le cnam

SEC102 - TP03
ROT13

Date	Version	Description	Auteurs
18/02/2023	1	Retranscription collective des informations présentées en cours	Bartel Cantin Bialas Alexis Dufourt Marvin Faussurier Marc N'Guessan Jérémy

Sommaire :

Contexte :

ROT13 (Rotation 13) est un type de chiffrement de substitution qui remplace chaque lettre d'un texte par la lettre située 13 positions plus loin dans l'alphabet. Par exemple, la lettre A deviendra la lettre N, la lettre B deviendra la lettre O, et ainsi de suite. Le chiffrement ROT13 est souvent utilisé pour masquer des informations sensibles ou pour rendre des messages moins lisibles sans avoir à utiliser des méthodes de chiffrement plus complexes.
Nous pouvons le trouver notamment dans le registre UserAssist de Windows, cette technique de chiffrement est issue du chiffrement de César.
En utilisant ROT13, les données dans la base de registre UserAssist sont simplement décalées de 13 caractères, ce qui peut rendre leur lecture plus difficile pour les personnes qui ne sont pas familières avec le chiffrement ROT13.

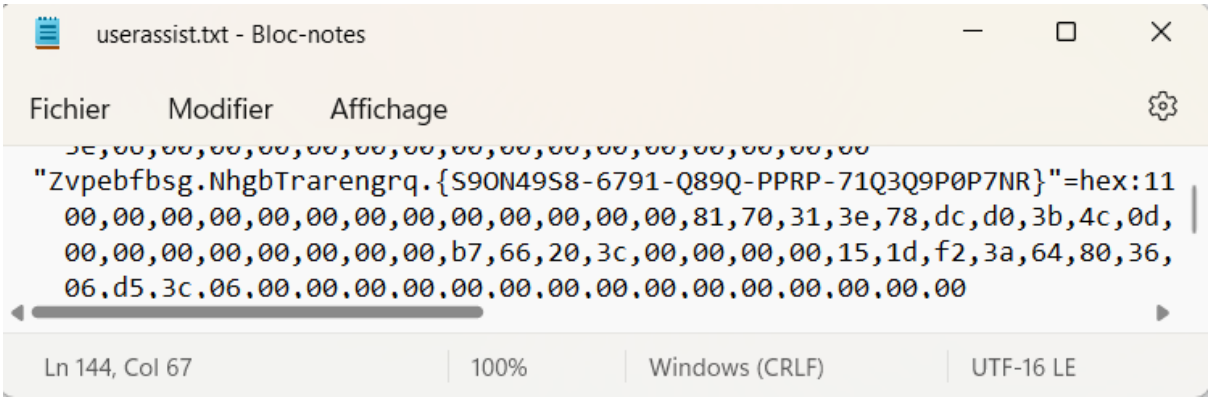
Code :

```
import java.io.*;

public class Main {
    public static void main(String[] args) {
        try {
            ProcessBuilder builder = new ProcessBuilder("reg", "export",
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count", "C:\userassist.txt");
            builder.start();
        } catch (IOException e) {
            e.printStackTrace();
        }
        try {
            BufferedReader reader = new BufferedReader(new FileReader("C:\userassist.txt"));
            BufferedWriter writer = new BufferedWriter(new
FileWriter("C:\decoded_userassist.txt"));
            String line;
            while ((line = reader.readLine()) != null) {
                String[] keys = line.split("""");
                for (int i = 1; i < keys.length; i += 2) {
                    String decodedKey = decodeROT13(keys[i]);
                    writer.write(decodedKey);
                    writer.newLine();
                }
            }
            reader.close();
            writer.close();
        } catch (IOException e) {
            System.out.println("Erreur");
        }
    }

    public static String decodeROT13(String encoded) {
        StringBuilder decoded = new StringBuilder();
        for (int i = 0; i < encoded.length(); i++) {
            char c = encoded.charAt(i);
            if (c >= 'a' && c <= 'm') {
                c += 13;
            } else if (c >= 'A' && c <= 'M') {
                c += 13;
            } else if (c >= 'n' && c <= 'z') {
                c -= 13;
            } else if (c >= 'N' && c <= 'Z') {
                c -= 13;
            }
            decoded.append(c);
        }
        return decoded.toString();
    }}
```

Explication du code :

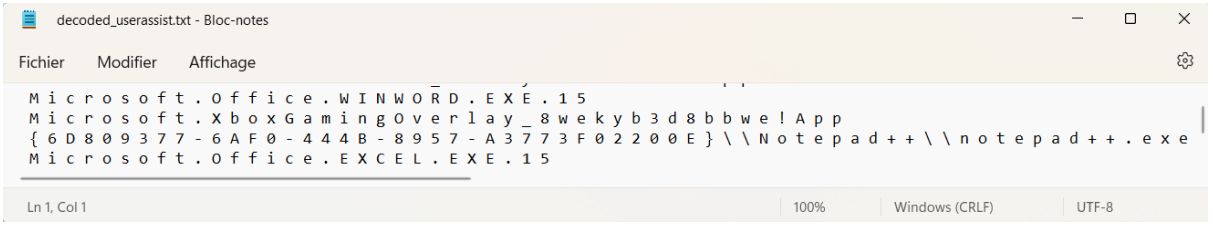
Tout d'abord, nous venons récupérer les clés contenues dans le registre UserAssist de Windows afin de les enregistrer dans un fichier nommé 'userassist.txt' en imitant, via un process builder, la commande Windows suivante : "reg", "export", "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count", "C:\userassist.txt".

Cette commande de Windows nous extrait un fichier UserAssist ressemblant à ceci :



Ensuite, on crée un reader pour accéder aux valeurs du fichier userassist.txt et parcourir celles-ci pour récupérer toutes nos clés (qui sont toutes contenues entre guillemets).

Nous faisons alors passer celles-ci par une méthode ROT13, puis via un writer, nous les enregistrons dans un fichier 'decoded_userassist.txt' ressemblant à ceci :



C’est ainsi qu’en quelques lignes de code, nous pouvons récupérer les données d’un utilisateur.

Il est important de noter qu’il est nécessaire d'exécuter celui-ci avec les droits administrateur, sans cela impossible d’exécuter la commande windows permettant l’extraction des clés.

Conclusion :

En conclusion, le chiffrement ROT13 est relativement simple à comprendre et à appliquer, car il suffit de prendre chaque lettre du texte original et de la remplacer par la lettre correspondante dans le tableau de substitution. Cependant, le chiffrement ROT13 est également facile à décoder, car il suffit de répéter le processus en sens inverse pour retrouver le texte original.

Glossaire :

Registre UserAssist : un registre de Windows qui contient des informations sur les programmes qui ont été exécutés sur un ordinateur. Il est utilisé par Windows pour afficher les raccourcis récemment utilisés dans le menu Démarrer et le menu Exécuter.

Chiffrement : la conversion d'un texte en clair en un texte chiffré, qui ne peut être compris que par le destinataire autorisé.

ROT13 : une technique de chiffrement par substitution qui consiste à décaler chaque lettre de l'alphabet de 13 positions. C'est un dérivé du code césar.

Chiffrement par substitution : une méthode de chiffrement qui remplace chaque lettre du texte en clair par une autre lettre, un chiffre ou un symbole.

Code César : une technique de chiffrement par substitution qui consiste à décaler chaque lettre de l'alphabet d'un nombre fixe de positions.

Chiffrement faible : une méthode de chiffrement qui peut être facilement déchiffrée ou cassée avec des méthodes connues.

Communications confidentielles : des communications qui doivent être protégées et ne doivent être accessibles qu'à des personnes autorisées.

Preuves numériques : des éléments de preuve numériques tels que des fichiers de journaux, des enregistrements de données et des métadonnées qui peuvent être utilisés pour prouver l'existence ou l'absence d'activités sur un système informatique.

Activités suspectes : des activités qui sont potentiellement malveillantes ou qui sont en contradiction avec les politiques de sécurité ou les procédures opérationnelles standard.

Process Builder : une classe Java qui permet de démarrer des processus externes sur le système d'exploitation Windows en spécifiant les arguments de la ligne de commande à exécuter (même principe que le Command Prompt).