

ENIGMA v 1.7

Ce programme est un programme de cryptographie selon le principe de clé publique clé privé reprenant la méthode du « sac à dos ». Il permet de coder et de décoder rapidement un message de 64 caractères au maximum. Vous pouvez aussi entrer de nouvelle clé privé et publique. Il est compatible avec toutes les calculatrices de la TI82 à la TI84 SE.

COMPATIBILITE

Ce programme est fourni en une seule version compatible avec les calculatrices : TI82, TI83, TI83+, TI83 SE, TI84 et TI84SE

INSTALATION :

Il suffit de copier le programme ainsi que ces sous programme ZCTBL et ZDTBL dans la calculatrice.

UTILISATION :

Le programme utilise les deux sous programme ZCTBL et ZDTBL indispensable pour pouvoir coder ou décoder.

CODAGE

Pour coder un message, il suffit d'entrez directement votre texte sur la calculatrice **SANS appuyer sur [ALPHA]** car le programme utilise la fonction getkey. Le code de votre message est alors entré dans L₃ vous pouvez alors quitter le programme et envoyer le message.

```
CODAGE v 1.7
-----
ENTREZ VOTRE MES
SAGE
-----
CODE= L3
```

DECODAGE

Avant de décoder un message : faite en sorte que votre message codé soit au préalable entrez dans la liste L_3 ou une liste personnelle (mais pas L_1 , L_2 , L_4 , L_5 , L_6 car elles sont utilisées par le programme votre message sera alors effacé). Ne rentrez pas non plus directement votre message codé car, il n'y aurait plus la place pour l'affichage du message décodé.

Après avoir entré la liste correspondant au message codé appuyer sur entrer et attendez la fin du décodage

```
DECODAGE v 1.7      DECODAGE v 1.7
-----
CODE=L3
CODE=L3
ENTREZ V
```

```
DECODAGE v 1.7
-----
CODE=L3
Fait
ENTREZ VOTRE MES
SAGE
```

ENTREER UNE NOUVELLE CLE

Le programme est fourni avec une clé publique et privé par défaut, vous pouvez cependant entrez des nouvelles clés qui seront effacé automatiquement après utilisation.

Pour entrer la clé de codage allez dans options et sélectionnez 1: CLE CODAGE entrez votre nouvelle clé en n'oubliant pas de mettre les {, }.

Même méthode pour entrer la clé de décodage mais ici il faut aussi entrer les entiers p et q et leur coefficient de Bézout tel que $Pv+Qv=1$

```
OPTIONS      ENIGMA v 1.7
1:CLE CODAGE
2:CLE DECODAGE
3:Par défaut
4:A-PROPOS
5:Return
6:Fin
entrez La cLe
de CODAGE :
```

```
ENIGMA v 1.7      ENIGMA v 1.7
-----
entrez La cLe      entiers P,Q,v,u
de DECODAGE :      tel Que Pv+Qu=1
cLe=
P=
```

CONDITIONS :

Pour que les clés fonctionnent sans problème elles doivent impérativement respecter les conditions suivantes :

Soit : $\{a_1, a_2, a_3, a_4, a_5\}$ la clé de codage

$\{b_1, b_2, b_3, b_4, b_5\}$ la clé de décodage

p et q deux entiers premier entre eux et v, u leur coefficients de Bézout respectif avec pour le décodage. (Attention v est le coefficient de p et u le coefficient de q)

Il faut alors que : $p*v+q*v=1$

$$p > \sum b_i$$

$$a_i \equiv b_1 * q \pmod{p}$$

A-PROPOS

Ce programme est **libre de droit**. Vous pouvez donc gratuitement et légalement le copier, le modifier, et le distribuer. N'hésitez pas à améliorer ce programme.

Fait par : PUJOL
Alexandre

Version : 1.7

Date de création : 10/06/2009

```
+---ENIGMA---+
| Par PUJOL  |
| ALEXANDRE  |
| 10/06/09   |
| 2641 0     |
+---version 1.7---+
```

Note sur la version 1.7 :

Il s'agit de la 1^{ère} version mise sur internet.

Espace libre nécessaire sur la calculatrice :

ENIGMA : 1377 Octets
ZCTBL : 880 Octets
ZDTBL : 384 Octets
TOTAL : 2641 Octets

MES AUTRES PROGRAMMES :

PROMGRAMME	DESCRIPTION	Version	COMPATIBLITE
COURS	Résumé de TOUT le cours de TS	4.0	TI 82 et TI83+
CQFD	Une bonne partie (mais pas toute) des démonstrations de cours faite en TS	1.5	TI 82 et plus
Limite	Calcule la limite d'une fonction en $+\infty$, $-\infty$, L^+ et L^-	3.0	TI 82 et TI83+
Degree 2	Pas nouveaux ce programme sauf que lui c'est moi qui les fait !	4.0	TI 82 et TI83+
Système	Utilise les fonctions matricielles de la calculette pour résoudre un système d'équation à 2 inconnues	4.0	TI 82 et TI83+
Spe Math	Principaux programme utilisé en spécialité Math plus une bonne partie du cours	4.0	TI 82 et TI83+

Ils sont tous disponibles sur TI BANK