

ENIGMA v 2.0

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. Vous pouvez aussi entrer de nouvelle clé privé et publique. Il fonctionne entièrement avec l'écran graphique de la calculatrice pour pouvoir coder le maximum de texte possible.

COMPATIBILITE

Ce programme n'est pas compatible avec les calculatrices TI82 et TI83 simple. Il a été conçu pour tourner sur TI83+, TI83+ SE, TI84. Si vous avez une de ces calculatrices : téléchargez la version 1.7 disponible sur TI Bank.

INSTALATION :

Il suffit de copier le programme ainsi que ces sous programmes ZCODE et ZDCODE dans la calculatrice.

UTILISATION :

Lancer le programme, utilisée la touche [y=] ou [Windows] pour quitter. Appuyer directement sur les touches 1, 2, 3, 4, 5 pour faire afficher les sous menus. Les touches [Graph] et [Trace] permettent d'afficher l'à-propos.

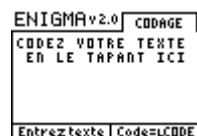
Le programme utilise les deux sous programme ZCODE et ZDCODE indispensable pour pouvoir coder ou décoder.



```
ENIGMA v2.0  MENU
1: CODAGE
2: DECODAGE
3: CLE DE CODAGE
4: CLE DE DECODAGE
5: CLE PAR DEFALT
Quitter | TI83+ | A-Propos
```

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 la liste LCODE vous pouvez alors quitter le programme et envoyer le message.

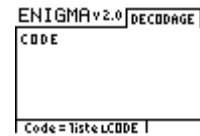


```
ENIGMA v2.0  CODAGE
CODEZ VOTRE TEXTE
EN LE TAPANT ICI
Entrez votre texte | Code=LCODE
```

DECODAGE

Avant de décoder un message : faite en sorte que votre message codé soit au préalable entrez dans la liste `L_CODE`

Le programme considérera automatiquement que le message à décoder est stocké dans `L_CODE`, il ne vous proposera donc pas d'entrer la liste codé à la main ou le nom d'une autres liste



Attendez le temps que le programme décode le message. Le message décodé s'affiche alors sur l'écran graphique de la calculatrice



Attention le décodage demande beaucoup de mémoire a la calculatrice (la liste `L_CODE` peut dépasser les 1000 Octets...) Pensez à archiver les vos autres programmes pour ne pas avoir une erreur de mémoire.

ENTRER UNE NOUVELLE CLE

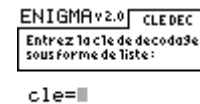
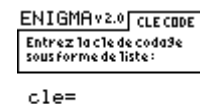
Le programme est fourni avec une clé publique et privé par défaut.

Ces clés sont :

{ 1837, 945, 3567, 1095, 2398 } Clé de codage

{ 13, 45, 183, 315, 802 } Clé de décodage

Ainsi que les entiers $v=-311$ et $p=1380$



Vous pouvez cependant entrez des nouvelles clés qui seront effacé automatiquement après utilisation.

Pour entrer la clé de codage allez dans options et sélectionnez 3: CLE DE 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 $pv+qv=1$



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 : $p*v+q*u=1$

$p > \sum b_i$

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

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 : 2.0



Date de création : 29/05/2010

Note sur la version 2.0 :

2^{ème} versions mise sur internet

Amélioration des algorithmes de codage et de décodage : gain de vitesse et de poids

Interface graphique entièrement repensée

Peut coder et décoder un message 2 fois plus long que la version 1.7

Espace libre nécessaire sur la calculatrice :

ENIGMA : 1854 Octets

ZCODE : 880 Octets

ZDCODE : 385 Octets

TOTAL : 3119 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/ 4.0	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/ 5.0	TI 82 et TI83+
Enigma	Programme de cryptographie suivant le système de clé publique et de clé privé	1.7	TI83+

Ils sont tous disponibles sur TI BANK