**DESENCRIPTACIÓN AMSCO**

**FASES DE DESENCRIPTACIÓN DEL MÉTODO CIFRADO AMSCO**

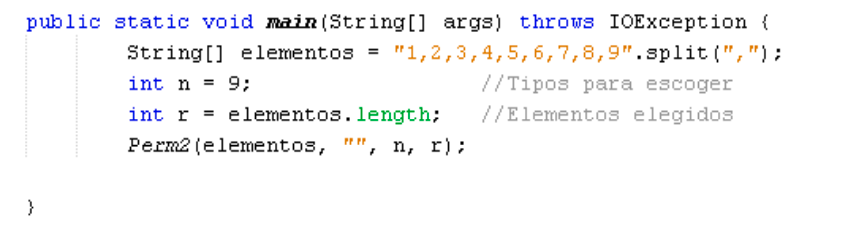
En la fase de desencriptación del método “CIFRADO AMSCO” se realizó en tres etapas las cuales describiremos a continuación;

**1.** **Generar las posibles claves:**

Las posibles claves para este algoritmos son una permutación de 9, el cual generamos a través del programa:

Claves:

El cual se tiene “elementos” un arreglo de lo que se quiere permutar “n” el número de tipos para escoger, “r” el número de elementos que podemos escoger en este caso 9 elementos, lo cuales son pasados como parámetros al metodo Perm2, quien nos devolverá todo las permutaciones posibles en un archivo llamado “claves09” el cual luego será utilizado.



2. **Generar las posibles matrices**

Las posibles matrices viene a ser las posibles soluciones que se puedan generar con las posibles claves que en el paso uno generamos por ejemplo:

Si tenemos que la posible clave fue 213456789

Y la cadena sifrrada es: NXVIAXEHXROMUVRDAAÑRMXSRNAOLILORXYUEEOXMMPAXAMPLXTOCEXPXAXEYEAAN

Entonces la posible matriz es una matriz de cinco por nueve ya que sabemos que la cadena contiene 64 elementos y la matriz podría contener 67, entonces nos sobran tres elementos los cuales serán reemplazados por “\*”. También se sabe que el algoritmo empieza siempre en la parte horizontal con una letra seguida de dos y así sucesivamente de la siguiente manera:

Posible clave: 213456798

Cadena sifrada: NXVIAXEHXROMUVRDAAÑRMXSRNAOLILORXYUEEOXMMPAXAMPLXTOCEXPXAXEYEAAN

Posible matriz:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| X | NX | D | SR | O | EO | A | XE | C |
| RO | V | AA | N | RX | X | MP | Y | EX |
| M | IA | Ñ | AO | Y | MM | L | AA | P |
| UV | X | RM | L | UE | P | XT | N | XA |
| R | EH | X | IL | E | AX | O | \* | \* |

Si nos damos cuenta siempre en las columnas pares como 0, 2,4,6,8 empiezan con un carácter y las demás columnas impares empiezan con dos caracteres esto se mantiene mientras empesemos a llenar nuestra matriz.

El código es el siguiente: el cual recibe un estring que viene a ser nuestra cadena cifrada y un arreglo de las posibles clave, entonces este método nos devuelve una posible respuesta la cual es leida de la matriz,en este ejemplo sería :

X NX D SR O EO A XE C RO V AA N RX X MP Y EX M IA Ñ AO Y MM L AA P UV X RM L UE P XT N XA R EH X IL E AX O \* \*

**3.** **Filtrado de la posible respuesta:**

Una vez obtenida nuestra posible respuesta la filtramos dos veces la primera con las combinaciones que no pueden estar en el idioma español como las palabra que terminan en “C”, y luego otro filtrado contando el número de conectores que contiene la posible respuesta com son: “LA”, “EN”, etc. Las cadenas que contengan e primer filtrado son eliminadas y las cadenas que contengan el segundo filtrado son puntuadas. Los cuales nosotros podemos elegir desde qué puntuación visualizar.

Los métodos son los siguiente:

En estos filtrados nos devuelven un número bastante reducidos de posibles respuestas

**UTILIZACIÓN DEL PROGRAMA GENERADO**

Esto se dividen en dos procedimientos las cuales son:

**Para encontrar la posible respuesta sin tener la clave:**

Para ello el programa requiere de dos entradas el código cifrado y un número que representa el puntaje de las respuestas lo que se explicó en el segundo paso, esto nos permite hacer más pequeño el número de posibilidades entre mayor sea el número menor son las posibles respuestas.

**Para encontrar la posible respuesta con la clave:**

Una vez conocida la clave se puede facilitar el procedimiento dándole al programa la clave y la cadena cifrada sin importar el puntaje, siguiendo con el ejemplo anterior tenemos que la clave es :

395714286, la cual colocaremos en el programa dando la siguiente frase cifrada con la misma clave

Sifrado : XXLESXSAULMIGEJOLEXMEXOXEREEXLTBRUQUENXMIESOOOXAEXOXCSOSXVSASPPR