Una Guia de como usar DataEnCrypto v0.6.1.2.5

Nishedcob et al.

January 16, 2014

Contents

1 Que es DataEnCrypto?

DataEnCrypto es un proyecto de codigo abierto que es un expirimento de varias formas de encriptar informacion. El idea es que uno puede ver el codigo y entender como cada metodo funciona y como es su implimentacion en Java. Ahora es un proyecto del ciclo, pero empezando Febrero 2014 dejara de ser esto y tal vez lo abrire para que todo el mundo, para los que quieren, pueden ayudar en su desarollo. Vivimos en una epoca peligroso con la NSA, GCHQ y otros agencias de espionaje digital que quieren accesso a todos nuestros datos y communicaciones personales – los que quieren privacidad necesitan proteger esta informacion de alguna forma – no poner los en linea, o usar las varias metodos de encriptacion que hay para esconderlos. Yo, como programador, como estudiante y como joven, tengo una resposibilidad de ver que todos tengan accesso a las harramientas que necesitan para proteger su propio informacion y que estas harramientas sean de una forma abierta para que, si tu quieres, puedes revisar el codigo abajo y verificar que no hay puertas traseras hecho por las mismas agencias o personas de cual queremos olcultar nuestros datos.

Uno se puede leer mas, y informacion mas actualizada en nuestro wiki: https://github.com/nishedcob/DataEnCrypto/wiki

2 Modos de Operacion

DataEnCrypto tiene dos formas de ejecutacion, por el interfaz de usuario de su sistema o por la consola. En el siguiente seccion, para los usuarios normales, vamos a ver como usar el interfaz de usuario. Para los usuarios mas avanzados que quieren ejecutar DataEnCrypto desde su consola, en la seccion de uso avanzado, vamos a ver las opciones para ejecutacion desde consola.
Usuarios Normales pueden ir directamente a seccion 2.2, "Para el Usuario Normal".

2.1 Argumentos por Consola

$-c$ Ejecutacion por Consola (Exclusiva con $-g\ -m\ -a\ -b$)

- $-h$ Ayuda (implica $-c$)
- $-t$ Prueba de cada cifra implica $-c$)

$-g$ Ejecutacion por Interfaz Grafica (Exclusiva con $-c\ -h\ -t$)

- $-m$ Abre el interfaz grafica abierto al Menu Principal (implica $-g$)
- $-a$ Abre el interfaz grafica abierto al Interfaz Avanzada (implica $-g$)
- $-b$ Abre el interfaz grafica abierto al Interfaz Basica (implica $-g$)

Otros casos:
sin argumentos Se ejecta la interfaz grafica abriendo el Menu Principal.
con solo argumentos disconocidos Se ejecuta ayuda por consola.

2.2 Para el Usuario Normal

2.3 Para el Usuario Avanzado

3 Algoritmos de Encriptacion

Cada metodo de encriptacion tiene sus adventejas y desadventejas. Si no, todos usarian el mismo metodo siempre. No... Hay que analizar el grado de proteccion que uno necesita y el tiempo y recursos que puede dar en los dos lados. Con estos dos, uno puede elegir su metodo que va a usar en el momento. Recuerda que uno debe hacer este analisis cada vez que va a encriptar algo porque su propio situacion puede cambiar a algo mejor o algo peor.

3.1 AutoLlave (AutoTexto)

AutoTexto Cifra, tambien conocido como la AutoLlave Cifra. Usa una clave como un offset y para encriptar los primeros datos. Despues usa la informacion para encriptar su mismo.

3.2 Cesar

La cifra Cesar es una de las cifras mas viejas y mas conocidas. Toma cada letra y suma o resta un valor constante a ello. Por lo tanto es facil de romper y nunca debe estar usado con datos que de verdad uno necesita proteger. Esta implimentado aqui para que uno puede estudiar como funciona.

3.3 Librereta de Un Solo Uso

El uso de la Librereta de un Solo Uso tiene reglas muy estrictas:

1. La llave (libreta) tiene que ser del mismo longitud o mas larga que los datos.
2. La llave (libreta) tiene que ser totalmente aletorio. Si hay como adivinar la llave, no es seguro.
3. La ley universal de la encriptacion: los que tienen tu llave, puden leer lo que encriptas, obviamente.

Pero, si estas condiciones se cumplen, esta forma de encriptacion es considerado como los professionales como lo absolutamente mas seguro. Nunca ha sido crackeado, porque es matematicamente impossible de crackear si estas tres condiciones se cumplen. Funciona en tomar cada caracter y sumarlo con un caracter de la llave. Ningun caracter de la llave se repita en ser usado en esta operacion (si no, seria la cifra de Vigenere) y normalmente se toma los datos y la llave en orden para que cuando llega a su destino, no hay que decirles un protocol del orden en que tengan que tomar el llave.

3.4 Matrices (Hill)

La cifra de matrices, tambien conocido la cifra de Hill es una cifra que usa multiplicacion entre matrices para encriptar y multiplicacion entre una matriz que representa el mensaje encriptado y la matriz inversa de la matriz usado para encriptar. Como usa multiplicacion de matrices para sus operaciones, esconde informacion del mensaje original para hacer su criptoanalisis mas dificil. Pero igual, de todas formas, esta cifra no debe ser considerado seguro ahora que computadoras tienen mucho poder. De todas formas, esta cifra es obsoleta.

3.5 VICTOR (VIC)

La cifra VIC, tambien conocido como la cifra VICTOR (por el criptonimo del agente de espianaje de la Union Sovetica que deserto su pais y mostro a la NSA como funciona) es un metodo bien seguro. En las aos de que la NSA sabia de su existencia en 1953 hasta la defectacion de agente VICTOR en 1957, la NSA no pudo crackear mensajes protegidos con este metodo y por lo tanto, no importa que es bastante simple que se puede hacerlo con lapiz y papel, hasta ahora es considerado ser muy seguro. El primer paso es codificar los datos como un serie de digitos. Durrante este proceso, las letras, los que el usuario elije con la primera fila de su tabla (que normalmente son la letras mas communes de un idioma, por ejemplo en ingles, se puede recordarlos con la frase: Ä SIN TO ERR̈) son comprimidas en la forma de un solo digito. Las demas caracteres se codifican con un digito de fila (que no puede tener un caracter en su columna en la primera fila) y un digito de columna. Este primer paso es muy importante porque, en comprimir algunas letras, se hace el criptoanalisis de todo el mensaje mucho mas dificil porque no hay como ver cuales digitos se pertenecen a cada letra (como algunas letras son de un digito y otros de dos digitos). El segundo paso suma una llave a todos estes digitos para esconder su contenido y despues en el terecer paso, se convirte este conjunto de digitos en texto de cifra.

3.6 Vigenre

La cifra vigenere es una implimentacion del cesar que lo hace mas dificil de crackear. En lugar de tener una solo constante o valor (llave) como el cesar, tiene un conjunto de llaves (valores, constantes, etc). Con cada nueva caracter en los datos, usa otro constante o llave en el conjunto de llaves hasta que no hay mas llaves y vuelve al inicio. De esta forma, con el mismo clave hasta la longtitud de la clave, el texto encifrado por AutoTexto sera igual que texto encifrado por este metodo. Desde alli es donde se usan metodos diferentes... El autotexto empieza a usar los datos, y este metodo, el vigenere solo repita la clave. Mientras que es mas dificil de crackear que el cesar, esto tambien no es una cifra recomendado para datos importantes.