Activitat 04: Xifrat per substitució polialfabètica

Introducció

Aquesta activitat servirà per introduir els sistemes de xifrat més contemporanis, i representa un augment de la seguretat en el xifratge respecte al xifrat mono-alfabètic.

Tot i que aquest sistema és més segur que el mono-alfabètic, no es considera de seguretat militar, però sí suficientment segur per a moltes aplicacions domèstiques.

Xifratge polialfabètic

Es parla de que un text es xifra amb xifratge polialfabètic quan per xifrar s'utilitza una permutació de l'abecedari original diferent per a la substitució de cada lletra del missatge. Es a dir, l'algorisme fa:

1. inicialitza la aleatorietat amb una llavor random (contrasenya).
2. Llegeix una lletra del missatge
3. permuta el alfabet
4. substitueix la lletra
5. si queden lletres ves al pas 2 sinó acaba

Per desxifrar el que s'ha de fer és:

1. inicialitza la aleatorietat amb la mateixa llavor random (contrasenya).
2. Llegeix una lletra del missatge xifrat
3. permuta l'alfabet
4. substitueix la lletra
5. si queden lletres ves al pas 2 sinó acaba

Exemple

Missatge = "Do"

a b c d e f g h i j k l m n o p q r s t u v w x y z (Alfabet original)

lletra = D
permuta l'alfabet: **Permutació1**: j p z a y n b v e q u w s f o i k l m v c d g h r
lletraXifrada = A

lletra = o
permuta l'alfabet: **Permutació2**: i k l m w s f o v c d g n b v e q u h r j p z a y
LletraXifrada = q

Missatge xifrat = "Aq"

Enunciat

Crea un programa en Java anomenat **Polialfabetic.java** que tingui un mètode `public static void permutaAlfabet()`, que generi una permutació de l'alfabet complet amb **accents greus**, **aguts**, **dièresi**, «**ç**» i «**ñ**» i ho emmagatzemi en una variable global.

Després crea els mètodes:

`public static String xifraPoliAlfa( String msg )` que xifre la cadena passada com a paràmetre amb xifratge polialfabètic.

`public static String desxifraPoliAlfa( String msgXifrat )` que desxifre la cadena del paràmetre i torni una cadena desxifrada amb polialfabètic.

Si ho necessites pots fer mètodes addicionals

El mètode principal "main" ha de ser aquest:

```
public static void main(String[] args) {
String msgs[] = {"Test 01 àrbritre, coixí, Perímetre",
"Test 02 Taüll, DÍA, año",
"Test 03 Peça, Òrrius, Bòvila");
String msgsXifrats[] = new String[msgs.length];

System.out.println("Xifratge:\n--------");
for (int i = 0; i < msgs.length; i++) {
initRandom(clauSecreta);
msgsXifrats[i] = xifraPoliAlfa(msgs[i]);
System.out.printf("%-34s -> %s%n", msgs[i], msgsXifrats[i]);
}

System.out.println("Desxifratge:\n-----------");
for (int i = 0; i < msgs.length; i++) {
initRandom(clauSecreta);
String msg = desxifraPoliAlfa(msgsXifrats[i]);
System.out.printf("%-34s -> %s%n", msgsXifrats[i], msg);
}
}
```

Lliurament

Has de penjar el link al teu github de la UF i la carpeta que contingui el projecte Java s'ha d'anomenar «**04-Polialfabetic**»