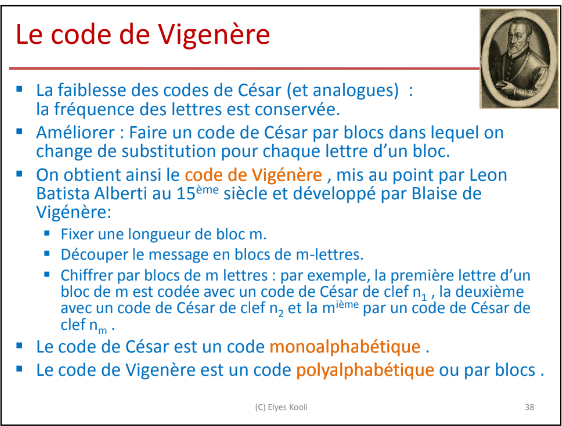
Projet de cryptographie

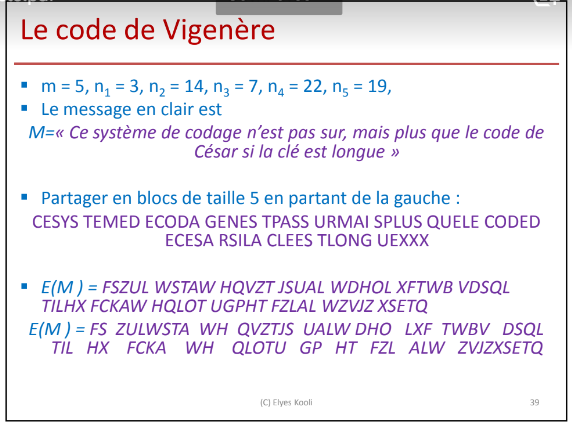
Réaliser par le binômes : -Ahmed Belkhiria

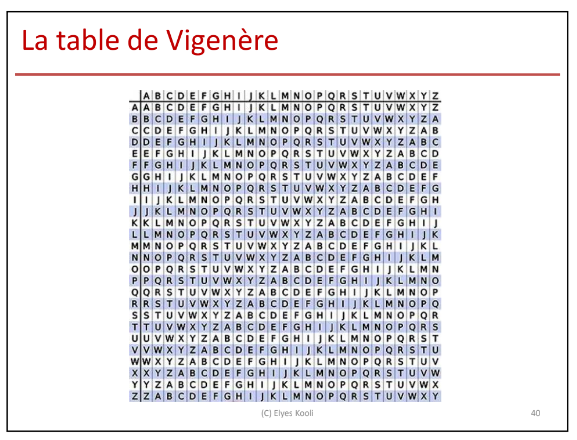
-Khalil Rached

But : implémentation de l algorithme de vigenere .

L’ énoncer de l algorithme :







System requirement : il faut avoir node js pour tester l algorithme implémenter . !!

Lancement de projet :

1. Au début écrire votre message dans message.txt ;

Ouvrir le terminal dans le dossier crypto\_projet ;



1. Pour crypter le message lancer la command :

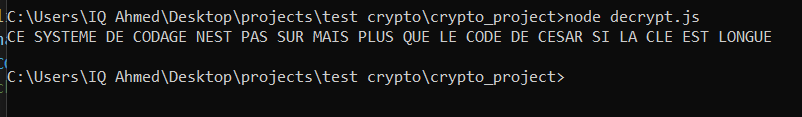
Node encrypt.js .



Ce message sera enregistrer dans crypted\_message.txt .

1. Pour décrypter le message lancer la command :

Node decrypt.js



Ce message sera enregistrer dans decrypted\_message.txt .

Les fichier .env contient les clefs utiliser lors de cryptage

Enregistrer dans un fichier sécurisé pour qu’ ont peut décrypter le message .

Remarques :

* Pour que on teste l’exemple de cours avec les clefs

clefs = [3,14,7,22,19];

il faut decommenter (annuler le commentaire effacer’//’)de la ligne 39 dans encrypt.js



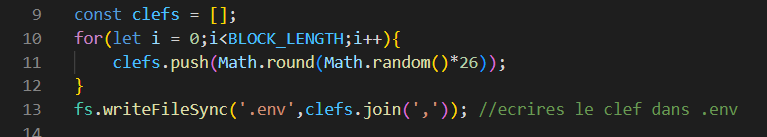
et

la ligne 17 dans decrypt.js



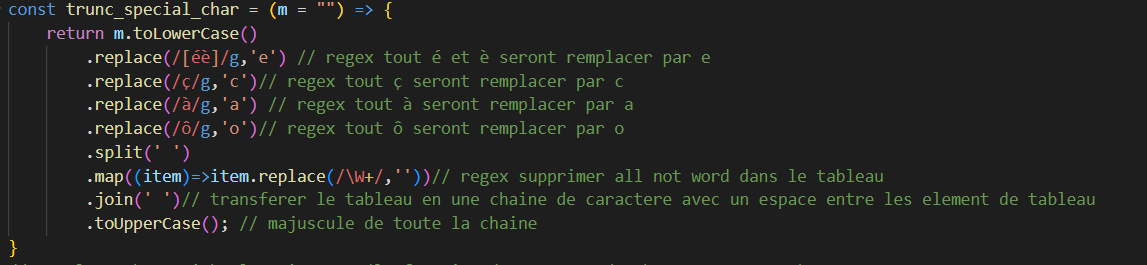
On peut aussi tester avec des clef prédéfini l’essentiel de saisir ces les mêmes clef dans encrypt.js et decrypt.js

Sinon on a implémenter un mécanisme de génération de clefs comme suit :



Ce mécanisme génère des clef aléatoirement(math.random) selon le longueur de bloc et l enregistre dans .env

* utilisation de regex : regular expression méthode pour chercher et remplacer dans une chaine de caractère facilement.



Exemple de utilisation : transférer notre message m en minuscule chercher les spécial caractères et les remplacer ou supprimer .

/\W +/ : représente les caractères notWord qui ne sont pas dans [a-z] [A-Z] et le remplace par ‘’ (supprimer) .

* Utiliser les fonction JS prédéfini pour manipuler les chaines et les tableau :
* Split()

Const Z= y.Split(‘x’) : découper la chaine de caractère selon x et mettre chaque élément dans un tableau

Exemple : y = ‘ aaa bb rr z’ x=espace ‘ ‘

Alors z= [aaa,bb,rr,z]

-join() joindre les element d un tableau dans une chaine

\*O=Z.join(‘x‘) \*z= [aaa,bb,rr,z] \* x=espace ‘ ‘

O=’aaa bb rr z’

* M.Slice(x,y) copier l intervalle[x,y] du caractere du M .

Const a= O.slice(2,5) \*O=‘ aaa bb rr z’

a = ‘a b’

* Replace(x,y) remplacer x par y

a= b.replace(‘x’,’y’) \*b= ‘aazretsxxxpxoxl’

alors a = ‘aazretsyyypyoyl’

* On choisi java script comme language de programmation car nous sommes des devellopeur js (backend :nodejs , frontend :reactjs)