Qu’est-ce que la cryptographie ? D'où vient-elle ?

La cryptographie c’est une technique d’écriture ou le message et chiffré, c’est à dire qu’il est écrit à l’aide de codes secrets ou de clefs de chiffrements.

La première trace de cryptographie connue date du XVI e siècle avant J-C. Il s’agirait d’une recette secrète de poterie écrite sur une tablette d’argile retrouvée en Irak

La cryptographie est déjà présente dans l'Egypte antique. Certaine scène représentée en hiéroglyphe semble contenir d’autre hiéroglyphes à l’intérieur de ceux-ci.

Il utilisé un système nommé acrophonie : c’est un système [linguistique](https://fr.wikipedia.org/wiki/Linguistique) qui consiste à nommer une [lettre](https://fr.wikipedia.org/wiki/Lettre_(alphabet)) alphabétique d'après un objet ou un animal dont le nom commence par la même lettre.

Ex : Bravo, Oscar, November , Juilet, Oscar, Uniform, Romeo = BONJOUR

On retrouve encore ce système encore aujourd’hui dans la communication par talkie-walkie ainsi que l’aéronautique.

Le code César est un célèbre système de cryptographie qui consiste à décaler l’alphabet de x lettre (x étant la clef du code). La force de ce code est que contrairement à l’acrophonie ce code possède 26 clefs différentes dans le cas de l'alp

habet latin.

Ex : avec une clef 4 hello= h->l ; e->i ; l->p ; l->p ; o->s = lipps

Essayer avec celui-là : la clef est 2 :

Mb OTJ D’ftu uspq cjfo

Pendant la seconde guerre mondiale les Allemands utilise une machine afin d’encoder et de décoder des messages. On l’appelle la machine Enigma. Enigma chiffre les informations en faisant passer un courant électrique à travers une série de composants. Ce courant est transmis en pressant la touche d'une lettre sur le [clavier](https://fr.wikipedia.org/wiki/Clavier_informatique) ; il traverse un réseau complexe de fils puis allume une lampe qui indique la lettre chiffrée. Le premier composant du réseau est une série de roues adjacentes, appelées « rotors », qui contiennent les fils électriques utilisés pour chiffrer le message. Les rotors tournent, modifiant la configuration complexe du réseau chaque fois qu'une lettre est tapée. Enigma utilise habituellement une autre roue, appelée « réflecteur », et un composant appelé « tableau de connexion », ce qui permet de rendre plus complexe encore le processus de chiffrement. **Enigma** est une machine électromécanique portative servant au déchiffrement de l'information.