# Pràctica 1 Cripto

**Exercici 1:**

El primer exercici demanava dues coses, analitzar la freqüència d'un text xifrat amb Cesar i trobar la clau i desxifrar-lo amb aquesta. S'ha fet un programa que fa genera un mapa amb l'anàlisi de freqüència i dona totes les possibles solucions amb el xifrat Cesar, es a dir, retorna 26 solucions, i es pot avaluar quina clau s'ha emprat per xifrar el text.

```
PS C:\Users\Mikael\Desktop\UNI\4\SEGURETAT D'APLICACIONS I COMUNICACIONS\Exercicis_Criptografia\Criptografia\Exercici 1> python ex1.py
Análisis de frecuencia del texto cifrado:
{'T': 17, 'S': 10, 'L': 13, 'G': 2, 'P': 27, 'D': 11, 'Y': 13, 'E': 19, 'R': 3, 'J': 1, 'Z': 14, 'F': 4, 'A': 3, 'W': 11, 'H': 3, 'O': 5, '
M': 3, 'N': 3, 'V': 3, 'Q': 4, 'C': 9, 'X': 5}
Desplazamiento 1: S RKFO COOX DRSXQC IYE ZOYZVO GYEVN XYD LOVSOFO, KDDKMU CRSZCYX PSBO YPP DRO CRYEVNOB YP YBSYX, S GKDMRON M-LOKWC QVSDDOB
SX DRO NKBU XOKB DRO DKXXRKECOB QKDO. KVV DRYCO WYWOXDC GSVVLO VYCD SX DSWO, VSUO DOKBC SX BKSX. DSWO DY NSO.
Desplazamiento 2: R QJEN BNNW CQRWPB HXD YNXYUN FXDUM WXC KNURNEN, JCCJLT BQRYBXW ORAN XOO CQN BQXDUMNA XO XARXW, R FJCLQNM L-KNJVB PURCCNA
RW CQN MJAT WNJA CQN CJWWQJDBNA PJCN. JUU CQXBN VXVNWCB FRUUKN UXBC RW CRVN, URTN CNJAB RW AJRW. CRVN CX MRN.
Desplazamiento 3: Q PIDM AMMV BPQVOA GWC XMWXTM EWCTL VWB JMTQMDM, IBBIKS APQXAWV NQZM WNN BPM APWCTLMZ WN WZQWV, Q EIBKPML K-JMIUA OTQBBMZ
QV BPM LIZS VMIZ BPM BIVVPICAMZ OIBM. ITT BPWAM UWUMVBA EQTTJM TWAB QV BQUM, TQSM BMIZA QV ZIQV. BQUM BW LQM.
Desplazamiento 4: P OHCL ZLLU AOPUNZ FVB WLVWSL DVBSK UVA ILSPLCL, HAAHJR ZOPWZVU MPYL VMM AOL ZOVBSKLY VM VYPVU, P DHAJOLK J-ILHTZ NSPAALY
PU AOL KHYR ULHY AOL AHUUOHBZLY NHAL. HSS AOVZL TVTLUAZ DPSSIL SVZA PU APTL, SPRL ALHYZ PU YHPU. APTL AV KPL.
Desplazamiento 5: O NGBK YKKT ZNOTMY EUA VKUVRK CUARJ TUZ HKROKBK, GZZGIQ YNOVYUT LOXK ULL ZNK YNUARJKX UL UXOUT, O CGZINKJ I-HKGSY MROZZKX
OT ZNK JGXQ TKGX ZNK ZGTTNGAYKX MGZK. GRR ZNUYK SUSKTZY CORRHK RUYZ OT ZOSK, ROQK ZKGXY OT XGOT. ZOSK ZU JOK.
Desplazamiento 6: N MFAJ XJJS YMNSLX DTZ UJTUQJ BTZQI STY GJQNJAJ, FYYFHP XMNUXTS KNWJ TKK YMJ XMTZQIJW TK TWNTS, N BFYHMJI H-GJFRX LQNYYJW
NS YMJ IFWP SJFW YMJ YFSSMFZXJW LFYJ. FQQ YMTXJ RTRJSYX BNQQGJ QTXY NS YNRJ, QNPJ YJFWX NS WFNS. YNRJ YT INJ.
Desplazamiento 7: M LEZI WIIR XLMRKW CSY TISTPI ASYPH RSX FIPMIZI, EXXEGO WLMTWSR JMVI SJJ XLI WLSYPHIV SJ SVMSR, M AEXGLIH G-FIEQW KPMXXIV
MR XLI HEVO RIEV XLI XERRLEYWIV KEXI. EPP XLSWI QSQIRXW AMPPFI PSWX MR XMQI, PMOI XIEVW MR VEMR. XMQI XS HMI.
Desplazamiento 8: L KDYH VHHQ WKLQJV BRX SHRSOH ZRXOG QRW EHOLHYH, DWWDFN VKLSVRQ ILUH RII WKH VKRXOGHU RI RULRQ, L ZDWFKHG F-EHDPV JOLWWHU
LQ WKH GDUN QHDU WKH WDQGKDXVHU JDWH. DOO WKRVH PRPHQWV ZLOOEH ORVW LQ WLPH, OLNH WHDUV LQ UDLQ. WLPH WR GLH.
Desplazamiento 9: K JCXG UGGP VJKPIU AQW RGQRNG YQWNF PQV DGNKGXG, CVVCEM UJKRUQP HKTG QHH VJG UJQWNFGT QH QTKQP, K YCVEJGF E-DGCOU INKVVGT
KP VJG FCTM PGCT VJG VCPPJCWUGT ICVG. CNN VJQUG OQOGPVU YKNNDG NQUV KP VKOG, NKMG VGCTU KP TCKP. VKOG VQ FKG.
Desplazamiento 10: J IBWF TFFO UIJOHT ZPV QFPQMF XPVME OPU CFMJFWF, BUUBDL TIJQTPO GJSF PGG UIF TIPVMEFS PG PSJPO, J XBUDIFE D-CFBNT HMJUUF
SJO UIF EBSL OFBS UIF UBOOIBVTFS HBUF. BMM UIPTF NPNFOUT XJMMCF MPTU JO UJNF, MJLF UFBST JO SBJO. UJNF UP EJF.
Desplazamiento 11: I HAVE SEEN THINGS YOU PEOPLE WOULD NOT BELIEVE, ATTACK SHIPSON FIRE OFF THE SHOULDER OF ORION, I WATCHED C-BEAMS GLITTE
RIN THE DARK NEAR THE TANNHAUSER GATE. ALL THOSE MOMENTS WILLBE LOST IN TIME, LIKE TEARS IN RAIN. TIME TO DIE.
```

Com es pot apreciar, la clau que s'ha emprat en el text, ha estat 11.

**Exercici 2:**

El segon exercici consistia en 3 parts, una d'elles no ha estat possible realitzar-la. El primer que es demanava era xifrar el text donat amb substitució simple i substitució homòfona. Per la simple, s'ha utilitzat una clau igual a 5, i per el xifrat amb substitució homòfona s'ha creat un diccionari per tal d'assignar més d'un símbol als caràcters més usats. El segon pas ha estat analitzar les freqüències dels dos textos xifrats, quedant bastant clar que el xifrat homòfon es bastant més efectiu, doncs no es repeteixen tant els símbols.

```
PS C:\Users\Mikael\Desktop\UNI\4\SEGURETAT D'APLICACIONS I COMUNICACIONS\Exercicis_Criptografia\Criptografia> python ex1.py
Texto Cesar analisis de frecuencia:
{'J': 3, 's': 124, 'z': 90, 'q': 114, 'l': 23, 'f': 249, 'w': 108, 'i': 100, 'j': 228, 'R': 1, 'h': 78, 'm': 19, 'd': 20, 't': 164, 'r': 46, 'g': 30, 'v': 30, 'n':
 93, 'y': 63, 'u': 27, 'a': 19, 'x': 140, 'e': 13, 'k': 12, 'Z': 1, 'o': 8, 'Y': 1, 'K': 2, 'c': 1, 'V': 4, 'U': 1, 'D': 2, 'X': 1, 'Q': 1}

Texto homofono analisis de frecuencia:
{'J': 105, 'Ξ': 82, 'H': 82, 'U': 107, 'v': 87, 'N': 61, 'β': 129, 'T': 82, 'Σ': 120, 'ρ': 60, 'L': 137, 'φ': 129, 'ζ': 49, 'Δ': 58, 'ψ': 126, 'X': 53, 'W': 98, 'Ψ
': 115, 'V': 69, 'Z': 144, 'D': 154, 'Y': 103, 'Q': 106, 'η': 106, 'C': 81, 'F': 143, 'π': 43, 'ϖ': 47, 'μ': 95, 'φ': 128, 'Θ': 116, 'κ': 123, 'G': 111, 'ω': 30, '
χ': 138, 'λ': 76, 'σ': 32, 'Ω': 72, 'δ': 81, 'M': 110, 'α': 45, 'K': 35, 'τ': 3}
```

Per últim, es demanava compartir un text xifrat a algun company i tractar de desxifrar el seu, el qual no ha estat possible. Tot i així, sí que s'ha xifrat un text, que ha estat un extracte de *La Vida es Sueño:*

*Es verdad; pues reprimamos esta fiera condición, esta furia, esta ambición, por si alguna vez soñamos. Y sí haremos, pues estamos en mundo tan singular, que el vivir solo es soñar; y la experiencia me enseña que el hombre que vive sueña lo que es, hasta despertar.*

*Suena el rey que es rey, y vive con este engaño mandando, disponiendo y gobernando; y este aplauso, que recibe prestado, en el viento escribe, y en cenizas le convierte la muerte, ¡desdicha fuerte! Que hay quien intente reinar, viendo que ha de despertar en el sueño de la muerte.*

*Suena el rico en su riqueza, que más cuidados le brinda que el bien que de ella se saca, y el que más la estimar solía, con solo ver que se acaba desengañado se queja; suena el que más vil se deja por honra de su parentela, y el que en libertad vivía somete al yugo su cabeza.*

*Suena el que a sus pensamientos daba ley y gobernación, y el que a su voluntad ponía todo el mundo a su alcance; suena el que en gran abundancia tenía oro, bienes y suerte, y el que en su pobreza fuerte soporta con paciencia; suena todo, y la evidencia desengaña toda muerte.*

**Exercici 3:**

Aquest exercici demanava dues coses, primer trobar quina és la longitud més possible de la clau amb la que s'ha xifrat el text proporcionat. I la segona trobar aquesta clau. S'ha anat una mica més enllà, i al trobar la clau, s'ha desxifrat el text per complet per tal de assegurar que la clau era la correcta.

```
PS C:\Users\Mikael\Desktop\UNI\4\SEGURETAT D'APLICACIONS I COMUNICACIONS\Exercicis_Criptografia\Criptografia\Exercici 3> python ex3a.py
La longitud estimada és de: 6
```

La longitud estimada per l'algorisme ha estat de 6. Per tant, el següent pas ha estat trobar aquesta clau. S'ha creat un programa per tal de trobar la clau més probable, amb la facilitat que ja es sap la longitud d'aquesta. El resultat ha estat el següent.

```
PS C:\Users\Mikael\Desktop\UNI\4\SEGURETAT D'APLICACIONS I COMUNICACIONS\Exercicis_Criptografia\Criptografia\Exercici 3> python ex3b.py
La longitud estimada és de: 6
La clave estimada es: PATITO
```

I per últim s'ha desxifrat el text usant la clau que s'ha obtingut.

```
PS C:\Users\Mikael\Desktop\UNI\4\SEGURETAT D'APLICACIONS I COMUNICACIONS\Exercicis_Criptografia\Criptografia\Exercici 3> python ex3.py
(['PATITO', 'TATITATA', 'TATATITITI'], 'el metode kasiski en criptoanalisi tambe conegut com a examen de kasiski o prova de\nkasiski es un
metode per atacar els xifratges de substitucio polialfabetica com el\nxifratge de vigenere\naquest metode deu el seu nom a loficial prussia
 friedrich kasiski que el va publicar el\n1863 pero sembla haver estat descobert de manera independent per charles babbage ja el\n1846\nen
els xifratges de substitucio polialfabetics on els alfabets de substitucio es trien\nmitjaneant lus d'una paraula clau lexamen de kasiski p
ermet a un criptoanalista deduir la\nlongitud de la paraula clau\nun cop descoberta la longitud de la paraula clau el criptoanalista alinea
 el text xifrat en\nn columnes on n es la longitud de la paraula clau\naleshores cada columna es pot tractar com el text xifrat dun xifrat
de substituciq\nmonoalfabftica\ncom a tal cada columna pot ser atacada amb analisi de frequencia De la mateixa manera\nquan sha utilitzat u
na maquina de xifratge de corrent de rotor aquest metode pot permetre deduir la longitud dels rotors individuals\nkasiski es va adonar de l
existencia de paraules repetides en el text xifrat el que significa\ngairebe amb tota probabilitat que aquestes paraules no nomes eren la m
ateixa abans\ndel xifrat sino que a mes la clau coincidia en la mateixa posicio en les dues ocurrencies\nsabent llavors que la distancia en
tre paraules repetides es multiple de la longitud de\nla clau era questio de cercar diferents paraules que es repetissin i trobar el seu ma
xim\ncomu divisor per daquesta manera trobar un multiple proper a la longitud de la clau\nla longitud de la clau sera aquest nombre o algun
 factor primer daquest\nun cop descoberta la longitud de la clau amb que es va xifrar el document nomes cal\ndividir el text en blocs de la
 mateixa mida que la longitud de la clau i aplicar el\nmetode estadistic tradicional del xifratge de cesar')
```

**Exercici 4:**

Aquest exercici demanava realitzar uns càlculs per tal que estimar quan es trigaria a resoldre les següents qüestions. Els càlculs s'han realitzat estimant que un ordinador potent pot arribar a provar 10^10 claus per segon.

El primer càlcul ens demana la estimació de temps de càlcul per força bruta amb una substitució simple de 26 lletres. El nombre de claus que es poden arribar a generar es de 26!. Per trobar el temps necessari hem de fer un factor de conversió entre les claus totals, i les claus que pot provar l'ordinador. El resultat ha estat el següent.

$$\frac{4.0329 \times 10^{26}}{10^{10}} = 4.0329 \times 10^{16}\ \text{s}$$

Aquesta xifra en anys 1.28 mil milions d'any

El segon càlcul demanava calcular el temps en desxifrar una permutació simple de blocs de llargada 10. El càlcul es el mateix que en el anterior. Al ser blocs de 10, les claus que es poden arribar a generar són 10!. S'ha de tornar a fer un factor de conversió.

$$\frac{3.6288 \times 10^6}{10^{10}} = 3.6288 \times 10^{-4}\ \mathrm{s}$$

Aquesta xifra equival a 0.36 milisegons.

I l'últim càlcul demanava fer el mateix càlcul que en els anteriors però ara per a un Vigenere amb clau de longitud *k*. *El nombre de claus possibles serà 26^k*. Per saber el temps necessari s'ha de fer un factor de conversió.

$$\frac{26^k}{10^{10}}\ \mathrm{s}$$

El resultat dependrà de la llargada de la clau. Per poder tenir una idea de quan trigaria, s'ha fet els càlculs amb *k*=4, *k*=8, *k*=12. Els resultats han estat 45 microsegons, 21 segons i 110 dies respectivament.