Orientacions

Criptografia

- Es poden treballar algunes de les xifres, però poques ja que codificar i descodificar és força lent. És bo l'intercanvi de missatges entre alumnes, és recomanable que siguin curts.
- Es poden proposar els models de xifra després d'haver fet una pràctica de criptoanàlisi. Convé veure dels dos tipus: de transposició i de substitució.
- La xifra de graella rotatòria té un valor afegit per la construcció de la graella-clau, fase en la que s'han de tenir en compte aspectes geomètrics de composició de girs.
- La xifra de Polibi es pot fer com a pràctica de classe indicant nombres amb les mans.

Criptoanàlisi

- Pot ser bona idea fer una pràctica abans de veure mètodes de xifra
- L'experiència tal com es va fer durant dos cursos a l'IES Alella (amb les idees de la professora Luisa Abad) va tenir el següent procés
    1. Al juny, a 1r d'ESO, es va encarregar de "feina d'estiu" la recollida de dades de freqüència de lletres
    2. Al setembre, en començar 2n, es van recollir els fulls i el professorat varem recopilar totes les dades (que acumulàvem d'un curs al següent)
    3. Es donava a cadascun dels quatre grups classe un fragment codificat amb Xifra de Cèsar. Entre els quatre fragments es formava un història. Cada fragment estava codificat amb una clau diferent, amb les paraules separades i els signes de puntuació conservats. També es donava la taula de freqüències recollides per tot el curs.
    4. Es demanava que es trobessin les freqüències del text codificat i, amb aquestes dades, s'intentés descodificar el missatge. (Val a dir que una part de l'alumnat, tot i fer aquest còmput, no el van utilitzar gaire al descodificar)
    5. Un cop descodificat es discutia sobre formes de complicar la xifra i es veia algun dels mètodes històrics de xifra clàssica.
    6. Opcionalment es donava un nou text a descodificar (amb xifra de substitució monoalfabètica) amb els signes agrupats de cinc en cinc i sense signes de puntuació.
- Per descodificar es pot fer servir un processador de textos. Les eines retallar-enganxar-substituir estalvien molta feina. Quan es fa servir l'eina de substituir s'ha de **procurar tenir en compte les opcions de format per diferenciar el text codificat de les proves** que s'estan fent. S'ha d'estudiar la forma de fer accessible el text en document informatitzat (el més pràctic és des de la pròpia web del centre)

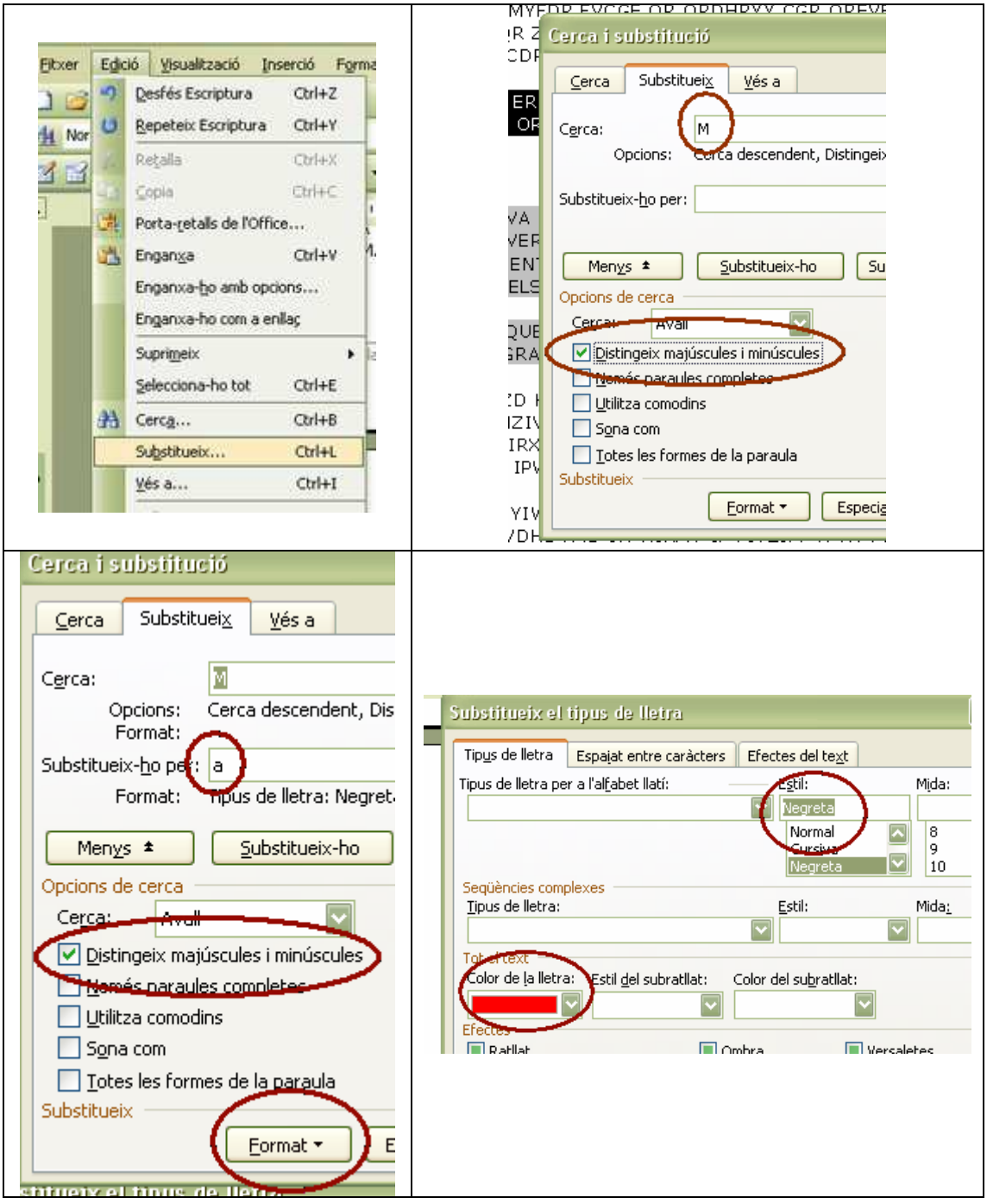
Exemple amb Word

GA NBA QVM ER YV HM CDRERAFMD, MY OVDGDTVM, GA OYVRAF V YV HM QR-ZMAMD ÇGR YV OMAHVRE RY ORDHRYY.

1) Seleccionar tros

GA NBA QVM ER YV HM CDRERAFMD, MY OVDGDTVM, GA OYVRAF V YV HM QR-ZMAMD ÇGR YV OMAHVRE RY ORDHRYY.

2) Reemplaçar M per a.



3) Resultat

GA NBA QV**a** ER YV H**a** CDRERAF**a**D, **a**Y OVDGDTV**a**, GA OYVRAF V YV H**a** QRZ**a**-A**a**D ÇGR YV O**a**AHVRE RY ORDHRYY.

Solucionari dels exercicis de xifra

Xifra ATBAS	1. ULG DUQUM ZIEUGFZ LQF 2. No podré venir
Xifra de Cèsar	2. WAKJKS GR RRUI JK YKSVXK 3. Millor al lloc de l'altre dia
Xifra de Polibi	1. 3211 45433512111411 1544 24334135444424123215 2. Vegem-nos demà
Xifra Pigpen	1. ¯| < _| |·¯ ¯| _| |¯| |·_ \/ |¯| |_ |·¯ |¯| > 2. No crec que pugui callar
Xifra de Bacon	1. abbbb aabaa baaab abaaa ababb ababb 2. (aaaba abbba baaab baaab aabaa abbaa) Correm
Xifra homofònica	*1. Hi ha més d'una solució* 2. Esperaré
Xifra ADFGVX	1. VVDXX FDFVA GFGFX VXVFX FFFAA 2. Millor a les 10
Xifra Playfair	1. ALNQA SRN 2. Ornitorinc
Xifra de Vigenère	1. PMFL CS PL TRBBCHZX CMVDJ 2. Sí que entenc aquest codi
Xifra en Rail	1. (2) NLDGIAIGOIIUSNNU (3) NDIIOIIUSNNULGAG 2. Quan es va despertar, el dinosaure encara hi era.
Xifra en matrius	1. UGADR NABNE QAUSE NTSCE ERTXX 2. No m'agrada que desconfiïs de mi.
Xifra en graella giratòria	1. ESNO BPMT OEAO DRRN 2. Demà a mateixa hora