Xifratge del Cèsar

En criptografia, un xifrat de Cèsar, conegut també com a codificació de Cèsar, xifratge per decalatge, codi de Cèsar o decalatge de Cèsar, és una de les tècniques de xifratge més senzilles i més a bastament conegudes.

És un tipus de xifratge per substitució en el qual cada lletra del text clar se substitueix per una altra lletra que estigui un determinat nombre fix de posicions desplaçades a l'alfabet. Per exemple, amb un decalatge de 3, la A se substituiria per la D, la B esdevindria E, i així. El mètode deu el seu nom a en Juli Cèsar, qui el feia servir per comunicar-se amb els seus generals.

Exemples:

- Text clar: SETZE JUTGES MENGEN FETGE
- Text xifrat: WIXDI NYXKIW QIRKIR JIXKI H'YR TIRNEX

Observem que s'ha fet servir un decalatge de 4 caràcters (la 'S' correspon a la 'W', la 'E' a la 'I'), etc...

La vostra tasca

Implementeu una classe anomenada "Caesar" (vegeu esquelet adjunt al moodle), amb els mètodes:

- static String cypher(String s, int delta) // Codifica un String mitjançant un xifrat del Cèsar amb el decalatge indicat a la variable "delta".
- static String decypher(String s, int delta) // Decodifica un String mitjançanat un xifrat del Cèsar amb el decalatge indicat a la variable "delta".
- static String magic(String s) // Decodifica un String mitjançant un xifrat del Cèsar, però endevinant el decalatge necessari. Exploteu el fet que les frases es troben en l'idioma Català.

Xifratge Vigenère

El xifratge Vigenère és un mètode per xifrar text, que empra una sèrie de «xifrats del Cèsar» basats en les lletres de l'alfabet. És un sistema de xifratge polialfabètic i de substitució.

El procediment de xifrat consisteix en «sumar» les lletres del missatge i de la clau. Per fer aquesta operació, heu d'assignar un número a cada lletra. Exemple: (A (1) + A (1) = B (2), A (1) + B (2) = C (3), Z (26) + B (2) = B (2), etc...).

Suposem que el missatge a encriptar és «AVUI PLOU», i la clau «LICEU», fem les següents sumes:

- A + L = M
- V + I = E
- U + C = X
- I + E = N
- P + U = K
- L + L = X
- O + I = X
- U + C = X

Per tant, el missatge «AVUI PLOU» codificat amb la clau «LICEU» és «MEXN KXXX».

S'observa que a una mateixa lletra en el text clar li poden correspondre diferents lletres en el text xifrat.

Exemples:

- Missatge: «ABC»; Clau: «AAA»; Resultat: «BCD»
- Missatge: «ZZZ»; Clau: «AA»; Resultat: «AAA»
- Missatge: «YYY»; Clau: «A»; Resultat: «ZZZ»
- Missatge: «BEN FET»; Clau: «AKYP»; Resultat: «CPM VFE»
- Missatge: «El camió és vermell»; Clau: «terra»; Resultat: «YQ USNCT WK WYWEWMF»

Observacions:

- S'empra l'alfabet de majúscules (26 lletres) exclusivament.
- Les minúscules es passen a majúscules, tant al missatge com a la clau.
- Les vocals accentuades es canvien per les corresponents sense accentuar.
- Els caràcters que no són lletres (apòstrofs, espais...) no es codifiquen.

La vostra tasca

Heu d'implementar una classe en JAVA, anomenada «Vigenere» amb els següents mètodes públics:

- public static String encode(String message, String password)
- public static String decode(String message, String password)

El primer mètode ha de codificar mitjançant el mètode de Vigenere un missatge (primer paràmetre) emprant la password (segon paràmetre), i ha de retornar el missatge xifrat.

El segon mètode ha de realitzar l'operació inversa.

Xifratge per transposició

En criptografia, un xifratge per transposició és un mètode d'encriptació en què les posicions del text pla (generalment caràcters o grups de caràcters) es desplacen seguint un sistema regular, de manera que el text xifrat consisteixi en una permutació del text pla. D'aquesta manera es canvia l'ordre de les unitats.

Exemple: Volem xifrar "AVUI FA BON DIA" amb una matriu de dimensió 3. El primer que fem és escriure el text horitzontalment en una taula que té 3 columnes:

A	V	U
I		F
A		B
O	N	
D	I	A

Si ara llegim el text per columnes, ens queda:

AIAODV NIUFB A

Una variant una mica més forta d'aquest sistema de xifratge, és el que empra una paraula clau per definir l'ordre de les columnes.

Per exemple, volem xifrar "AVUI FA BON DIA" amb la paraula clau "LICEU". Ens quedaria el següent:

L	**I**	**C**	**E**	**U**
A	V	U	I	
F	A		B	O
N		D	I	A

Ara posem en ordre alfabètic les lletres de la clau (LICEU), arrosegant també les columnes:

C	**E**	**I**	**L**	**U**
U	I	V	A	
	B	A	F	O
D	I		N	A

Ara llegim per columnes:

U DIBIVA AFN OA

La vostra tasca

Implementeu una classe anomenada "Transposition" amb els mètodes:

- static String cypher(String s, int dim) // Realitza un xifrat per transposició del text "s" usant una matriu de "dim" columnes
- static String decypher(String s, int dim) // Realitza un decodificat del text "s" per transposició usant una matriu de "dim" columnes
- static String cypher(String s, String key) // Realitza un xifrat per transposició variable del text "s" usant la clau "key".
- static String decypher(String s, String key) // Realitza un decodificat del text "s" per transposició variable del text "s" usant la clau "key".

Teniu disponible al moodle un esquelet amb tots els mètodes i amb els tests unitaris que heu de superar. Bona sort!!!