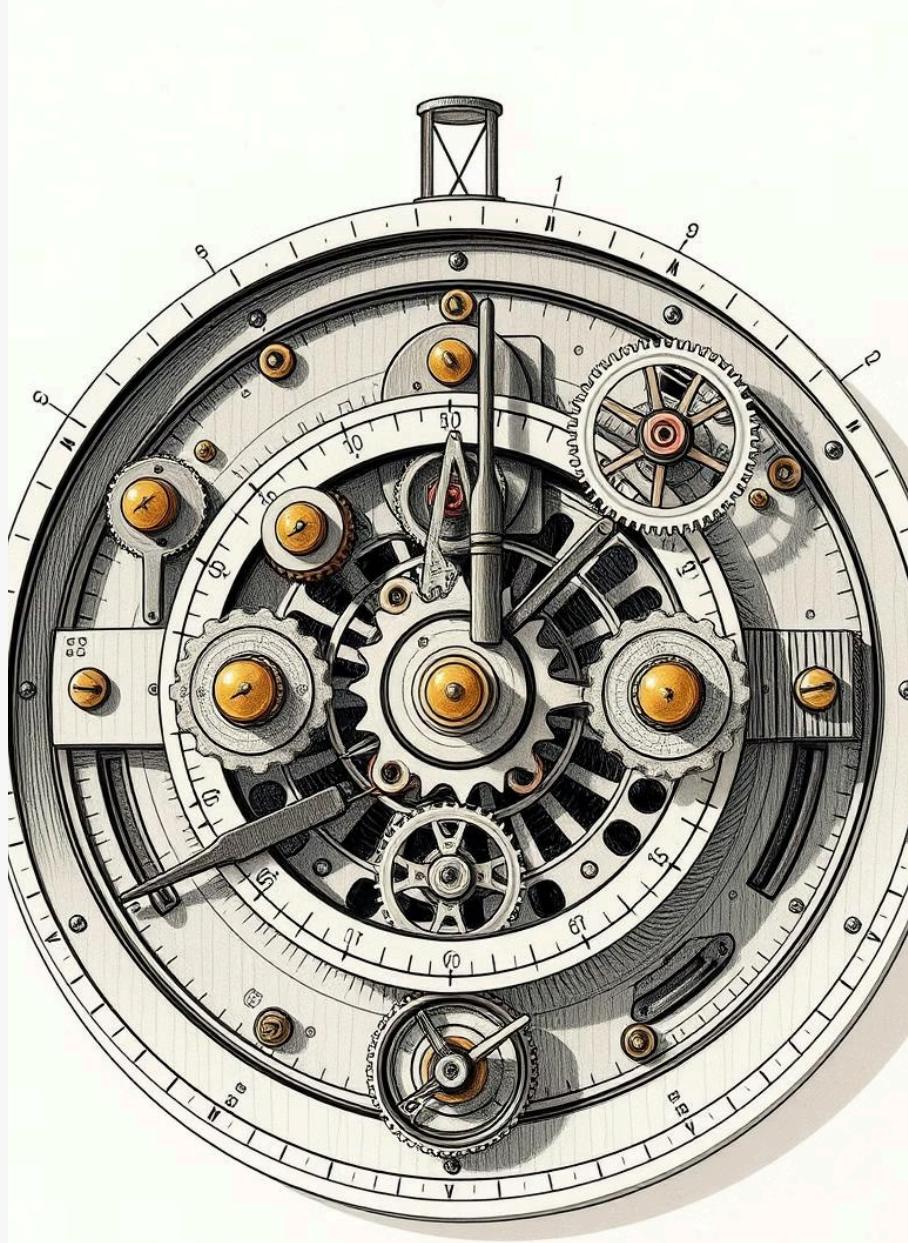
Le Chiffrement de Vigenère : Veille Cybersécurité

Explorons le chiffrement de Vigenère. Il s'agit d'une méthode de chiffrement polyalphabétique. Cette méthode a été autrefois réputée incassable. Nous allons analyser son fonctionnement, ses utilisateurs et des exemples concrets.



Fonctionnement du Chiffrement de Vigenère

Le chiffrement utilise une clé répétée. Chaque lettre du message est décalée. Le décalage est basé sur la lettre correspondante de la clé. C'est une amélioration du chiffrement de César.

Clé

Choisissez une clé secrète, par exemple, "CLE".

Message

Votre message clair : "ATTAQUE".

Chiffrement

Appliquez la clé répétée pour chiffrer chaque lettre.

Utilisateurs Historiques du Chiffrement de Vigenère

Ce chiffrement a été utilisé militairement et diplomatiquement. Il a servi au 19e siècle. On le pensait impénétrable avant le travail de Charles Babbage.

Militaire

Pour protéger les communications stratégiques.

Diplomatie

Pour sécuriser les échanges entre pays.

Secrets

Pour maintenir la confidentialité des informations.

Tw llu Vigenre, blear is the hé Vigenere cifher

Die tiscrypt. fichype, wit a liun's cifher,

Exemples de Messages Cryptés et Décryptés

Voici un exemple simple. Le message est "BONJOUR". La clé est "CLE". Le message chiffré devient "DPPQXWU". Le déchiffrement inverse le processus.

Message Clair	Clé
BONJOUR	CLE

Message Chiffré
DPPQXWU

Déchiffrement de Messages avec le Code de Vigenère

Pour déchiffrer, on utilise la même clé. On effectue l'opération inverse du chiffrement. Il faut soustraire le décalage induit par la clé.

1

Message Chiffré

DPPQXWU

2

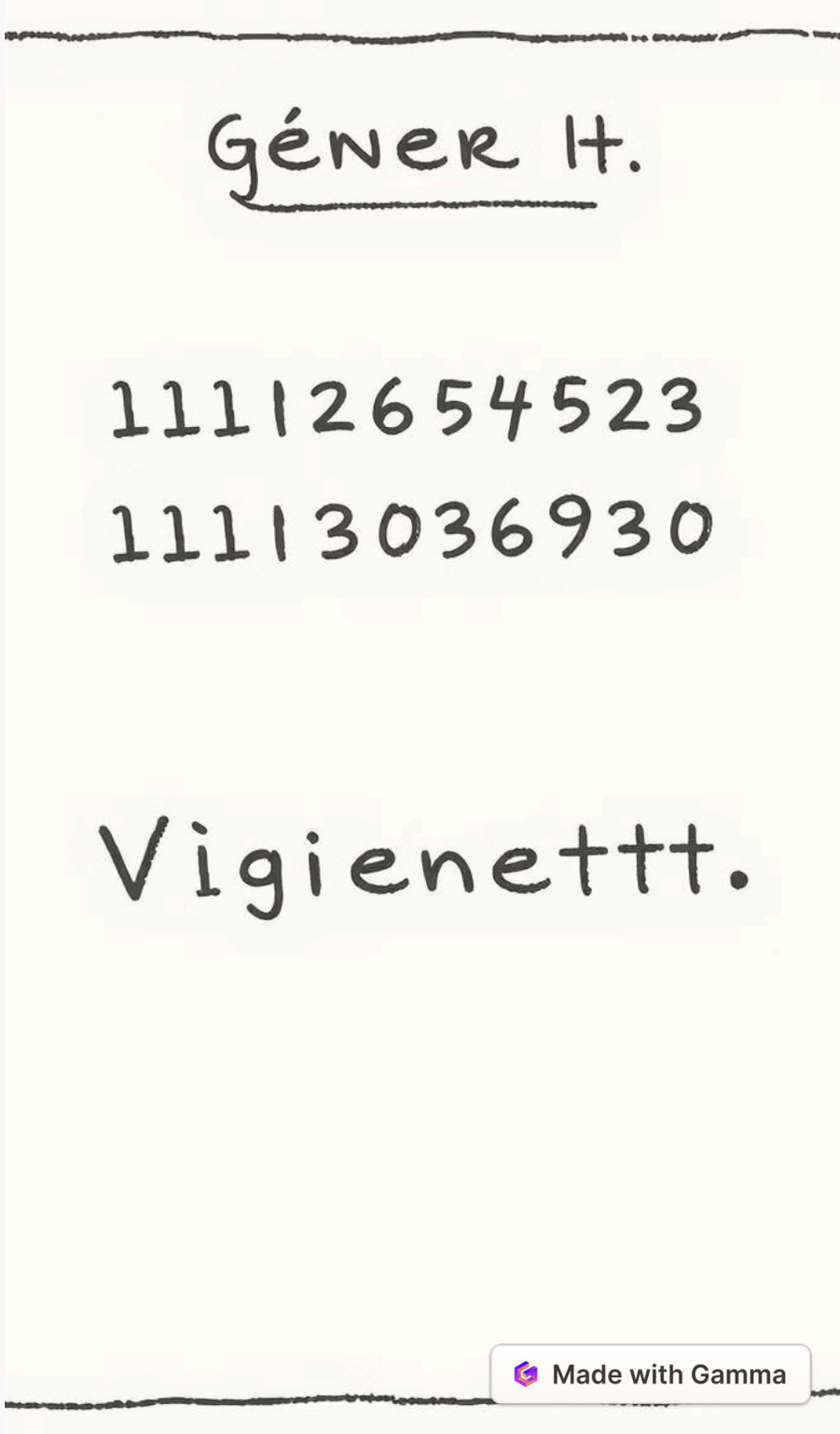
Clé

CLE

3

Déchiffrement

Retour à BONJOUR



Sources et Références

Voici quelques références clés sur le chiffrement de Vigenère. Elles couvrent l'histoire et l'analyse de cette méthode de chiffrement polyalphabétique.

- Wikipedia - Chiffre de Vigenère
- dCode - Chiffre de Vigenère