nouvelle fenêtre, on peut retrouver, comme pour RC4, une division en 2 parties. La partie supérieure contenant les informations que l'utilisateur peut saisir, et la partie inférieure contenant l'affichage des résultats. Le bouton *Decipher* est, comme pour RC4, rendu inutilisable.

Les champs *Enter the first prime number* et *Enter the second prime number* correspondent aux champs de saisie des nombres p et q dans le cryptage RSA. Si l'un des deux nombres - ou les deux - ne sont pas premiers, un message d'erreur s'affiche.



Erreur affichée lorsque p et q ne sont pas premiers

Une fois p et q renseignés correctement, nous pouvons entrer le texte que nous souhaitons crypter. Une fois de plus, le texte peut contenir des espaces ainsi que des accents, l'application se chargera de les supprimer avant tout traitement.

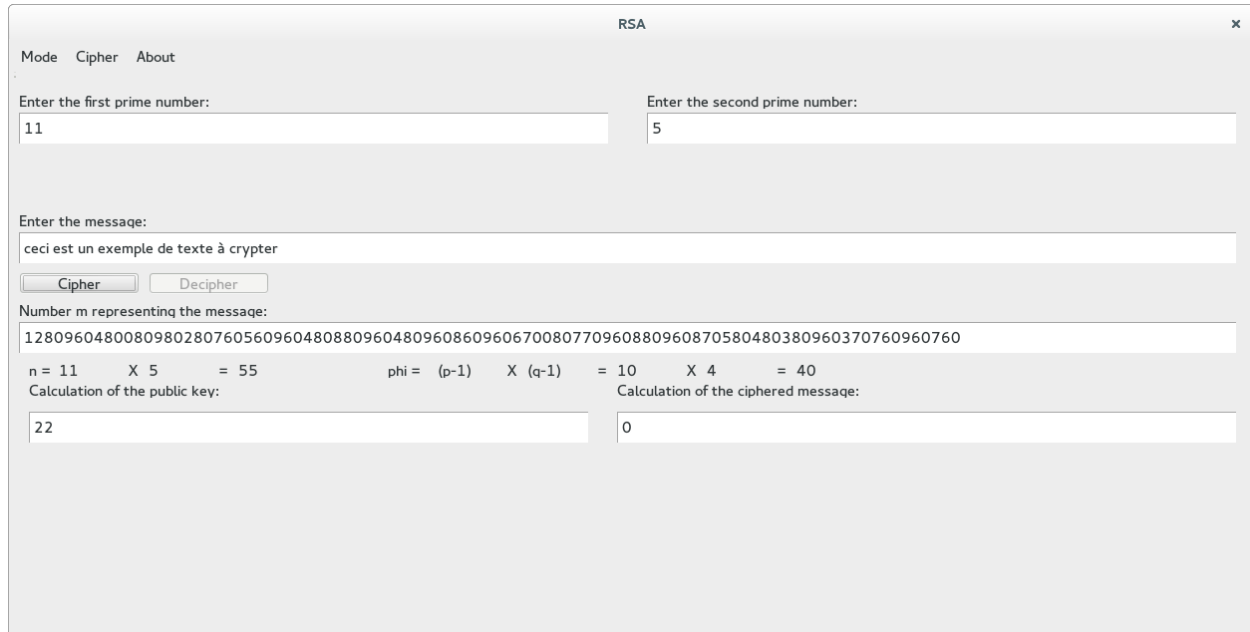


The screenshot shows a web application window titled "RSA". It has a menu bar with "Mode", "Cipher", and "About". The main interface is divided into several sections:

- Prime Numbers:** Two input fields. The first is labeled "Enter the first prime number:" and contains the value "11". The second is labeled "Enter the second prime number:" and contains the value "5".
- Message Entry:** A text area labeled "Enter the message:" containing the text "ceci est un exemple de texte à crypter". Below it are two buttons: "Cipher" and "Decipher".
- Message Representation:** A label "Number m representing the message:" followed by an empty input field.
- Public Key Calculation:** A label "n =" followed by the text "Calculation of the public key:" and an empty input field.
- Private Key Calculation:** A label "phi =" followed by the text "Calculation of the ciphered message:" and an empty input field.

*Affichage une fois les nombres p et q renseignés
et le message à crypter entré*

Ces opérations effectuées, un clic sur le bouton *Cipher* permet de réaliser le cryptage avec l'algorithme RSA.



The screenshot shows a window titled "RSA" with a menu bar containing "Mode", "Cipher", and "About". The interface is divided into several sections:

- Enter the first prime number:** A text box containing "11".
- Enter the second prime number:** A text box containing "5".
- Enter the message:** A text box containing "ceci est un exemple de texte à crypter".
- Buttons:** Two buttons labeled "Cipher" and "Decipher". The "Cipher" button is highlighted.
- Number m representing the message:** A text box containing a long decimal string: "1280960480080980280760560960480880960480960860960670080770960880960870580480380960370760960760".
- Calculation of the public key:** A section showing the calculation of n and $\phi(n)$. It displays:

$$n = 11 \times 5 = 55$$

$$\phi = (p-1) \times (q-1) = 10 \times 4 = 40$$
 Below this, a text box contains the value "22".
- Calculation of the ciphered message:** A text box containing the value "0".

Affichage après réalisation du cryptage RSA

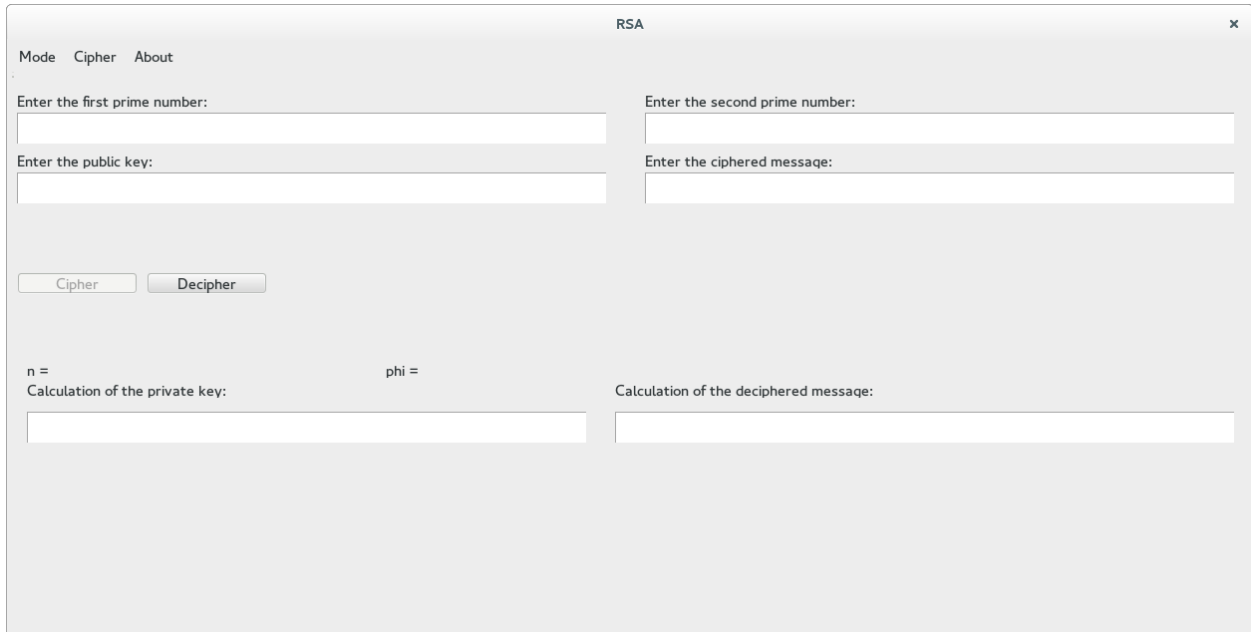
Number m representing the message est la représentation en un nombre entier du message clair, tel que définit dans la [RFC 3447](#).

Le calcul afin de trouver n et le totient $\phi(n)$ est également affiché.

Le champ *Calculation of the public key* représente le nombre e . Celui-ci est choisi aléatoirement, tout en respectant les conditions pour le bon fonctionnement de RSA. Enfin, le champ *Calculation of the ciphered message* représente l'entier caractéristique du message crypté.

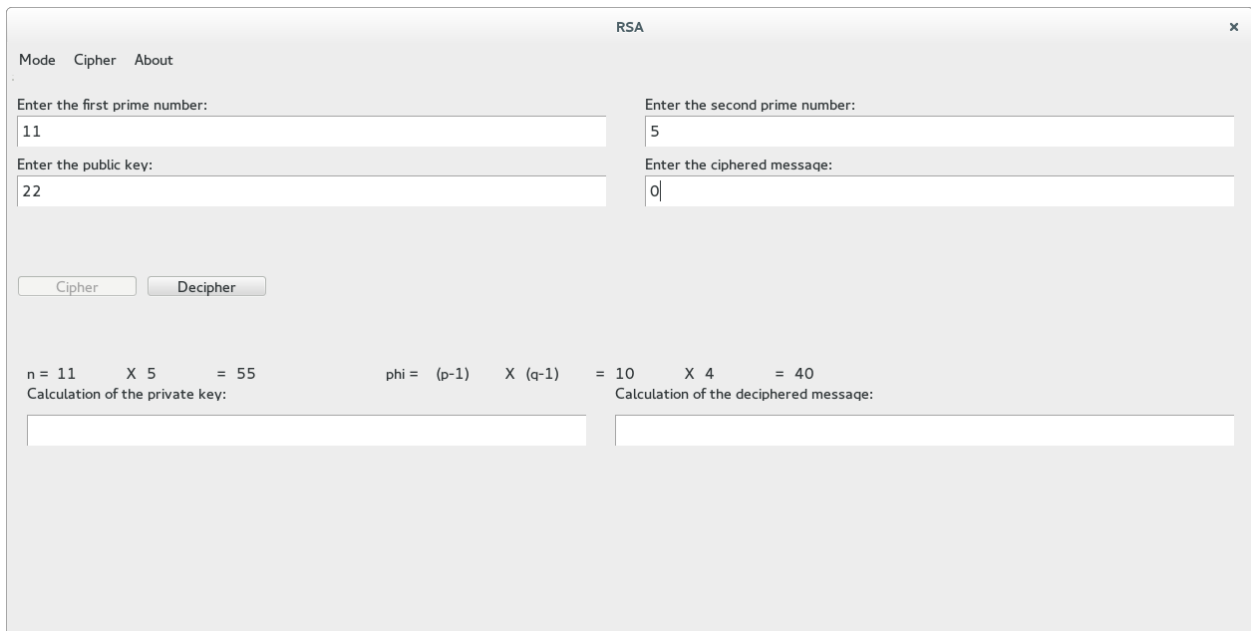
4.2. Décryptage

Pour passer en mode *Decipher*, on utilise l'option *Decipher* du menu *Mode*. L'interface pour le décryptage RSA est assez proche du cryptage RC4. Comme pour RC4, le bouton *Cipher* sera rendu inutilisable une fois passé en mode *Decipher*.



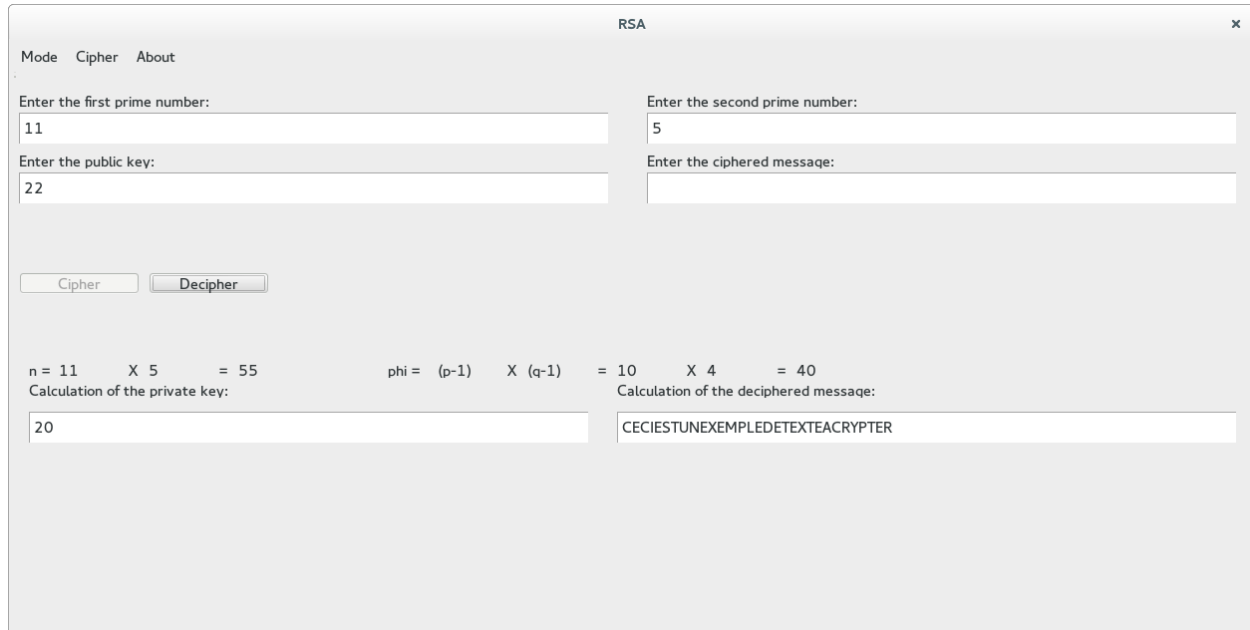
Ecran d'accueil pour le mode décryptage de RSA

Comme pour le cryptage, les champs permettant de renseigner les nombres p et q sont présents. Nous rajoutons les nombres e (champ *Enter the public key*), la clé publique générée lors du cryptage, et c , l'entier représentant l'entier crypté (*Enter the ciphred message*).



Affichage après renseignement des 4 nombres p , q , e et c

Enfin, en cliquant sur le bouton *Decipher*, les zones détaillant le calcul de n , du totient $\varphi(n)$, du calcul de la clé privée d (*Calculation of the private key*) et du message décrypté (*Calculation of the deciphered message*) seront remplies.



The screenshot shows a window titled "RSA" with a menu bar (Mode, Cipher, About). It contains two input fields for prime numbers (11 and 5), a public key input (22), and a ciphered message input. Below these are "Cipher" and "Decipher" buttons. The "Decipher" button is active. The results section shows the calculation of $n = 11 \times 5 = 55$ and $\phi = (p-1) \times (q-1) = 10 \times 4 = 40$. The private key calculation shows $d = 20$. The deciphered message is displayed as "CECIESTUNEXEMPLEDETETEXTTEACRYPTER".

Affichage après décryptage du message crypté obtenu dans la partie 4.1.

5. Exemple d'utilisation

5.1. RC4

5.1.1. Cryptage

Texte en clair : "Ceci est un exemple de texte que l'on peut crypter avec l'algorithme RC4"

Clé : "ma clef de chiffrement"

En cliquant droit une première fois, nous avons l'opération $43 \text{ XOR } E1 = A2$ qui s'affiche. 43 correspond au C du texte clair, E1 au premier caractère du Keystream généré, et A2 correspond donc au premier caractère du texte crypté. On recommence les clics droit ainsi de suite jusqu'à obtenir le résultat final :

"A271D1953AFFAC5B940275B5C5C6B09F375FF7684C051135DE000BB92579C0A5487130D72AC3843A3DC519589E163C73AC66D077D11BD3509F12D44F"

5.1.2. Décryptage

On reprend le texte crypté obtenu au point 5.1.2., ainsi que la clé.

Comme précédent, en utilisant les clics droit, on obtient pour la première opération $A2 \text{ XOR } E1 = 43$. A2 correspond au premier caractère du texte crypté, E1 au première caractère du Keystream généré, et 43 correspond bien au premier caractère du texte chiffré entré à l'étape précédente.

Dans l'encart *Final Result in Hex*, on voit bien 43 s'afficher au premier clic droit, puis 45 se rajouter derrière au second... Construisant ainsi le résultat du cryptage au fur et à mesure. Dans l'encart *Final Result in clear text*, on obtient un C pour la première opération, puis un E ensuite, ... La reconstruction du message en texte clair depuis l'héxadécimal est réalisée ici. Un 6ème et dernier clic nous permet d'obtenir le résultat en entier.

On obtient alors, après avoir cliqué sur le bouton *Decipher* le résultat :

"CECIESTUNEXEMPLEDETEXTEQUELONPEUTCRYPTERAVECLALGORITHMERC4"

5.2. RSA

5.2.1. Cryptage

p : 11

q : 7

(p et q sont bien des nombres premiers)

Texte en clair : "Ceci est un exemple de texte que l on peut crypter avec RSA"

En cliquant sur le bouton *Cipher*, on obtient le résultat suivant :

m :

156038028096077027048037028097017067056067076096068056028096048008098028076048
 058096008087097067096058018096048088096048096086096067008077096088096087058048
 0380960370760960760

e : 31(tiré aléatoirement, peut être différent)

c : 58 (dépend de e)

5.2.2. Décryptage

On reprend p et q tels qu'ils ont été définis ci-dessus.

On remplit les cases *Enter the public key* avec e calculé à l'étape précédente (31 dans notre cas), et dans *Enter the ciphered message* avec c calculé précédemment (58 dans notre cas).

On obtient comme texte décrypté :

"CECIESTUNEXEMPLEDETEXTEQUELONPEUTCRYPTERAVECRSA"