***Imagen que contiene Logotipo

Descripción generada automáticamente***

Alejandro Ortega Martínez

Grado en Ingeniería Informática

3/5/2021

Practica 3

Seguridad Informática

Contenido

[1. Fundamentos teóricos 2](#_Toc70936192)

[Apartado 1: Primalidad 2](#_Toc70936193)

[Apartado 2: Modularidad 2](#_Toc70936194)

[Apartado 3: Máximo común Divisor 2](#_Toc70936195)

[Apartado 4: Conjunto reducido de restos 2](#_Toc70936196)

[Apartado 5 Indicador de Euler 2](#_Toc70936197)

[Apartado 6: Inversos 2](#_Toc70936198)

[Apartado 7: Exponenciación dentro de un cuerpo 2](#_Toc70936199)

[Informe 2](#_Toc70936200)

[Criptosistemas clásicos 4](#_Toc70936201)

[Cifradores Monoalfabéticos por sustitución: Desplazamiento Puro 4](#_Toc70936202)

[Apartado 1 4](#_Toc70936203)

[Apartado 2 4](#_Toc70936204)

[Informe 6](#_Toc70936205)

[Cifradores Monoalfabéticos por sustitución: Decimación Pura 7](#_Toc70936206)

[Apartado 1 7](#_Toc70936207)

[Apartado 2 8](#_Toc70936208)

[Informe 10](#_Toc70936209)

[Cifradores polialfabeticos por sustitución: Cifradores Periódicos 12](#_Toc70936210)

[Cifrado de Vigenère 12](#_Toc70936211)

[Cifrado de Beaufort 20](#_Toc70936212)

[Cifrado variante de Beaufort 26](#_Toc70936213)

[Cifradores polialfabeticos por sustitución: Cifradores Periódicos 30](#_Toc70936214)

[Cifrado de Vernam 30](#_Toc70936215)

[Cifradores polialfabeticos por sustitución: Cifradores de Transposición 33](#_Toc70936216)

[Cifradores por Transposición de Filas 33](#_Toc70936217)

[Cifradores por Transposición de Columnas 33](#_Toc70936218)

[Bibliografía 38](#_Toc70936219)

# 1. Fundamentos teóricos

### Apartado 1: Primalidad

**a)Confeccione una tabla con los 100 primeros números primos.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 2 | 3 | 5 | 7 | 11 | 13 | 17 |
| 19 | 23 | 29 | 31 | 37 | 41 | 43 |
| 47 | 53 | 59 | 61 | 67 | 71 | 73 |
| 79 | 83 | 89 | 97 |  |  |  |

**b)Compruebe si los siguientes números son primos.**

* **97:Si**
* **981:No** -> es divisible entre 3
* **1283:Si**
* **14371:No**->es divisible entre 7
* **27773:Si**
* **27777:No**->es divisible por 3
* **30011:Si**

**c)Encuentre los primos que hay en los siguientes intervalos:**

* **[500,550]:** 503,509,521,523,541,547
* **[5000,5050]:**5003, 5009, 5011, 5021, 5023, 5039
* **[50000,50050]:**Ninguno

### Apartado 2: Modularidad

**a)Encuentre los siguientes restos:**

* **487 mod 13**->6
* **12532 mod 493**->207
* **8440 mod 97**->1
* **955 mod 15**->10
* **5202 mod 867**->0
* **31551 mod 123**->63
* **2001 mod 77**->76
* **1997 mod 19**->2

### Apartado 3: Máximo común Divisor

**a)Encuentre el Máximo Común Divisor (mcd) entre:**

* **mcd (35,16)**->1
* **mcd (2488,390)**->2
* **mcd (186,21)** ->3
* **mcd (448,196)** ->4
* **mcd (599,131)** ->1
* **mcd (1573,913)** ->11
* **mcd (1350,1005)** ->15
* **mcd (2488,392)** ->8

### Apartado 4: Conjunto reducido de restos

**a) Encuentre el Conjunto Reducido de Restos CRR, de los cuerpos que se indican:**

#### **CRR (4)** –> **(2)** (click en el desplegable de la izquierda para ver el conjunto)

1,3

#### **CRR (6)** –> **(2)** (click en el desplegable de la izquierda para ver el conjunto)

1,5

#### **CRR (7)** –> **(6)** (click en el desplegable de la izquierda para ver el conjunto)

1,2,3,4,5,6

#### **CRR (9)** –> **(6)** (click en el desplegable de la izquierda para ver el conjunto)

1,2,4,5,7,8

#### **CRR (74)** –> **(36)** (click en el desplegable de la izquierda para ver el conjunto)

1,3,5,7,9,11,13,1517,19,21,23,25,27,29,31,33,35,39,41,43,45,47,49,51,53,55,57,59,61,63,65,67,69,71,73

#### **CRR (100)** –> **(50)** (click en el desplegable de la izquierda para ver el conjunto)

1,3,7,9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 49, 51, 53, 57, 59, 61, 63, 67, 69, 71, 73, 77, 79, 81, 83, 87, 89, 91, 93, 97, 99

#### **CRR (1001)** –> **(720)** (click en el desplegable de la izquierda para ver el conjunto)

1 , 2 , 3 , 4 , 5 , 6 , 8 , 9 , 10 , 12 , 15 , 16 , 17 , 18 , 19 , 20 , 23 , 24 , 25 , 27 , 29 , 30 , 31 , 32 , 34 , 36 , 37 , 38 , 40 , 41 , 43 , 45 , 46 , 47 , 48 , 50 , 51 , 53 , 54 , 57 , 58 , 59 , 60 , 61 , 62 , 64 , 67 , 68 , 69 , 71 , 72 , 73 , 74 , 75 , 76 , 79 , 80 , 81 , 82 , 83 , 85 , 86 , 87 , 89 , 90 , 92 , 93 , 94 , 95 , 96 , 97 , 100 , 101 , 102 , 103 , 106 , 107 , 108 , 109 , 111 , 113 , 114 , 115 , 116 , 118 , 120 , 122 , 123 , 124 , 125 , 127 , 128 , 129 , 131 , 134 , 135 , 136 , 137 , 138 , 139 , 141 , 142 , 144 , 145 , 146 , 148 , 149 , 150 , 151 , 152 , 153 , 155 , 157 , 158 , 159 , 160 , 162 , 163 , 164 , 166 , 167 , 170 , 171 , 172 , 173 , 174 , 177 , 178 , 179 , 180 , 181 , 183 , 184 , 185 , 186 , 188 , 190 , 191 , 192 , 193 , 194 , 197 , 199 , 200 , 201 , 202 , 204 , 205 , 206 , 207 , 211 , 212 , 213 , 214 , 215 , 216 , 218 , 219 , 222 , 223 , 225 , 226 , 227 , 228 , 229 , 230 , 232 , 233 , 235 , 236 , 237 , 239 , 240 , 241 , 243 , 244 , 246 , 248 , 249 , 250 , 251 , 254 , 255 , 256 , 257 , 258 , 261 , 262 , 263 , 265 , 267 , 268 , 269 , 270 , 271 , 272 , 274 , 276 , 277 , 278 , 279 , 281 , 282 , 283 , 284 , 285 , 288 , 289 , 290 , 291 , 292 , 293 , 295 , 296 , 298 , 300 , 302 , 303 , 304 , 305 , 306 , 307 , 309 , 310 , 311 , 313 , 314 , 316 , 317 , 318 , 320 , 321 , 323 , 324 , 326 , 327 , 328 , 331 , 332 , 333 , 334 , 335 , 337 , 339 , 340 , 342 , 344 , 345 , 346 , 347 , 348 , 349 , 353 , 354 , 355 , 356 , 358 , 359 , 360 , 361 , 362 , 365 , 366 , 367 , 368 , 369 , 370 , 372 , 373 , 375 , 376 , 379 , 380 , 381 , 382 , 383 , 384 , 386 , 387 , 388 , 389 , 391 , 393 , 394 , 395 , 397 , 398 , 400 , 401 , 402 , 404 , 405 , 408 , 409 , 410 , 411 , 412 , 414 , 415 , 417 , 419 , 421 , 422 , 423 , 424 , 425 , 426 , 428 , 430 , 431 , 432 , 433 , 435 , 436 , 437 , 438 , 439 , 443 , 444 , 445 , 446 , 447 , 449 , 450 , 452 , 453 , 454 , 456 , 457 , 458 , 459 , 460 , 461 , 463 , 464 , 465 , 466 , 467 , 470 , 471 , 472 , 474 , 475 , 477 , 478 , 479 , 480 , 482 , 485 , 486 , 487 , 488 , 489 , 491 , 492 , 493 , 496 , 498 , 499 , 500 , 501 , 502 , 503 , 505 , 508 , 509 , 510 , 512 , 513 , 514 , 515 , 516 , 519 , 521 , 522 , 523 , 524 , 526 , 527 , 529 , 530 , 531 , 534 , 535 , 536 , 537 , 538 , 540 , 541 , 542 , 543 , 544 , 545 , 547 , 548 , 549 , 551 , 552 , 554 , 555 , 556 , 557 , 558 , 562 , 563 , 564 , 565 , 566 , 568 , 569 , 570 , 571 , 573 , 575 , 576 , 577 , 578 , 579 , 580 , 582 , 584 , 586 , 587 , 589 , 590 , 591 , 592 , 593 , 596 , 597 , 599 , 600 , 601 , 603 , 604 , 606 , 607 , 608 , 610 , 612 , 613 , 614 , 615 , 617 , 618 , 619 , 620 , 621 , 622 , 625 , 626 , 628 , 629 , 631 , 632 , 633 , 634 , 635 , 636 , 639 , 640 , 641 , 642 , 643 , 645 , 646 , 647 , 648 , 652 , 653 , 654 , 655 , 656 , 657 , 659 , 661 , 662 , 664 , 666 , 667 , 668 , 669 , 670 , 673 , 674 , 675 , 677 , 678 , 680 , 681 , 683 , 684 , 685 , 687 , 688 , 690 , 691 , 692 , 694 , 695 , 696 , 697 , 698 , 699 , 701 , 703 , 705 , 706 , 708 , 709 , 710 , 711 , 712 , 713 , 716 , 717 , 718 , 719 , 720 , 722 , 723 , 724 , 725 , 727 , 729 , 730 , 731 , 732 , 733 , 734 , 736 , 738 , 739 , 740 , 743 , 744 , 745 , 746 , 747 , 750 , 751 , 752 , 753 , 755 , 757 , 758 , 760 , 761 , 762 , 764 , 765 , 766 , 768 , 769 , 771 , 772 , 773 , 774 , 775 , 776 , 778 , 779 , 782 , 783 , 785 , 786 , 787 , 788 , 789 , 790 , 794 , 795 , 796 , 797 , 799 , 800 , 801 , 802 , 804 , 807 , 808 , 809 , 810 , 811 , 813 , 815 , 816 , 817 , 818 , 820 , 821 , 822 , 823 , 824 , 827 , 828 , 829 , 830 , 831 , 834 , 835 , 837 , 838 , 839 , 841 , 842 , 843 , 844 , 846 , 848 , 849 , 850 , 851 , 852 , 853 , 855 , 856 , 857 , 859 , 860 , 862 , 863 , 864 , 865 , 866 , 867 , 870 , 872 , 873 , 874 , 876 , 877 , 878 , 879 , 881 , 883 , 885 , 886 , 887 , 888 , 890 , 892 , 893 , 894 , 895 , 898 , 899 , 900 , 901 , 904 , 905 , 906 , 907 , 908 , 909 , 911 , 912 , 914 , 915 , 916 , 918 , 919 , 920 , 921 , 922 , 925 , 926 , 927 , 928 , 929 , 930 , 932 , 933 , 934 , 937 , 939 , 940 , 941 , 942 , 943 , 944 , 947 , 948 , 950 , 951 , 953 , 954 , 955 , 956 , 958 , 960 , 961 , 963 , 964 , 965 , 967 , 969 , 970 , 971 , 972 , 974 , 976 , 977 , 978 , 981 , 982 , 983 , 984 , 985 , 986 , 989 , 991 , 992 , 993 , 995 , 996 , 997 , 998 , 999 , 1.000 ,

#### **CRR (1213)** –> **(1212)** (click en el desplegable de la izquierda para ver el conjunto)

1 , 2 , 3 , 4 , 5 , 6 , 7 , 8 , 9 , 10 , 11 , 12 , 13 , 14 , 15 , 16 , 17 , 18 , 19 , 20 , 21 , 22 , 23 , 24 , 25 , 26 , 27 , 28 , 29 , 30 , 31 , 32 , 33 , 34 , 35 , 36 , 37 , 38 , 39 , 40 , 41 , 42 , 43 , 44 , 45 , 46 , 47 , 48 , 49 , 50 , 51 , 52 , 53 , 54 , 55 , 56 , 57 , 58 , 59 , 60 , 61 , 62 , 63 , 64 , 65 , 66 , 67 , 68 , 69 , 70 , 71 , 72 , 73 , 74 , 75 , 76 , 77 , 78 , 79 , 80 , 81 , 82 , 83 , 84 , 85 , 86 , 87 , 88 , 89 , 90 , 91 , 92 , 93 , 94 , 95 , 96 , 97 , 98 , 99 , 100 , 101 , 102 , 103 , 104 , 105 , 106 , 107 , 108 , 109 , 110 , 111 , 112 , 113 , 114 , 115 , 116 , 117 , 118 , 119 , 120 , 121 , 122 , 123 , 124 , 125 , 126 , 127 , 128 , 129 , 130 , 131 , 132 , 133 , 134 , 135 , 136 , 137 , 138 , 139 , 140 , 141 , 142 , 143 , 144 , 145 , 146 , 147 , 148 , 149 , 150 , 151 , 152 , 153 , 154 , 155 , 156 , 157 , 158 , 159 , 160 , 161 , 162 , 163 , 164 , 165 , 166 , 167 , 168 , 169 , 170 , 171 , 172 , 173 , 174 , 175 , 176 , 177 , 178 , 179 , 180 , 181 , 182 , 183 , 184 , 185 , 186 , 187 , 188 , 189 , 190 , 191 , 192 , 193 , 194 , 195 , 196 , 197 , 198 , 199 , 200 , 201 , 202 , 203 , 204 , 205 , 206 , 207 , 208 , 209 , 210 , 211 , 212 , 213 , 214 , 215 , 216 , 217 , 218 , 219 , 220 , 221 , 222 , 223 , 224 , 225 , 226 , 227 , 228 , 229 , 230 , 231 , 232 , 233 , 234 , 235 , 236 , 237 , 238 , 239 , 240 , 241 , 242 , 243 , 244 , 245 , 246 , 247 , 248 , 249 , 250 , 251 , 252 , 253 , 254 , 255 , 256 , 257 , 258 , 259 , 260 , 261 , 262 , 263 , 264 , 265 , 266 , 267 , 268 , 269 , 270 , 271 , 272 , 273 , 274 , 275 , 276 , 277 , 278 , 279 , 280 , 281 , 282 , 283 , 284 , 285 , 286 , 287 , 288 , 289 , 290 , 291 , 292 , 293 , 294 , 295 , 296 , 297 , 298 , 299 , 300 , 301 , 302 , 303 , 304 , 305 , 306 , 307 , 308 , 309 , 310 , 311 , 312 , 313 , 314 , 315 , 316 , 317 , 318 , 319 , 320 , 321 , 322 , 323 , 324 , 325 , 326 , 327 , 328 , 329 , 330 , 331 , 332 , 333 , 334 , 335 , 336 , 337 , 338 , 339 , 340 , 341 , 342 , 343 , 344 , 345 , 346 , 347 , 348 , 349 , 350 , 351 , 352 , 353 , 354 , 355 , 356 , 357 , 358 , 359 , 360 , 361 , 362 , 363 , 364 , 365 , 366 , 367 , 368 , 369 , 370 , 371 , 372 , 373 , 374 , 375 , 376 , 377 , 378 , 379 , 380 , 381 , 382 , 383 , 384 , 385 , 386 , 387 , 388 , 389 , 390 , 391 , 392 , 393 , 394 , 395 , 396 , 397 , 398 , 399 , 400 , 401 , 402 , 403 , 404 , 405 , 406 , 407 , 408 , 409 , 410 , 411 , 412 , 413 , 414 , 415 , 416 , 417 , 418 , 419 , 420 , 421 , 422 , 423 , 424 , 425 , 426 , 427 , 428 , 429 , 430 , 431 , 432 , 433 , 434 , 435 , 436 , 437 , 438 , 439 , 440 , 441 , 442 , 443 , 444 , 445 , 446 , 447 , 448 , 449 , 450 , 451 , 452 , 453 , 454 , 455 , 456 , 457 , 458 , 459 , 460 , 461 , 462 , 463 , 464 , 465 , 466 , 467 , 468 , 469 , 470 , 471 , 472 , 473 , 474 , 475 , 476 , 477 , 478 , 479 , 480 , 481 , 482 , 483 , 484 , 485 , 486 , 487 , 488 , 489 , 490 , 491 , 492 , 493 , 494 , 495 , 496 , 497 , 498 , 499 , 500 , 501 , 502 , 503 , 504 , 505 , 506 , 507 , 508 , 509 , 510 , 511 , 512 , 513 , 514 , 515 , 516 , 517 , 518 , 519 , 520 , 521 , 522 , 523 , 524 , 525 , 526 , 527 , 528 , 529 , 530 , 531 , 532 , 533 , 534 , 535 , 536 , 537 , 538 , 539 , 540 , 541 , 542 , 543 , 544 , 545 , 546 , 547 , 548 , 549 , 550 , 551 , 552 , 553 , 554 , 555 , 556 , 557 , 558 , 559 , 560 , 561 , 562 , 563 , 564 , 565 , 566 , 567 , 568 , 569 , 570 , 571 , 572 , 573 , 574 , 575 , 576 , 577 , 578 , 579 , 580 , 581 , 582 , 583 , 584 , 585 , 586 , 587 , 588 , 589 , 590 , 591 , 592 , 593 , 594 , 595 , 596 , 597 , 598 , 599 , 600 , 601 , 602 , 603 , 604 , 605 , 606 , 607 , 608 , 609 , 610 , 611 , 612 , 613 , 614 , 615 , 616 , 617 , 618 , 619 , 620 , 621 , 622 , 623 , 624 , 625 , 626 , 627 , 628 , 629 , 630 , 631 , 632 , 633 , 634 , 635 , 636 , 637 , 638 , 639 , 640 , 641 , 642 , 643 , 644 , 645 , 646 , 647 , 648 , 649 , 650 , 651 , 652 , 653 , 654 , 655 , 656 , 657 , 658 , 659 , 660 , 661 , 662 , 663 , 664 , 665 , 666 , 667 , 668 , 669 , 670 , 671 , 672 , 673 , 674 , 675 , 676 , 677 , 678 , 679 , 680 , 681 , 682 , 683 , 684 , 685 , 686 , 687 , 688 , 689 , 690 , 691 , 692 , 693 , 694 , 695 , 696 , 697 , 698 , 699 , 700 , 701 , 702 , 703 , 704 , 705 , 706 , 707 , 708 , 709 , 710 , 711 , 712 , 713 , 714 , 715 , 716 , 717 , 718 , 719 , 720 , 721 , 722 , 723 , 724 , 725 , 726 , 727 , 728 , 729 , 730 , 731 , 732 , 733 , 734 , 735 , 736 , 737 , 738 , 739 , 740 , 741 , 742 , 743 , 744 , 745 , 746 , 747 , 748 , 749 , 750 , 751 , 752 , 753 , 754 , 755 , 756 , 757 , 758 , 759 , 760 , 761 , 762 , 763 , 764 , 765 , 766 , 767 , 768 , 769 , 770 , 771 , 772 , 773 , 774 , 775 , 776 , 777 , 778 , 779 , 780 , 781 , 782 , 783 , 784 , 785 , 786 , 787 , 788 , 789 , 790 , 791 , 792 , 793 , 794 , 795 , 796 , 797 , 798 , 799 , 800 , 801 , 802 , 803 , 804 , 805 , 806 , 807 , 808 , 809 , 810 , 811 , 812 , 813 , 814 , 815 , 816 , 817 , 818 , 819 , 820 , 821 , 822 , 823 , 824 , 825 , 826 , 827 , 828 , 829 , 830 , 831 , 832 , 833 , 834 , 835 , 836 , 837 , 838 , 839 , 840 , 841 , 842 , 843 , 844 , 845 , 846 , 847 , 848 , 849 , 850 , 851 , 852 , 853 , 854 , 855 , 856 , 857 , 858 , 859 , 860 , 861 , 862 , 863 , 864 , 865 , 866 , 867 , 868 , 869 , 870 , 871 , 872 , 873 , 874 , 875 , 876 , 877 , 878 , 879 , 880 , 881 , 882 , 883 , 884 , 885 , 886 , 887 , 888 , 889 , 890 , 891 , 892 , 893 , 894 , 895 , 896 , 897 , 898 , 899 , 900 , 901 , 902 , 903 , 904 , 905 , 906 , 907 , 908 , 909 , 910 , 911 , 912 , 913 , 914 , 915 , 916 , 917 , 918 , 919 , 920 , 921 , 922 , 923 , 924 , 925 , 926 , 927 , 928 , 929 , 930 , 931 , 932 , 933 , 934 , 935 , 936 , 937 , 938 , 939 , 940 , 941 , 942 , 943 , 944 , 945 , 946 , 947 , 948 , 949 , 950 , 951 , 952 , 953 , 954 , 955 , 956 , 957 , 958 , 959 , 960 , 961 , 962 , 963 , 964 , 965 , 966 , 967 , 968 , 969 , 970 , 971 , 972 , 973 , 974 , 975 , 976 , 977 , 978 , 979 , 980 , 981 , 982 , 983 , 984 , 985 , 986 , 987 , 988 , 989 , 990 , 991 , 992 , 993 , 994 , 995 , 996 , 997 , 998 , 999 , 1.000 , 1.001 , 1.002 , 1.003 , 1.004 , 1.005 , 1.006 , 1.007 , 1.008 , 1.009 , 1.010 , 1.011 , 1.012 , 1.013 , 1.014 , 1.015 , 1.016 , 1.017 , 1.018 , 1.019 , 1.020 , 1.021 , 1.022 , 1.023 , 1.024 , 1.025 , 1.026 , 1.027 , 1.028 , 1.029 , 1.030 , 1.031 , 1.032 , 1.033 , 1.034 , 1.035 , 1.036 , 1.037 , 1.038 , 1.039 , 1.040 , 1.041 , 1.042 , 1.043 , 1.044 , 1.045 , 1.046 , 1.047 , 1.048 , 1.049 , 1.050 , 1.051 , 1.052 , 1.053 , 1.054 , 1.055 , 1.056 , 1.057 , 1.058 , 1.059 , 1.060 , 1.061 , 1.062 , 1.063 , 1.064 , 1.065 , 1.066 , 1.067 , 1.068 , 1.069 , 1.070 , 1.071 , 1.072 , 1.073 , 1.074 , 1.075 , 1.076 , 1.077 , 1.078 , 1.079 , 1.080 , 1.081 , 1.082 , 1.083 , 1.084 , 1.085 , 1.086 , 1.087 , 1.088 , 1.089 , 1.090 , 1.091 , 1.092 , 1.093 , 1.094 , 1.095 , 1.096 , 1.097 , 1.098 , 1.099 , 1.100 , 1.101 , 1.102 , 1.103 , 1.104 , 1.105 , 1.106 , 1.107 , 1.108 , 1.109 , 1.110 , 1.111 , 1.112 , 1.113 , 1.114 , 1.115 , 1.116 , 1.117 , 1.118 , 1.119 , 1.120 , 1.121 , 1.122 , 1.123 , 1.124 , 1.125 , 1.126 , 1.127 , 1.128 , 1.129 , 1.130 , 1.131 , 1.132 , 1.133 , 1.134 , 1.135 , 1.136 , 1.137 , 1.138 , 1.139 , 1.140 , 1.141 , 1.142 , 1.143 , 1.144 , 1.145 , 1.146 , 1.147 , 1.148 , 1.149 , 1.150 , 1.151 , 1.152 , 1.153 , 1.154 , 1.155 , 1.156 , 1.157 , 1.158 , 1.159 , 1.160 , 1.161 , 1.162 , 1.163 , 1.164 , 1.165 , 1.166 , 1.167 , 1.168 , 1.169 , 1.170 , 1.171 , 1.172 , 1.173 , 1.174 , 1.175 , 1.176 , 1.177 , 1.178 , 1.179 , 1.180 , 1.181 , 1.182 , 1.183 , 1.184 , 1.185 , 1.186 , 1.187 , 1.188 , 1.189 , 1.190 , 1.191 , 1.192 , 1.193 , 1.194 , 1.195 , 1.196 , 1.197 , 1.198 , 1.199 , 1.200 , 1.201 , 1.202 , 1.203 , 1.204 , 1.205 , 1.206 , 1.207 , 1.208 , 1.209 , 1.210 , 1.211 , 1.212 ,

### Apartado 5 Indicador de Euler

**a)Encuentre los siguientes Indicadores de Euler:**

* **Φ(1)**->El numero ha de ser mayor que 1
* **Φ(2)** ->1
* **Φ(4)** ->2
* **Φ(6)** ->2
* **Φ(7)** ->6
* **Φ(9)** ->6
* **Φ(74)** ->36
* **Φ(100)** ->40
* **Φ(1001)** ->720
* **Φ(1213)** ->1212

### Apartado 6: Inversos

**a)Encuentre los siguientes inversos:**

* **inv (3,7)**->5
* **inv (7,9)** ->4
* **inv (17, 40)** ->33
* **inv (28,39)** ->7
* **inv (85,166)** ->125
* **inv (150,2999)** ->20
* **inv (1234,4321)** ->3239
* **inv (3311,1133)** ->No existe

### Apartado 7: Exponenciación dentro de un cuerpo

**a)Usando la calculadora de Windows encuentre los siguientes valores:**

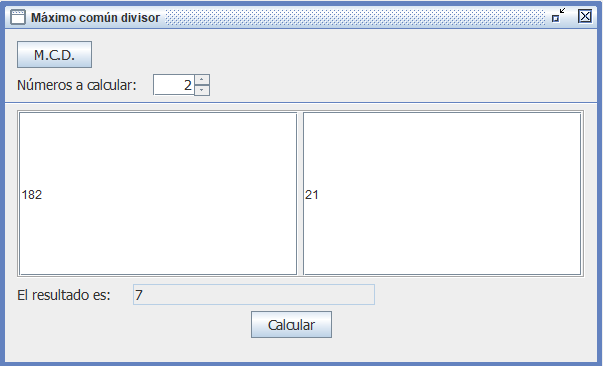
* **59 mod 13**->7
* **210 mod 31**->24
* **198 mod 77**->44
* **39737 mod 141**->116
* **2011 mod 51**->22

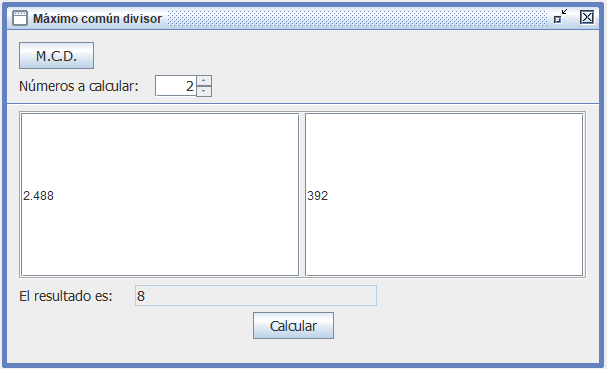
### Informe

**1.¿Qué puede concluir de los valores encontrados en el apartado 1.c?**

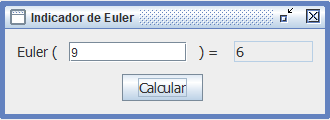
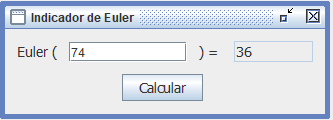
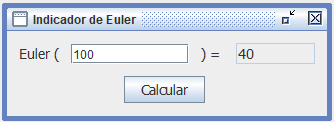
Que cuanto mayores se van haciendo los números, más difícil es encontrar alguno que sea primo: En el intervalo entre 500 y 550 había bastantes, en el intervalo [5000, 5050] había alguno menos, y ya en el ultimo intervalo [50000,50050] no había ninguno.

**2.Calcule y compruebe los valores de mcd (186,21) y mcd (2488,392).**

Mcd(182,21)=7 Mcd(2488,392)=8

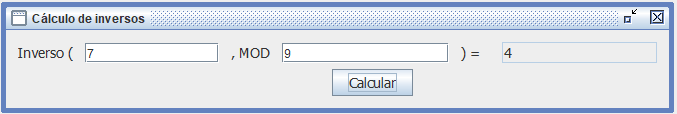


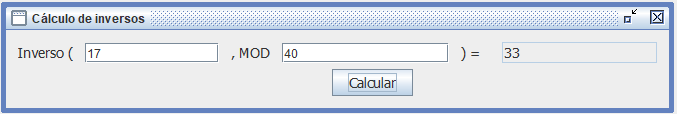
**3.Calcule y compruebe los valores de Φ(9),** **Φ(74) y Φ(100).**

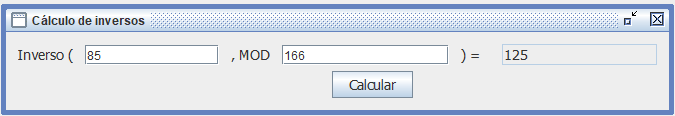
Φ(9)=6 Φ(74)=36 Φ(100)=40

**4.Calcule y compruebe los valores inv (7,9), inv (17,40) e inv (85,166).**

inv (7,9)=4 inv (17,40)=33 inv (85,166)=125







**5.Calcule y compruebe mediante reducción del exponente 198 mod 77.**

Factores de 198-> 2·3·3·11

Factores de 77->7·11

Simplificando nos queda 2 + 4/7

Si multiplicamos 4/7 por 77, nos queda 44, que es el modulo

**6.Mediante la reducción del exponente calcule los valores 39737 mod 141 y 2011 mod 51. ¿Qué puede concluir de estos resultados?.**

Factores de 393737-> 217·19·23·53

Factores de 141->3·47

Aplicando la regla del ejercicio anterior, tenemos que el módulo es: 65

# Criptosistemas clásicos

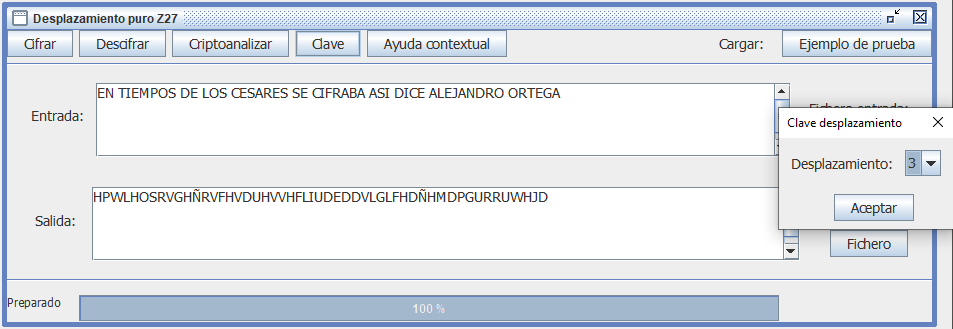
## Cifradores Monoalfabéticos por sustitución: Desplazamiento Puro

### Apartado 1

**a)Cifrar con un desplazamiento b=3 el siguiente mensaje:**

EN TIEMPOS DE LOS CESARES SE CIFRABA ASI DICE <NombreAlumno/s>

Lo cifraremos utilizando la herramienta criptoclasicos, en el apartado criptosistemas nos deja seleccionar este tipo de encriptación:

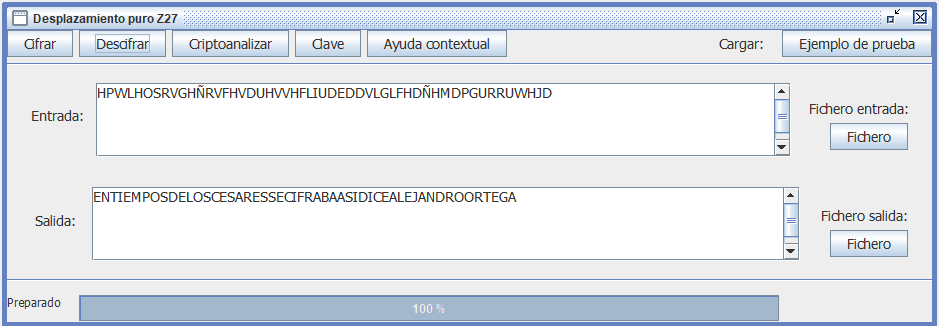


El resultado es:

HPWLHOSRVGHÑRVFHVDUHVVHFLIUDEDDVLGLFHDÑHMDPGURRUWHJD

**b)Descifrar el criptograma obtenido.**

Podemos descifrar dando al botón “descifrar” en la parte superior:

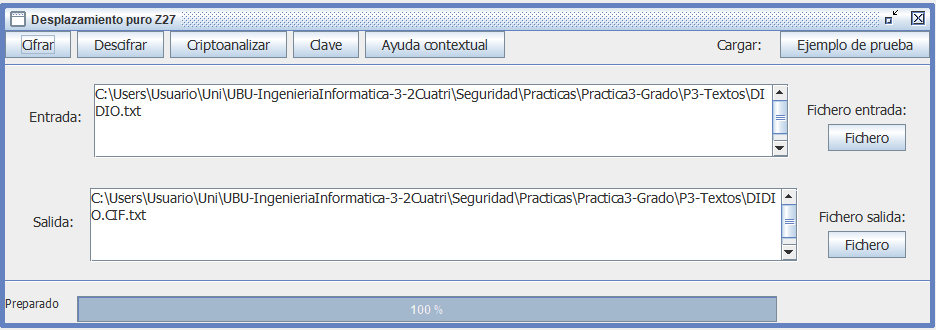


Como podemos observar, Descifra y cifra sin espacios, porque no cuenta como un carácter.

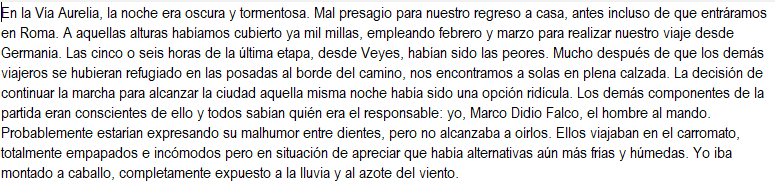
### Apartado 2

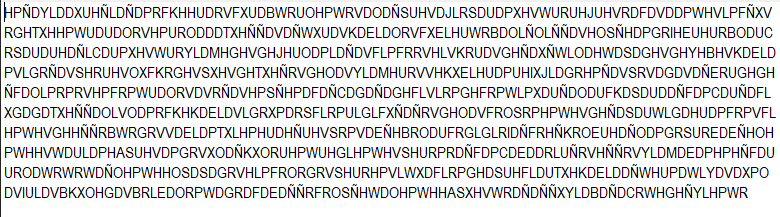
**a)Cifrar con un desplazamiento b=7 el fichero DIDIO.TXT. El fichero de salida se llamará DIDIO.CIF.**

Dentro de la opción comentada anteriormente, nos deja subir un fichero seleccionando la opción “Fichero”

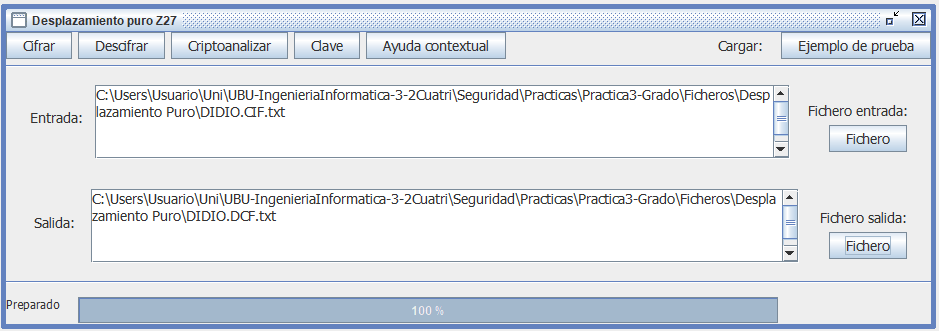


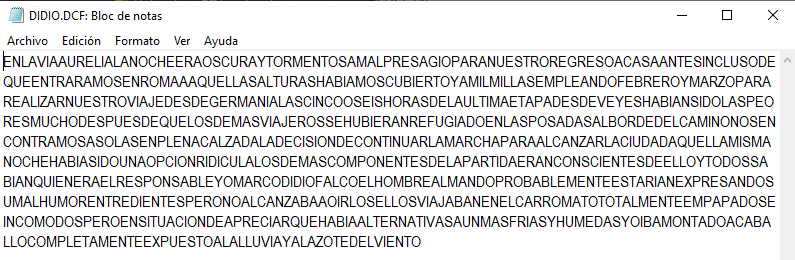
En entrada seleccionamos el path del fichero de entrada, y en salida lo propio con el de salida. Aquí vemos el resultado del cifrado.



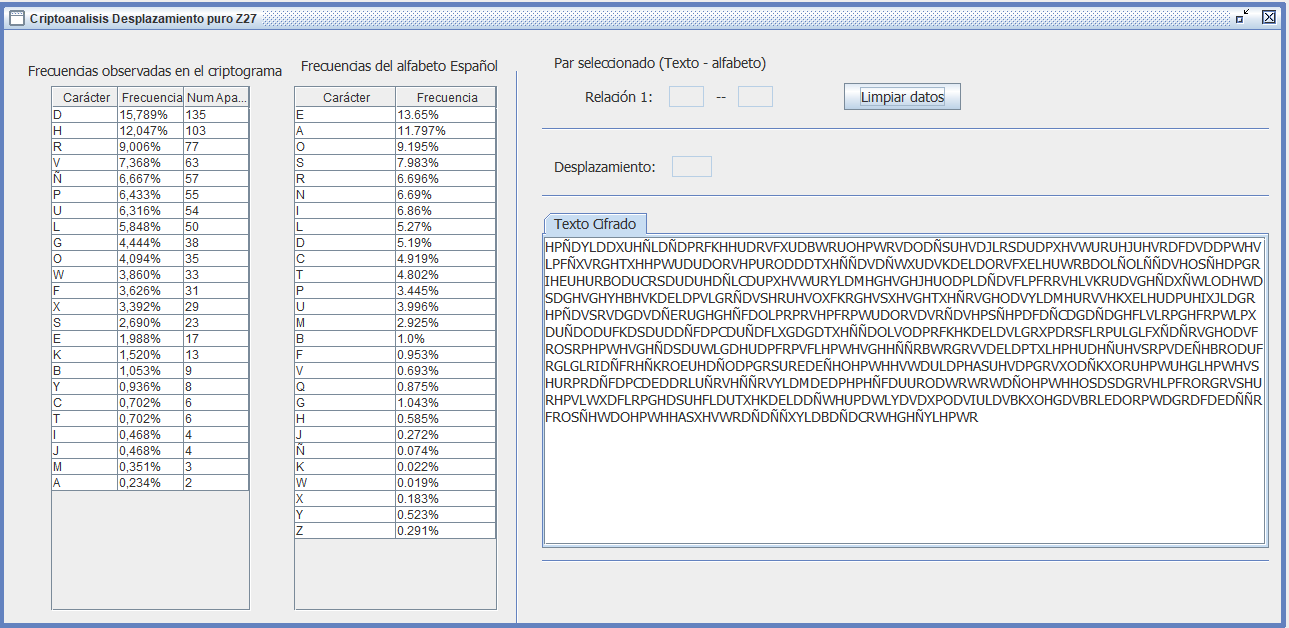
****

**b)Descifrar el fichero DIDIO.CIF, guardándolo como DIDIO.DCF.**

Hacemos la operación inversa:



**c)Criptoanalizar el fichero DIDIO.CIF, guardándolo como DIDIO.CRI.**

Para esto, cargaremos el fichero origen y destino como es habitual, y seleccionaremos la opción “criptoanalizar”. Esto nos proporcionara unas características sobre el fichero criptoanalizado, como las mostradas a continuación:

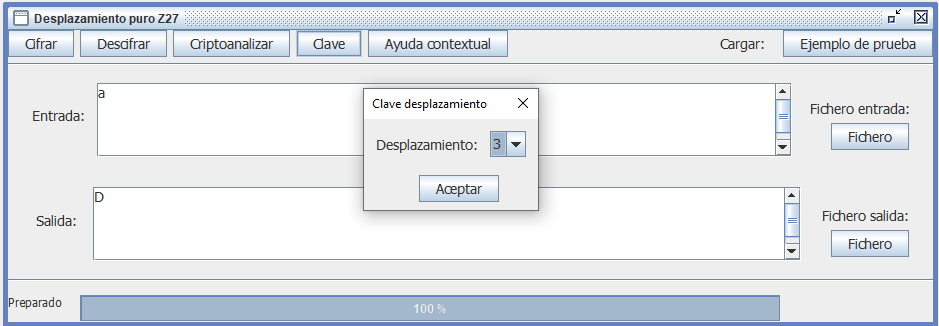
### Informe

**1.¿Qué resultados obtiene si intenta descifrar o atacar un mensaje que ya está en claro?**

La operación de descifrar es la inversa que de cifrar, por lo que si decidimos descifrar un texto en claro, el programa realizara las operaciones pertinentes a cada carácter, obteniendo un mensaje ilegible.

**2.Explique la relación que existe entre el valor de b de cifra y el valor de desplazamiento encontrado en el criptoanálisis.**

El valor b es la cantidad de desplazamientos que se realizan. Así, con un valor b=4, si por ejemplo tenemos una A, la conversión sería A-B-C-D, convirtiéndose en una D.



**3.¿Qué sucede si se cifra con desplazamiento b=31, b=58 y b=-27?**

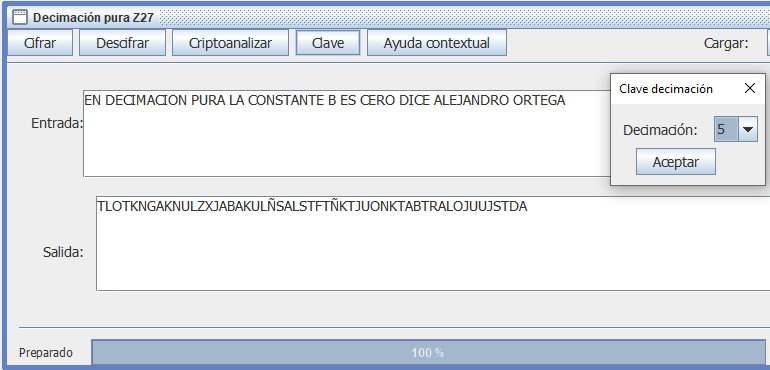
El alfabeto solo tiene 27 caracteres (contando la ñ), por lo que si quisiéramos hacer un desplazamiento de 31, seria un desplazamiento de (31-27) 4. Así, con 58 tendríamos un desplazamiento de (58-27-27) 4. Con -27 tendríamos que hacer la operación contraria, obteniendo un desplazamiento de (27+27) 0, que sería como no cifrarlo.

## Cifradores Monoalfabéticos por sustitución: Decimación Pura

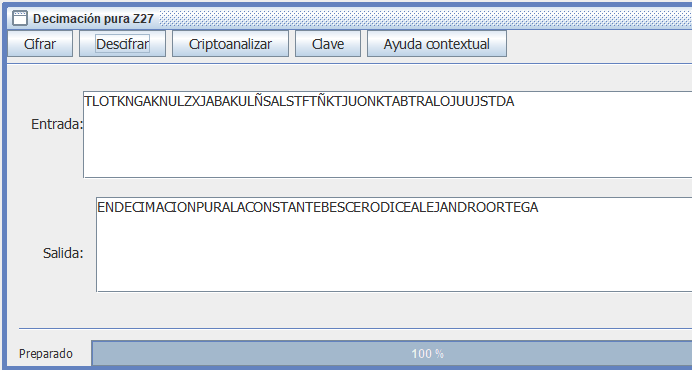
### Apartado 1

**a)Cifrar con un valor de a=5 el siguiente mensaje:**

EN DECIMACIÓN PURA LA CONSTANTE B ES CERO DICE <NombreAlumno/s>.

Para cifrar los pasos son iguales que en el apartado anterior (Desplazamiento Puro), solo que con la herramienta de Decimación pura, que se puede encontrar en l mismo lugar. Por esto, no iremos explicando cada proceso de encriptación ni desencriptación, sino solo se adjuntarán capturas de los resultados.

**b)Descifrar el criptograma obtenido.**

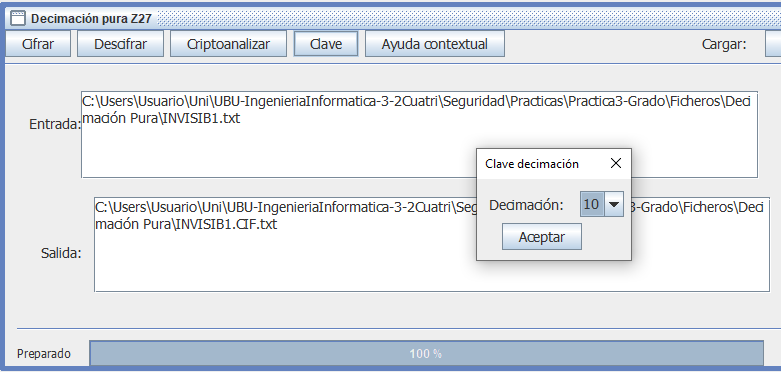
****

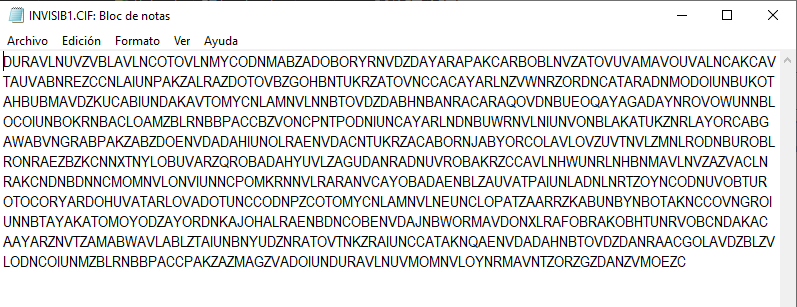
**c)Intente volver a cifrarlo con los valores a=0, a=-6, a=12 y a=1.**

No se puede, porque para poder aplicar este algoritmo, a y el orden del grupo deben de ser primos entre sí. El orden de nuestro grupo es el número de letras (26), por lo que ninguna de las a dadas en el enunciado y 26 son primos entre sí.

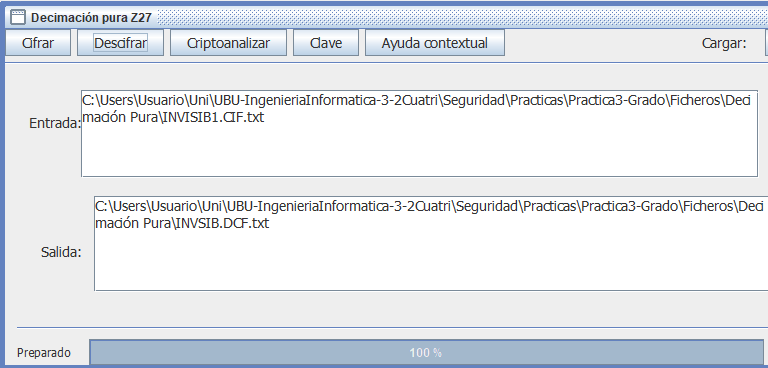
### Apartado 2

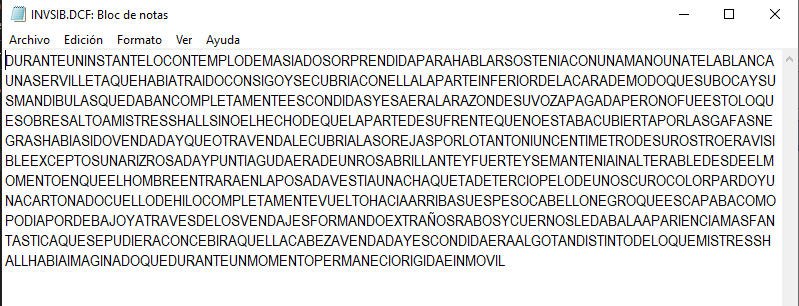
**a)Cifrar con un valor de a=10 el fichero INVISIB1.TXT. El fichero de salida se llamará INVISIB1.CIF.**

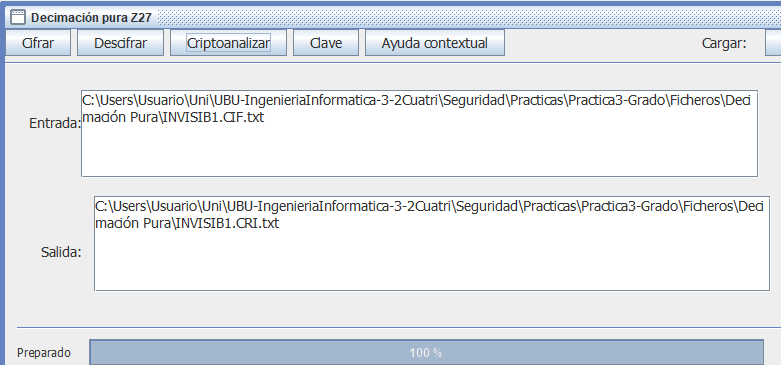
****

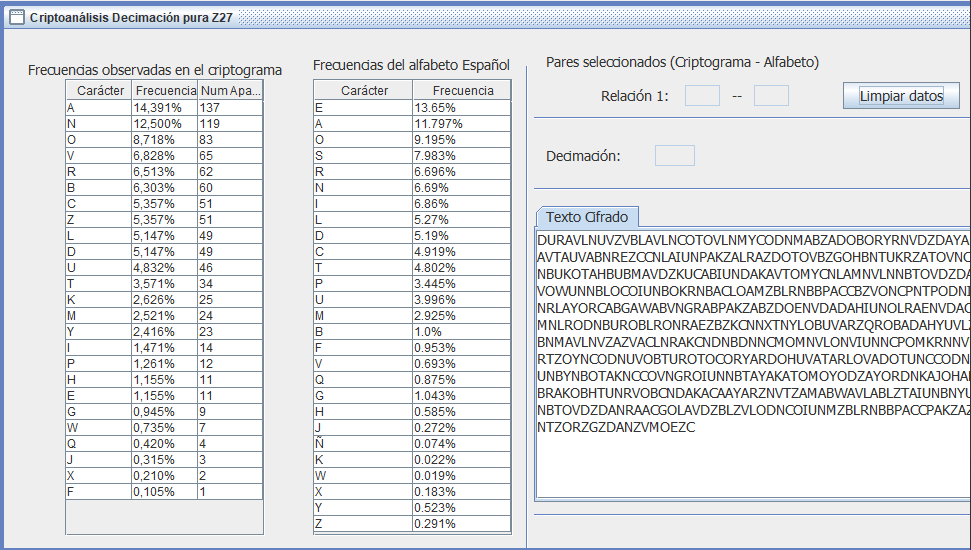
****

**b)Descifrar el fichero INVISIB1.CIF, guardándolo como INVISIB1.DCF.**

****

****

**c)Criptoanalizar el fichero INVISIB1.CIF, guardándolo como INVISIB1.CRI.**

****el resultado nos proporcionara unas características sobre el fichero criptoanalizado, como las mostradas a continuación:

### Informe

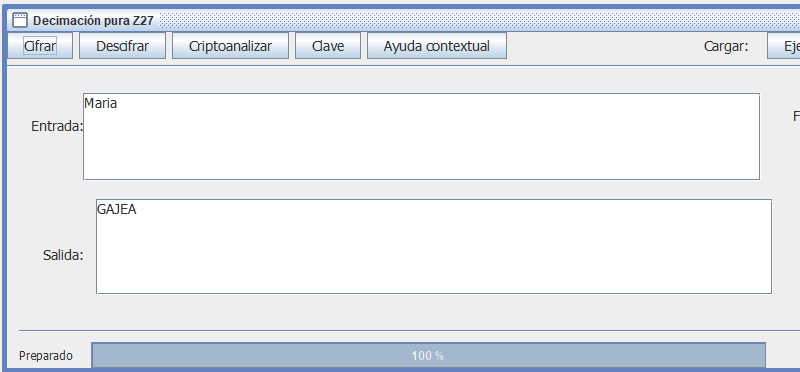
**1.Indique qué ha sucedido al intentar cifrar el mensaje en el apartado 1c. ¿Cuál es el motivo de que no lo permita el software?**

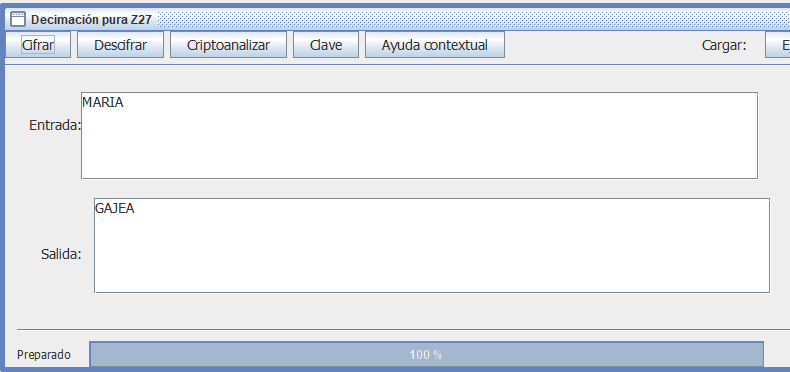
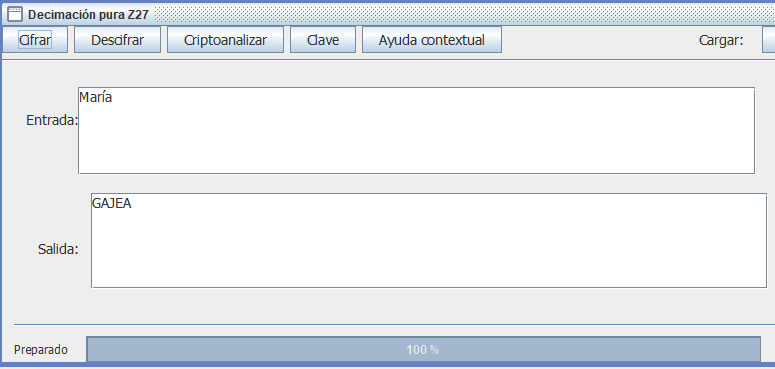
El software no podía cifrarlo, por lo anteriormente descrito:

No se puede, porque para poder aplicar este algoritmo, a y el orden del grupo deben de ser primos entre sí. El orden de nuestro grupo es el número de letras (27), por lo que ninguna de las a dadas en el enunciado y 27 son primos entre sí.

**2.Si cifra con a=14 los mensajes M1=MARIA, M2=María y M3=María, ¿los criptogramas son iguales o distintos? ¿Por qué?**

M1-> GAJEA M2-> GAJEA M3->CAJEA



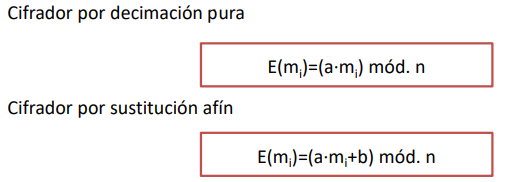


Al ser las mismas letras, lo cifra igual, porque no distingue entre mayúsculas, minúsculas y caracteres con tilde. Esto es cosa del programa, pero podríamos añadir estos caracteres a la “pool” de posibles caracteres, por lo que nuestro orden del grupo crecería, y podríamos hacer cifrados mas potentes, pero eso es cosa del software.

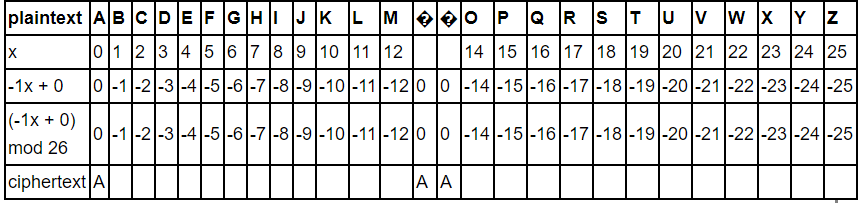
**3.Si cifra el mensaje M=ABCDEFGHIJKLMÑOPQRSTUVWXYZ con el factor de Decimación a=-1, ¿qué obtiene como salida?**

En el programa no deja cifrar con a=-1, por lo que no se puede cifrar.

Sin embargo, podemos hacer el truco usando el cifrado de sustitución afín, las diferencias entre las fórmulas son las siguientes:



Podemos observar que el cifrado afín es una mezcla entre desplazamiento puro y Decimación pura. Poniendo la constante b a 0, y la constante a=-1, obtenemos:



Si consideramos que las letras en el abecedario “dan la vuelta”, tendríamos:

AZYXWVUTSRQPOÑNMLKJIHGFEDCB

**4.¿Cuántas opciones para romper el criptograma tiene de acuerdo a la pantalla que le muestra la aplicación en el apartado 2.c? ¿Cuál sería el método óptimo en función del tiempo necesario para romper la cifra?**

El programa no da ninguna opción

## Cifradores polialfabeticos por sustitución: Cifradores Periódicos

### Cifrado de Vigenère

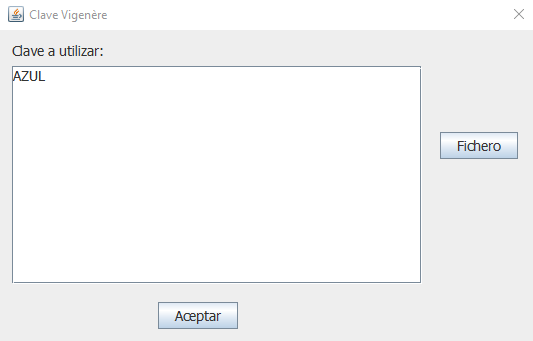
##### Apartado 1

**a)Cifrar con clave K = AZUL el siguiente mensaje:**

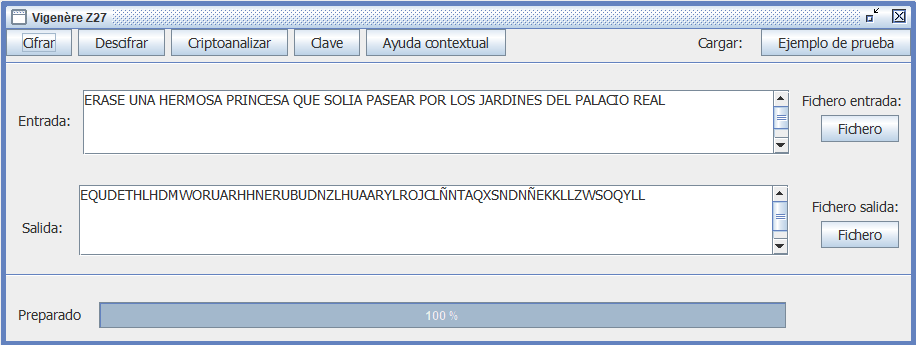
**ERASE UNA HERMOSA PRINCESA QUE SOLÍA PASEAR POR LOS JARDINES DEL PALACIO REAL.**

En el mismo apartado donde estaban las anteriores herramientas, encontraremos la del cifrado de Vigènere.

El funcionamiento es similar a las anteriores, per en esta ocasión, al seleccionar la clave, nos deja tanto escribirla, como seleccionarla de un fichero.

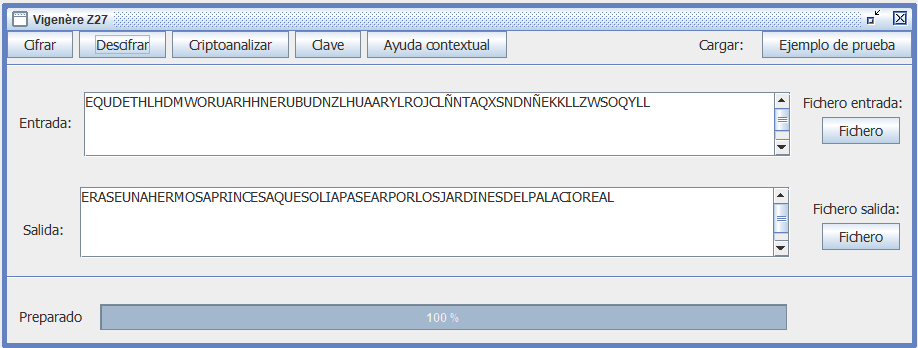


El resultado es el siguiente:



**b)Descifrar el criptograma obtenido.**

Realizando la operación inversa, obtenemos:

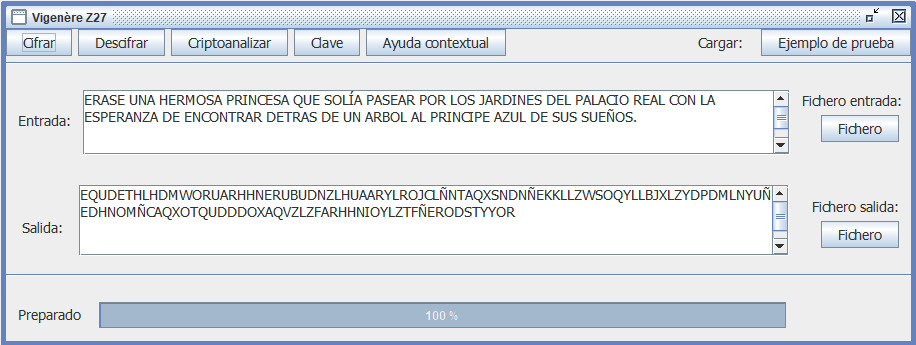


**c)Intente romper la cifra obtenida en el punto anterior.**

No se puede, porque no hay repeticiones

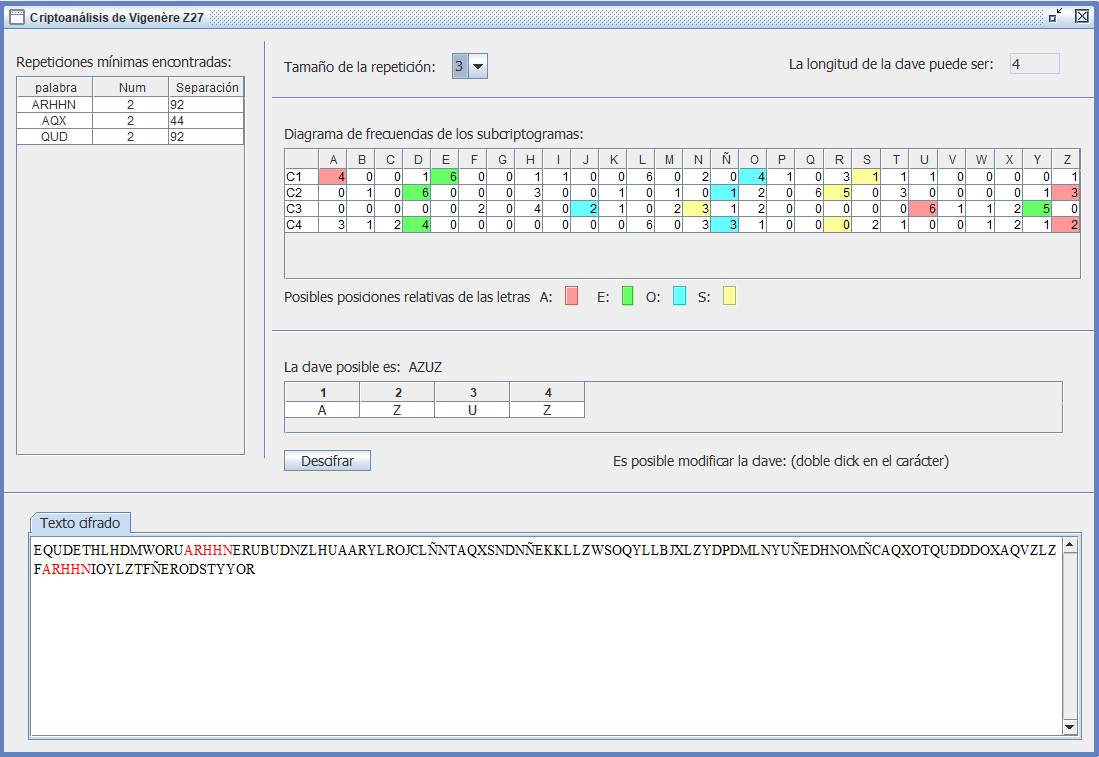
**d)Con la misma clave cifrar el mensaje anterior modificado como se indica:**

**ERASE UNA HERMOSA PRINCESA QUE SOLÍA PASEAR POR LOS JARDINES DEL PALACIO REAL CON LA ESPERANZA DE ENCONTRAR DETRAS DE UN ARBOL AL PRINCIPE AZUL DE SUS SUEÑOS.**

****

**e)Criptoanalizar el texto cifrado obtenido en el punto anterior.**

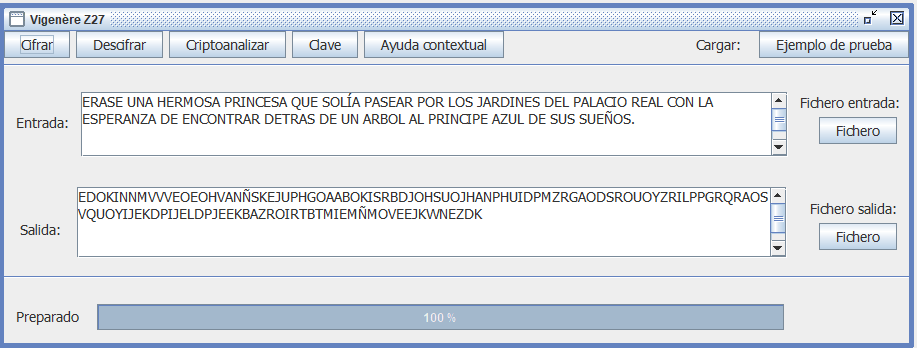
Seleccionando el apartado de criptoanalizar, obtenemos lo siguiente:



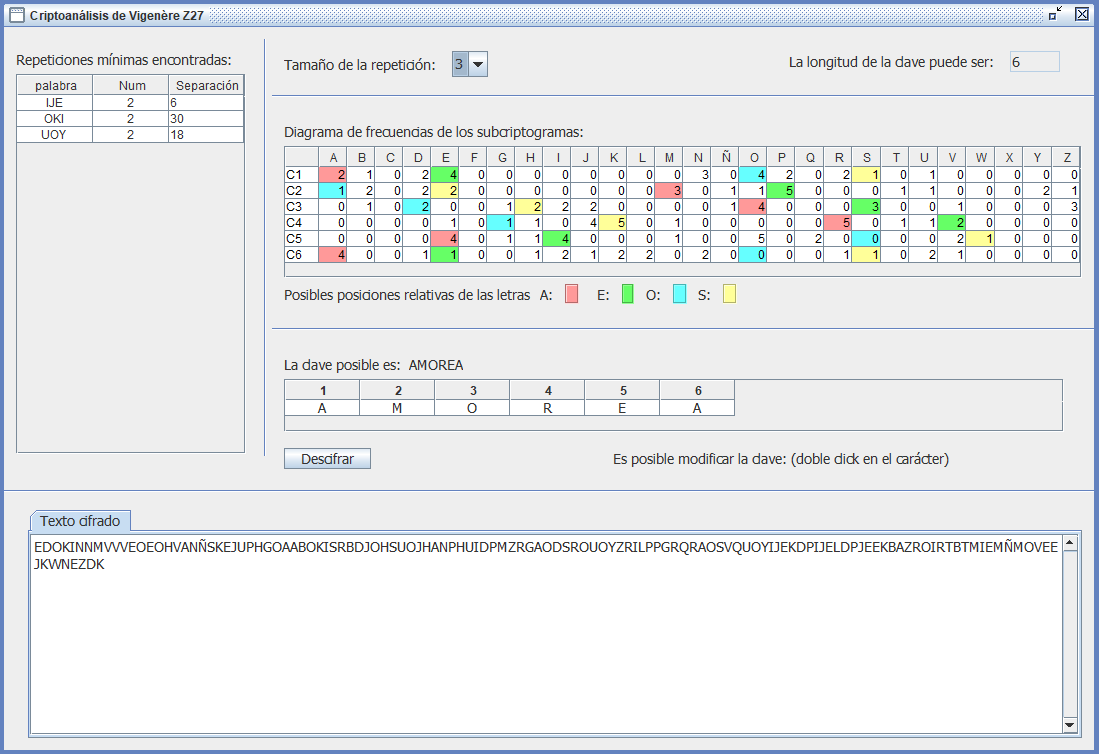
Si seleccionamos que nos muestre las repeticiones de tamaño 3, podemos inferir la clave, que en efecto, es AZUL

**f)Repetir la cifra y el criptoanálisis del mensaje del punto 1.d) usando ahora la clave K = AMORES.**

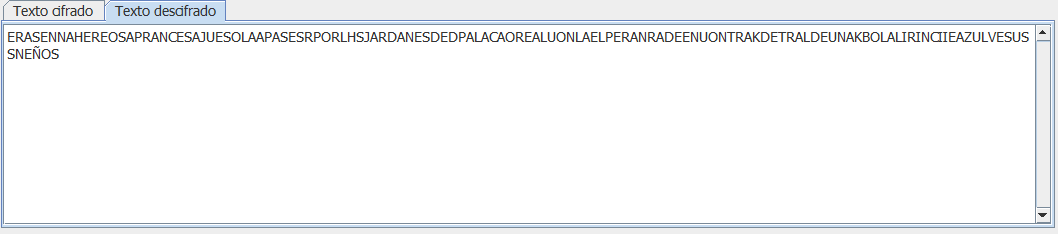
Primero, ciframos el mensaje con la nueva clave:



Ahora, procederemos a su criptoanálisis:



Como podemos observar, la clave que infiere al tener en cuenta todas las repeticiones de tamaño 3 es muy similar. Si le damos a descifrar el mensaje con esa clave, obtenemos lo siguiente:

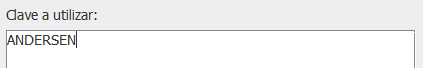


No es exactamente el mismo texto pero se puede deducir de él el texto original.

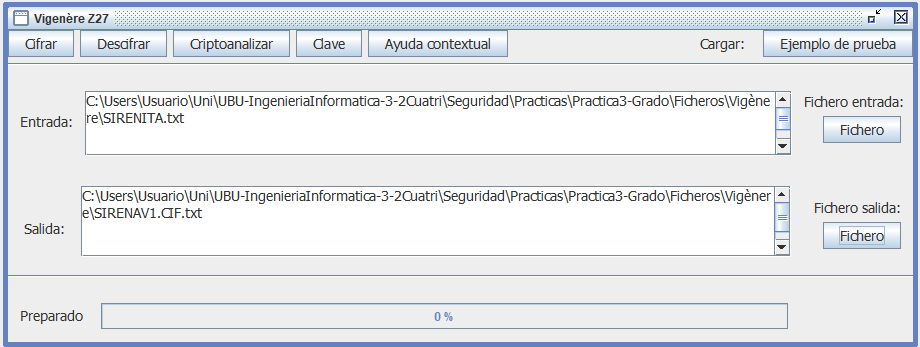
##### Apartado 2

**a)Cifrar con la clave K = ANDERSEN el fichero SIRENITA.TXT. El fichero de salida se llamará SIRENAV1.CIF.**

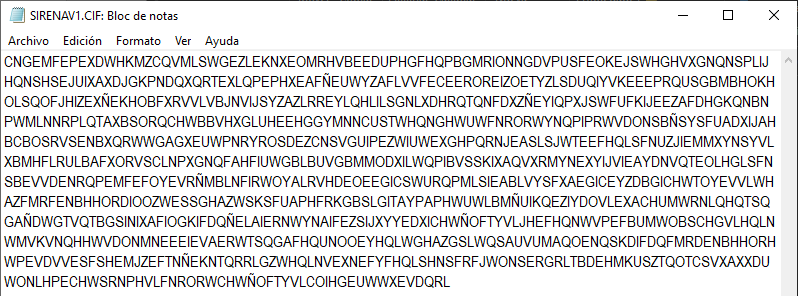
Primero seleccionamos la clave:



Y posteriormente, ciframos el archivo como se muestra a continuación:

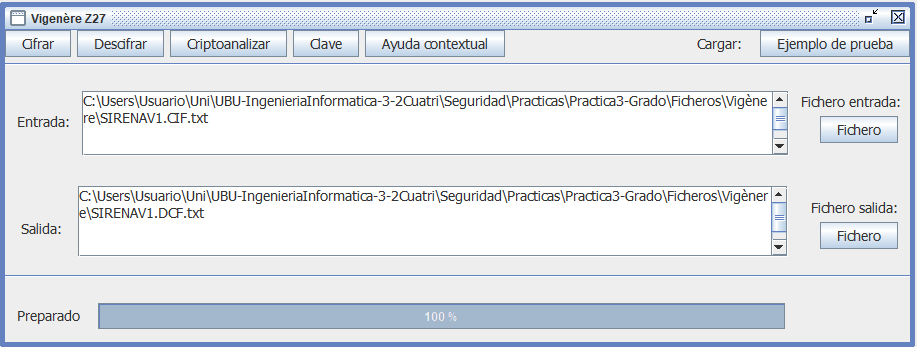


Obteniendo el siguiente resultado:



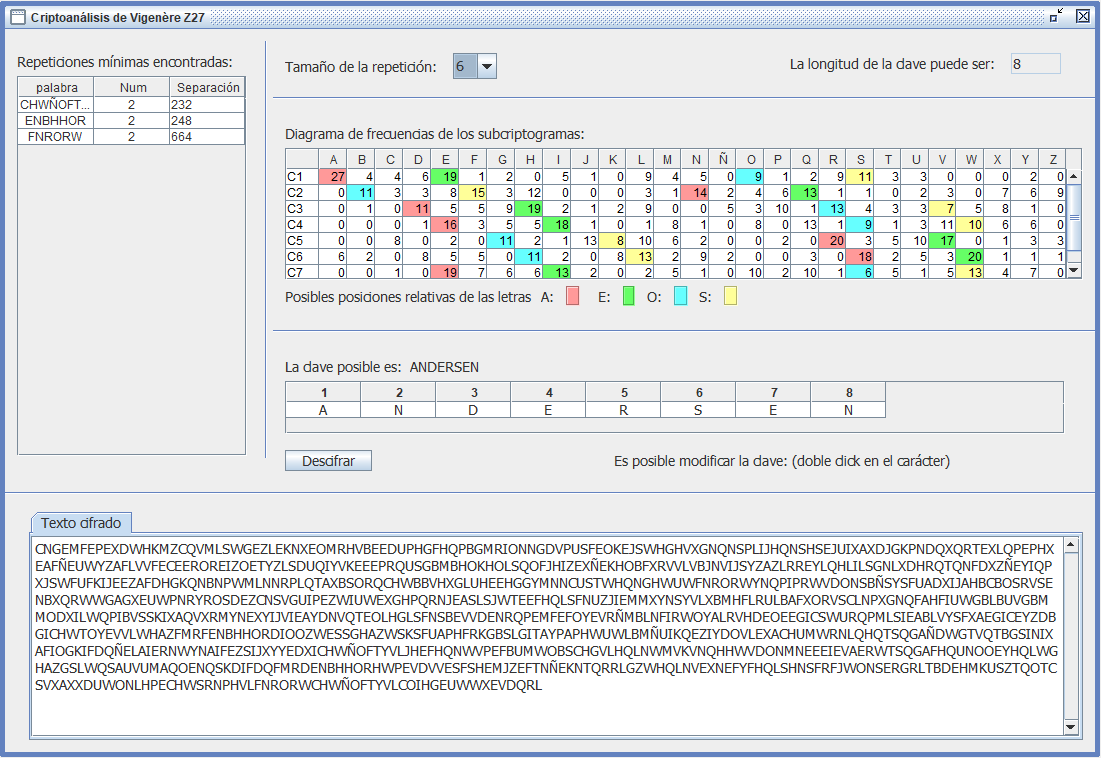
**b)Descifrar el fichero SIRENAV1.CIF, guardándolo como SIRENAV1.DCF.**

Realizamos la operación inversa:

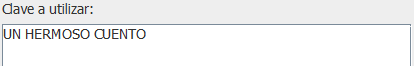


**c)Criptoanalizar el fichero SIRENAV1.CIF, guardándolo como SIRENAV1.CRI.**

Al criptoanalizarlo, podemos observar que teniendo en cuenta las repeticiones de 8 caracteres, podemos ya inferir la clave:

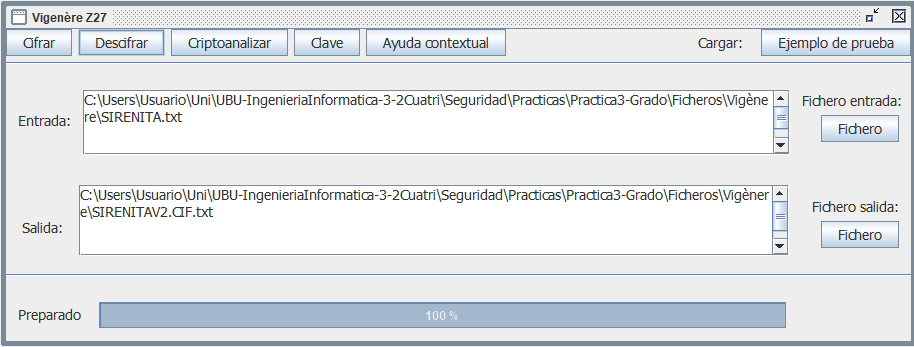


**d)Repetir los puntos a), b) y c) usando como clave K = UN HERMOSO CUENTO. Los ficheros de salida serán SIRENAV2.CIF, SIRENAV2.DCF y SIRENAV2.CRI.**

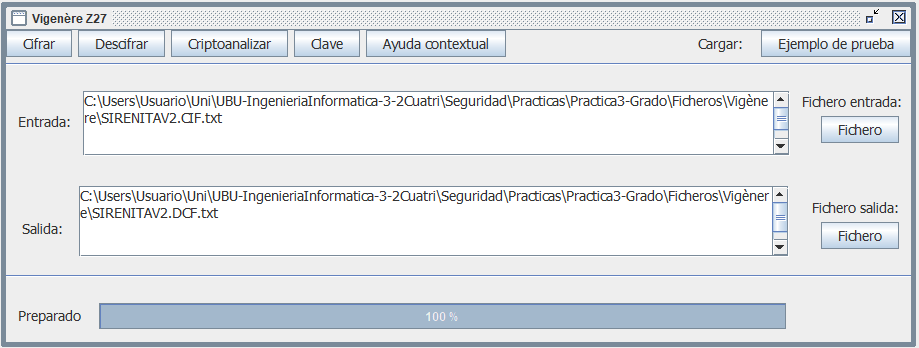
****

Puesto que el proceso es el mismo, no se explicará, sino que se adjuntaran directamente las capturas:

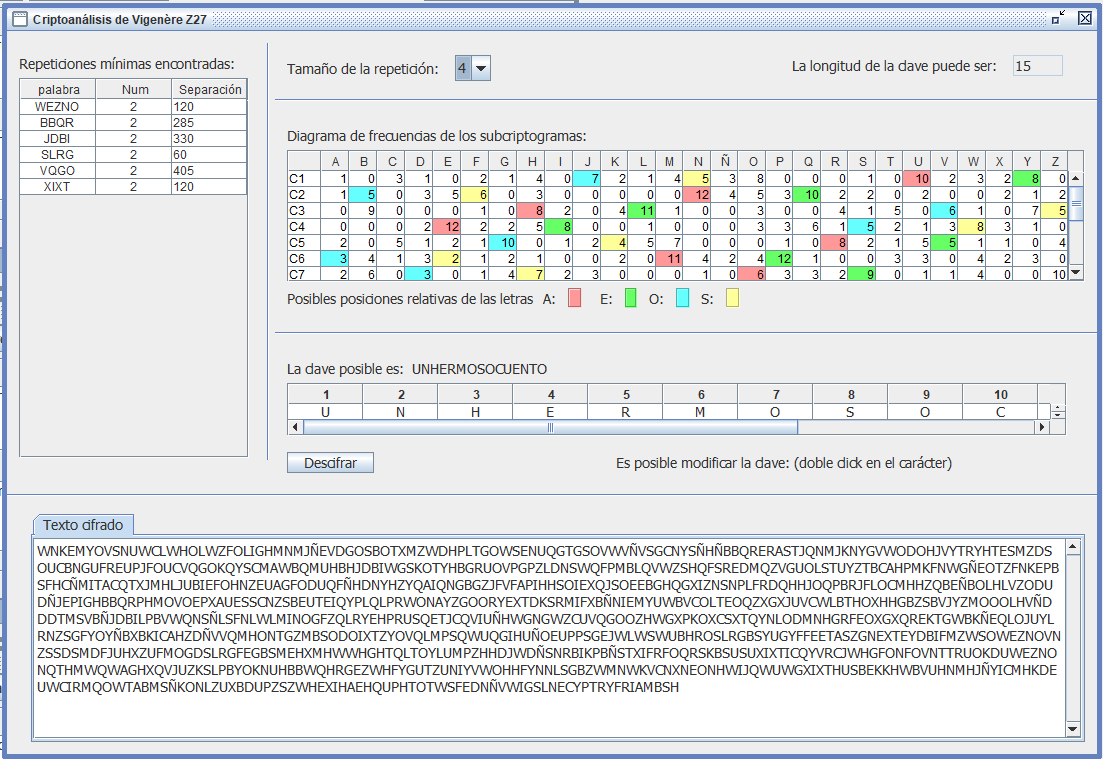
Cifrado:



Descifrado:



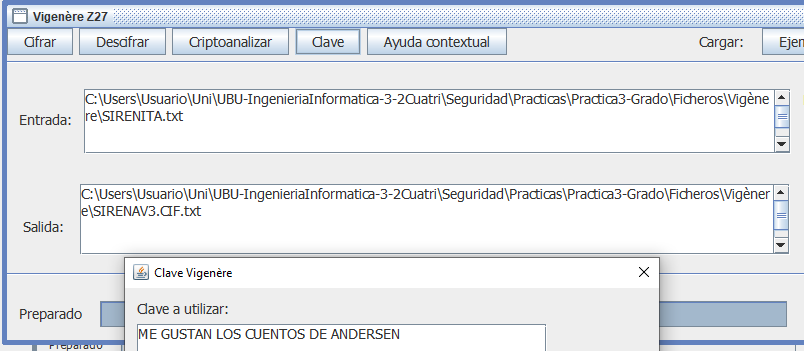
Criptoanálisis:

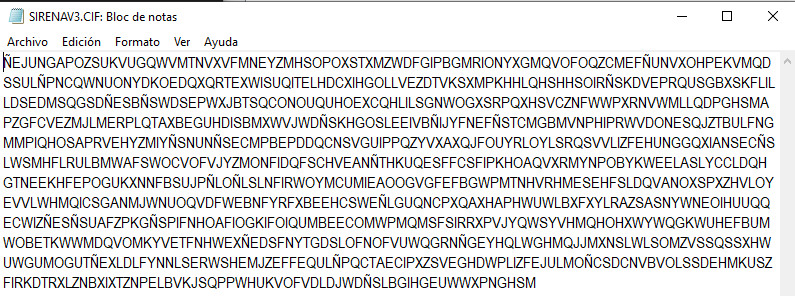


Se infiere la contraseña fijándonos en las repeticiones de 4 caracteres.

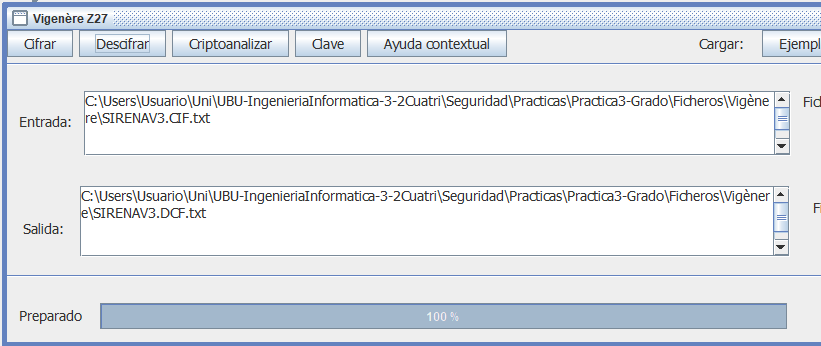
**e)Repetir el punto anterior usando ahora como clave K = ME GUSTAN LOS CUENTOS DE ANDERSEN. Los ficheros de salida serán SIRENAV3.CIF, SIRENAV3.DCF y SIRENAV3.CRI.**

Cifrado

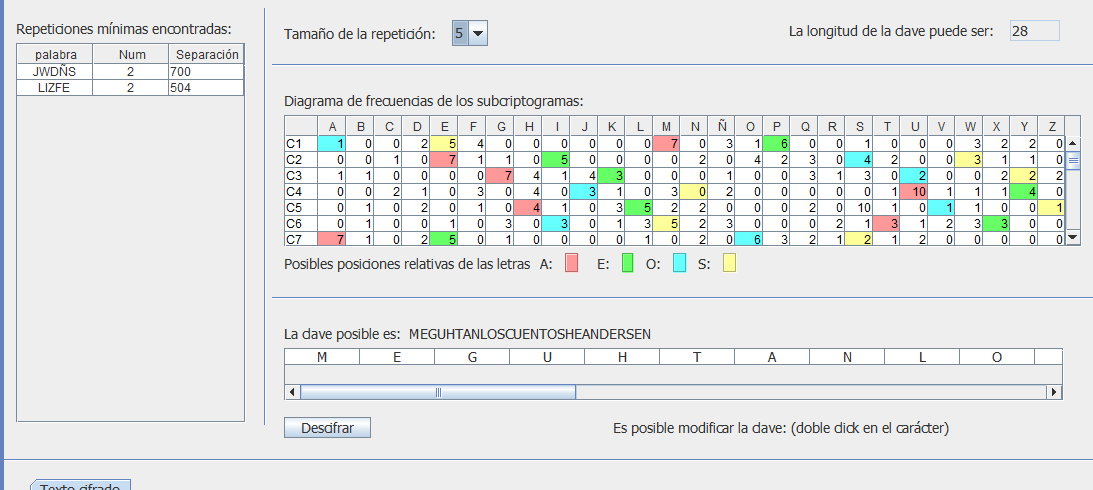
****

****

Descifrado



Criptoanálisis



Con repeticiones de 5 caracteres, se infiere una contraseña, pero no es la correcta exactamente, ya que se infiere la contraseña “MEGUHTANLOSCUENTOSHEANDERSEN”

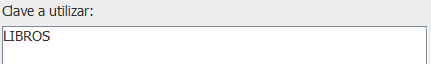
### Cifrado de Beaufort

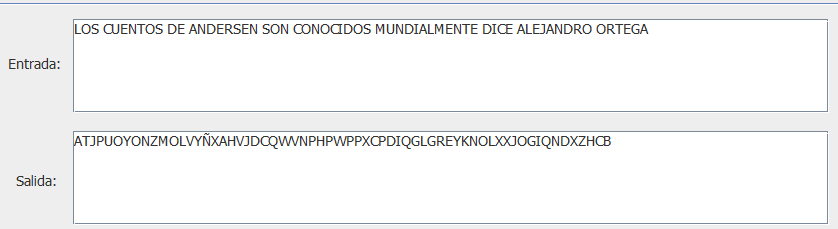
#### Apartado 1

**a)Cifrar con clave K = LIBROS el siguiente mensaje:**

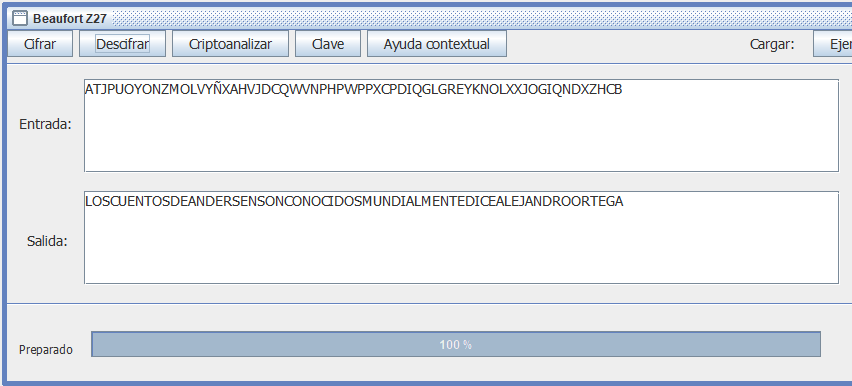
**LOS CUENTOS DE ANDERSEN SON FAMOSOS MUNDIALMENTE DICE <NombreAlumno/s>**

A la hora de realizar las operaciones de cifra y descifrado, se realizan de forma análoga al cifrado de Vigènere, por lo que no se explicara mucho el proceso, más allá de unas capturas de este.





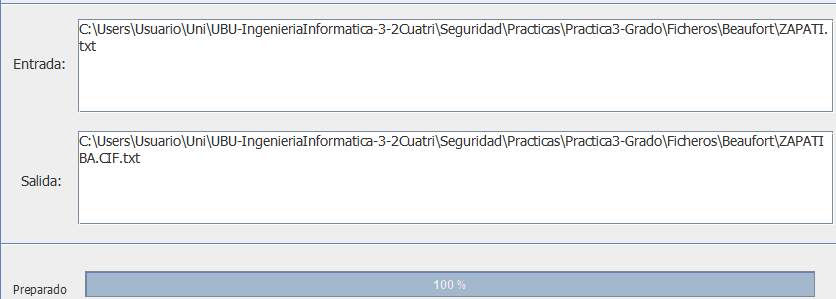
**b)Descifrar el criptograma obtenido**

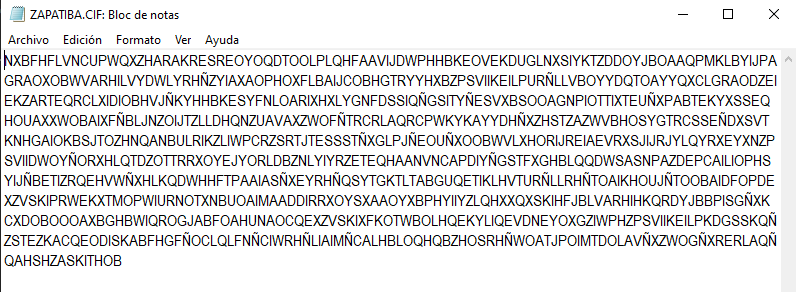


#### Apartado 2

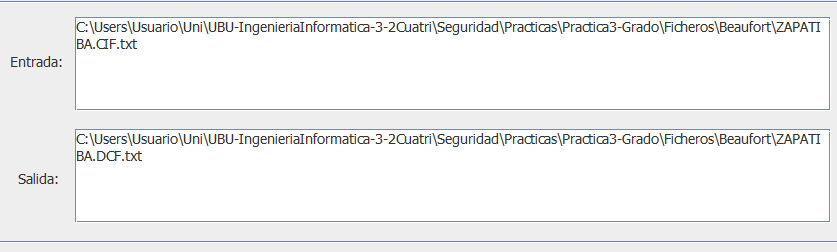
**a)Cifrar con clave K = ROJAS el fichero ZAPATI.TXT. El fichero de salida se llamará ZAPATIBA.CIF.**

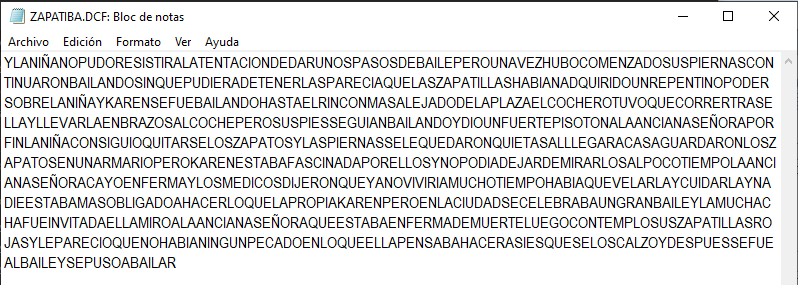
****

****

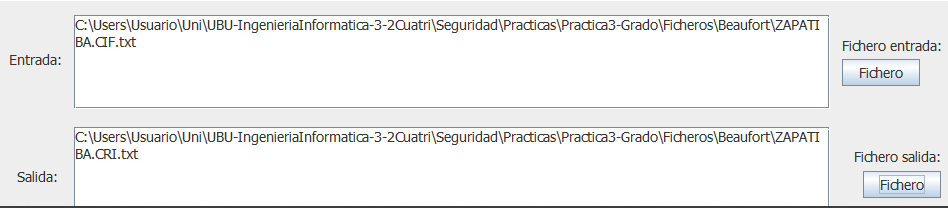
****

**b)Descifrar el fichero ZAPATIBA.CIF, guárdelo como ZAPATIBA.DCF.**

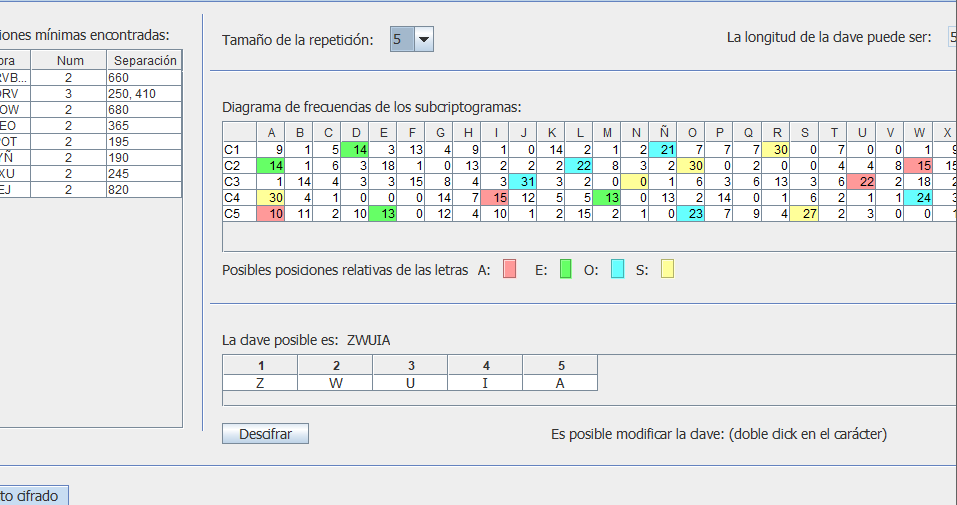
****

****

**c)Criptoanalizar el fichero ZAPATIBA.CIF, guárdelo como ZAFATIBA.CRI.**

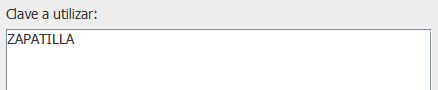
****

Con 5 repeticiones el programa puede inferir una clave, aunque no es la correcta:

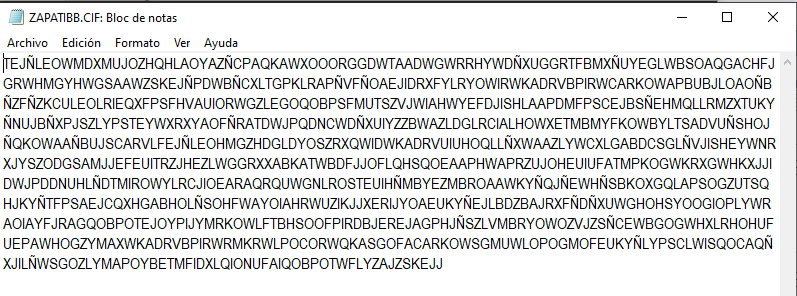


**d)Repita los puntos a), b) y c) primero usando la clave K = ZAPATILLA y luego con K = ZAPATILLAS. Los archivos de salida serán ZAPATIBB.CIF, ZAPATIBB.DCF, ZAPATIBB.CRI Y ZAPATIBC.CIF, ZAPATIBC.DCF y ZAPATIBC.CRI.**

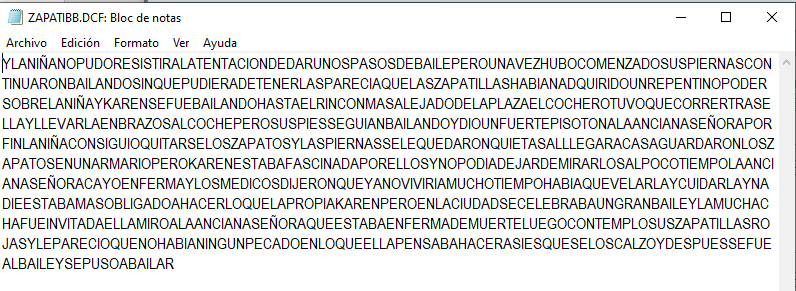
Se va a repetir, pero no se harán capturas del proceso, solo de los resultados, para no cargar el trabajo de capturas de pantalla:



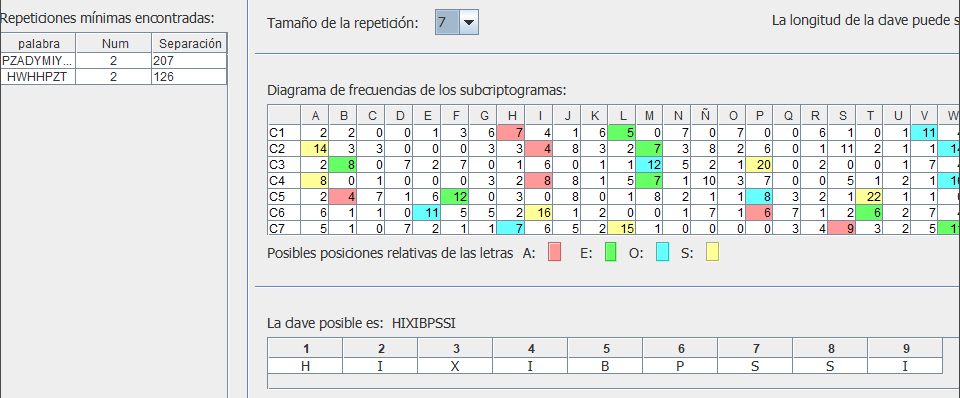
Cifrado



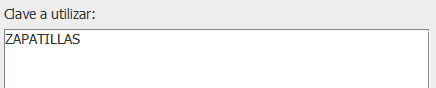
Descifrado



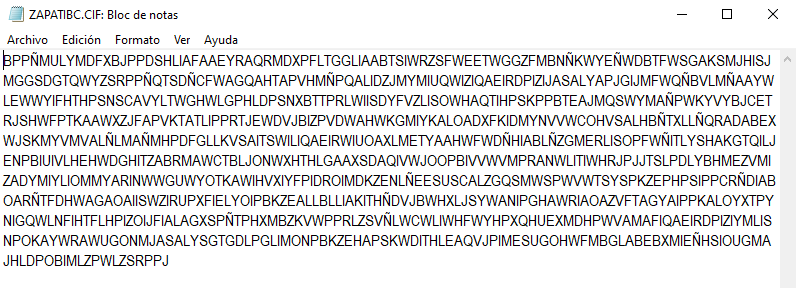
Criptoanálisis



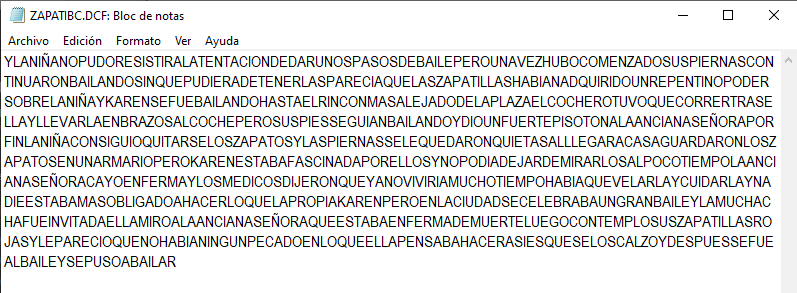
Podemos observar que el programa intenta inferir una clave fijándose en claves de longitud 7, pero no tiene éxito



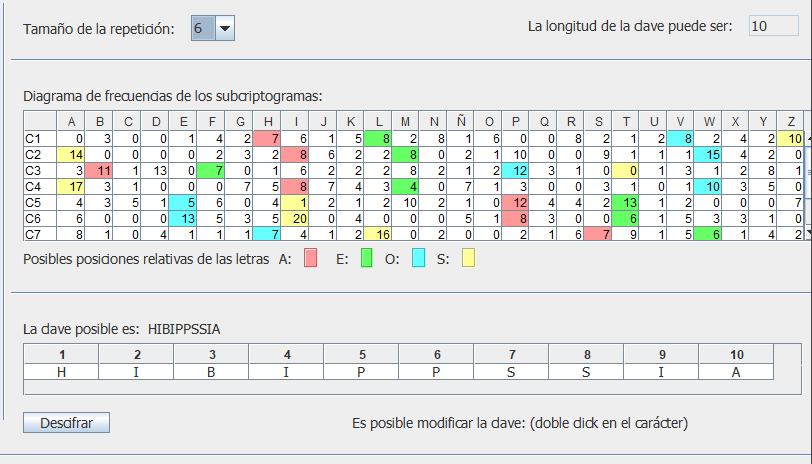
Encriptar



Desencriptar



Criptoanálisis



Tampoco ha podido encontrar la clave

#### Informe

**1.Compruebe la cifra del mensaje del apartado 1.a aplicando directamente aritmética modular.**

Se ha invertido el orden de las letras del alfabeto, y se les ha desplazado ki posiciones a la derecha según la formula Ci = (ki-Mi) mod n

Así, teniendo en cuenta lo siguiente:

* Entrada: LOS CUENTOS DE ANDERSEN SON FAMOSOS MUNDIALMENTE DICE ALEJANDRO ORTEGA
* Salida: ATJPUOYONZMOLVYÑXAHVJDCÑLWNZAAZÑOOHSAWXFVOIAZÑOIHZBFMBWTKYLNL
* Clave: LIBROS

Podemos observar que a la primera L se le ha desplazado a la izquierda tantas posiciones como el valor de la primera letra de la clave (L=12), convirtiéndose en una A.

A la segunda letra (O), se le ha desplazado tantas posiciones como la segunda letra de la clave (I=9), obteniendo una T.

Así hasta que terminan todos los caracteres de la clave, y se vuelve a empezar.

Nota: Hay que tener en cuenta que se ha invertido el alfabeto.

**2.Explique brevemente cómo se ha realizado el criptoanálisis al archivo del apartado 2.c.**

Teniendo en cuenta el numero de repeticiones que podemos encontrar, y según el tamaño de estas repeticiones, se puede intentar inferir la clave.

**3.Explique qué sucede en los ataques a la cifra del apartado 2.d.**

Cuanto mas larga sea la clave, más difícil es deducirla. Como en este apartado era un clave notablemente mas larga que las anteriores, no se ha podido deducir.

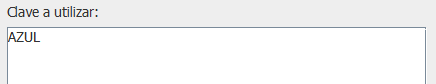
### Cifrado variante de Beaufort

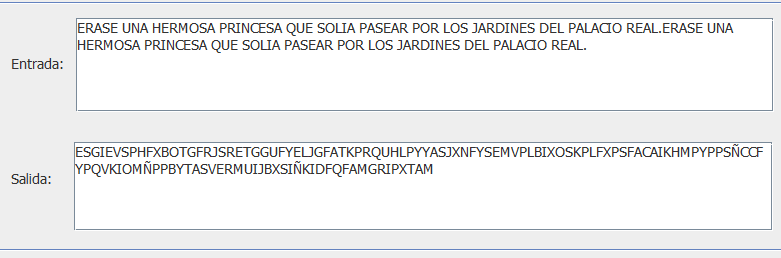
#### Apartado 1

**a)Cifrar con clave K = AZUL el mensaje de la práctica de Vigenère:**

**ERASE UNA HERMOSA PRINCESA QUE SOLIA PASEAR POR LOS JARDINES DEL PALACIO REAL.**

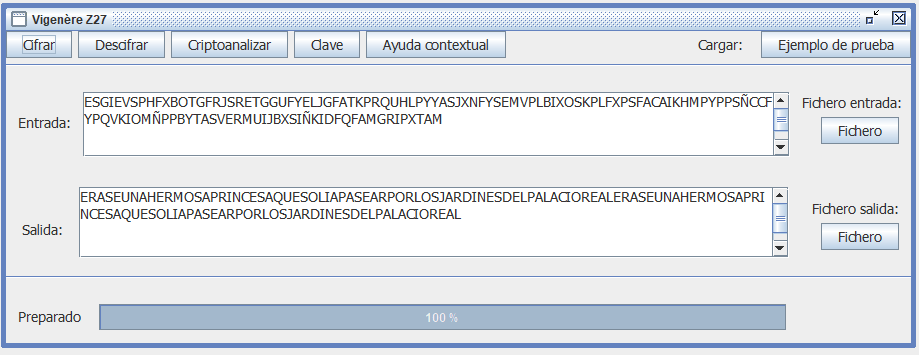
El proceso es similar a los anteriores, por lo que, siguiendo con los puntos anteriores, se demostrara el proceso mediante capturas:





**b)Descifrar el criptograma obtenido pero volviendo a cifrarlo ahora con el algoritmo de Vigenère.**

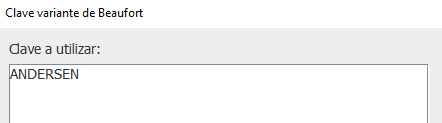
Primero ciframos lo anterior con Vigenère:

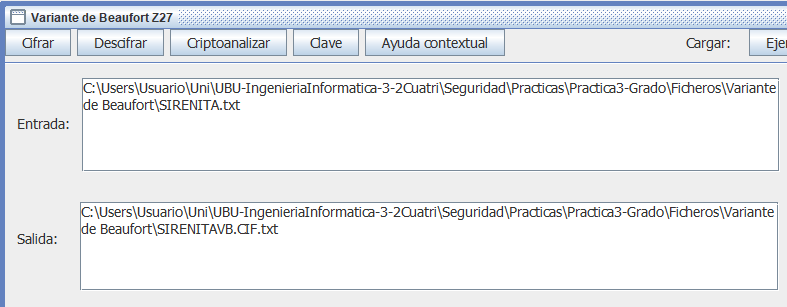


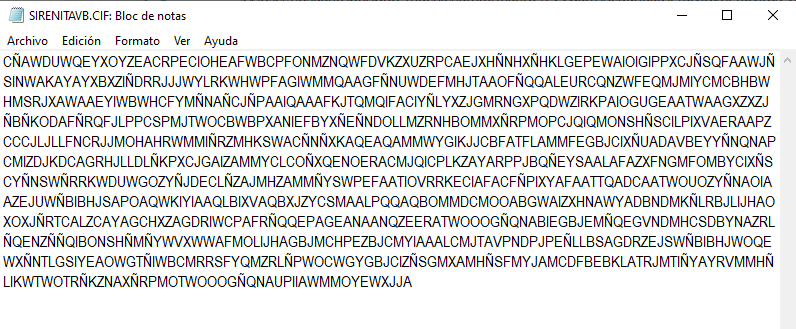
Al cifrarlo con Vigenère, y la misma clave, obtenemos el texto original.

#### Apartado 2

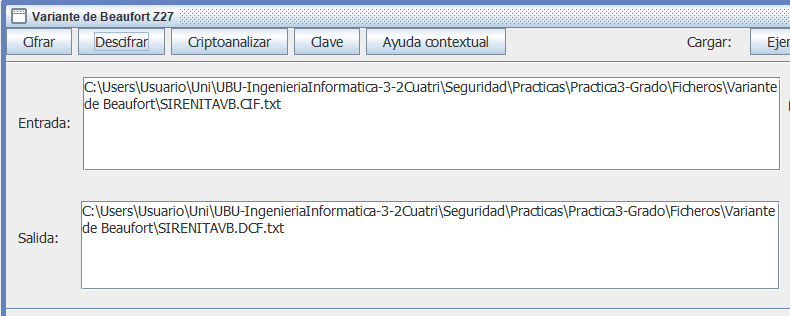
**a)Cifrar con clave K = ANDERSEN el fichero SIRENITA.TXT. El fichero de salida se llamará SIRENAVB.CIF.**

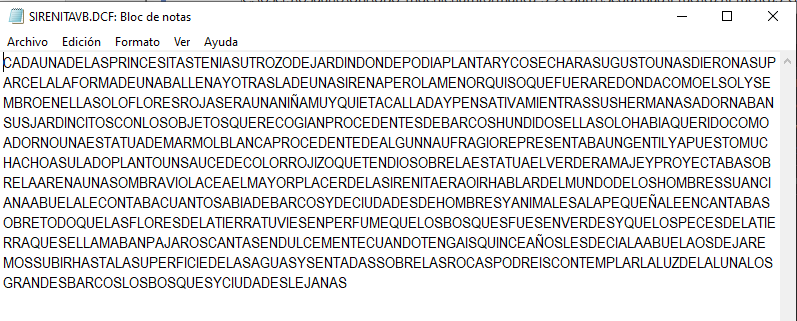




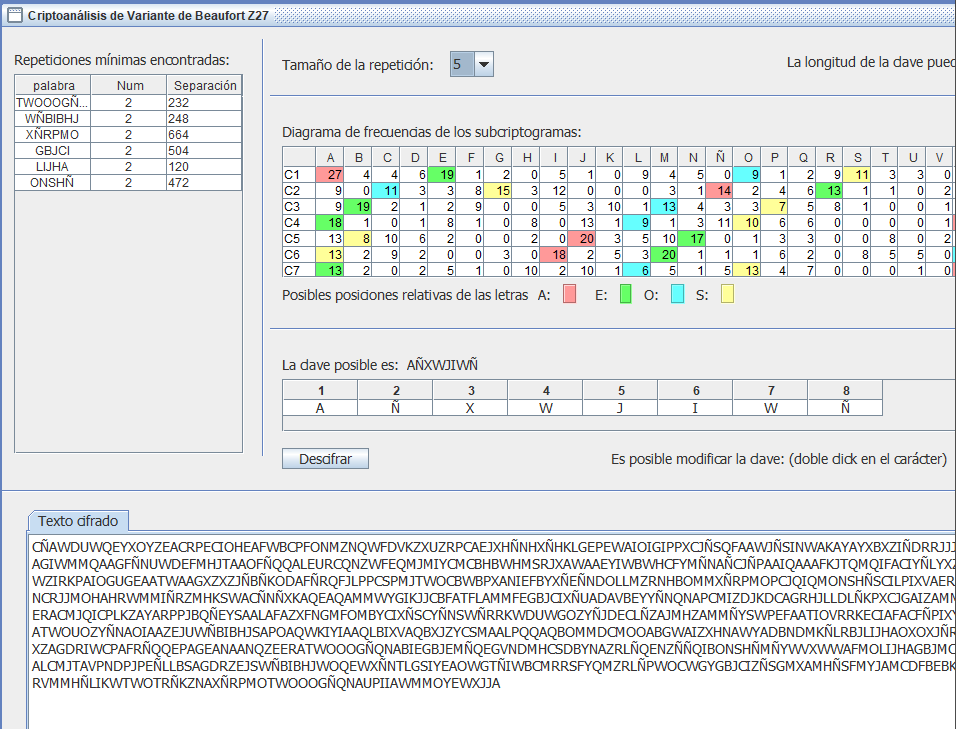


**b)Descifrar el fichero SIRENAVB.CIF, guardándolo como SIRENAVB.DCF.**

****

****

**c)Criptoanalizar el fichero SIRENAVB.CIF, guardándolo como SIRENAVB.CRI.**

****

Como podemos observar, teniendo en cuenta las repeticiones de 5 caracteres se ha podido inferir una contraseña, aunque no ha sido la correcta.

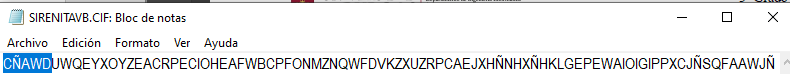
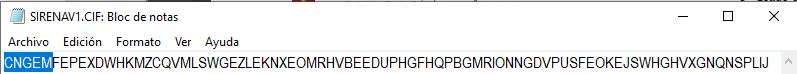
#### Informe

**1.Explique qué ha sucedido al cifrar con Vigenère lo cifrado antes por Variante de Beaufort.**

Al cifrar con Vigenère lo cifrado antes por Variante de Beaufort, usando la misma clave, hemos obtenido el texto original.

Esto es porque el proceso de cifra con Vigenère es “lo contrario” al proceso de cifra de variante de Beaufort, por lo que podemos usar uno como descifrador del otro.

**2.Compare los cinco primeros caracteres del criptograma SIRENAVB.CIF con el criptograma obtenido con Vigenère SIRENAV1.CIF. ¿Qué puede concluir de los valores encontrados?**

**** ****

## Cifradores polialfabeticos por sustitución: Cifradores Periódicos

### Cifrado de Vernam

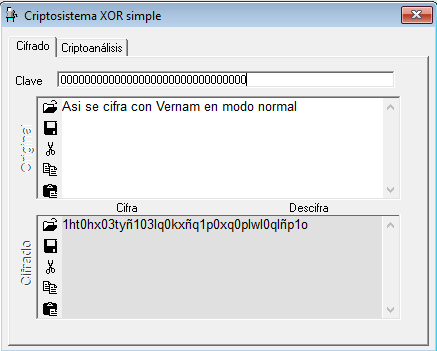
#### Apartado 1

**a)Cifrar con Vernam orientado a caracteres o XOR el siguiente mensaje:**

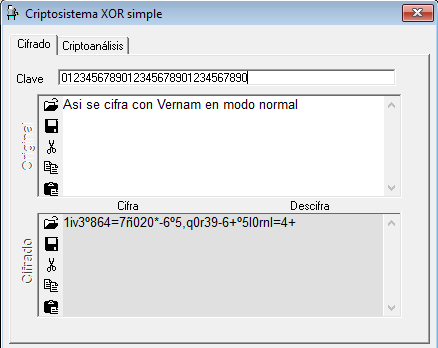
**Así se cifra con Vernam en modo normal.**

**b)Utilizar para ello las siguiente secuencias:**

**1. 0000000000000000000000000000000**



**2. 0123456789012345678901234567890**

****

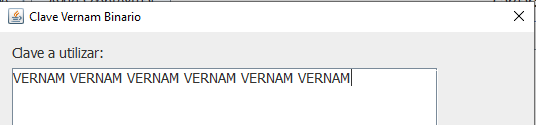
**c)Cifrar con Vernam binario el siguiente mensaje:**

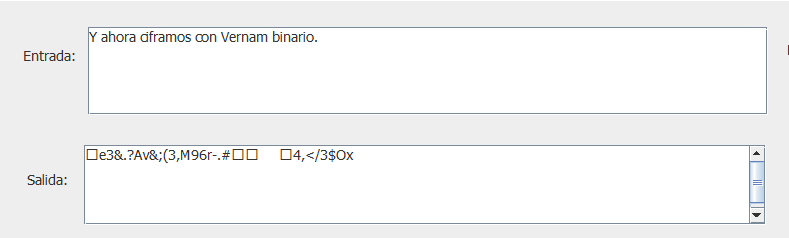
**Y ahora ciframos con Vernam binario.**

Esta vez si que lo cifraremos con la herramienta criptoclasicos, siguiendo la dinámica de los anteriores puntos.

**d)Utilizar para ello las siguiente secuencias:**

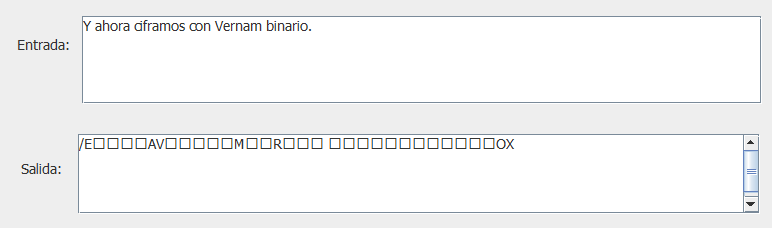
**1. VERNAM VERNAM VERNAM VERNAM VERNAM VERNAM**

****

****

Como vemos, también tiene caracteres no imprimibles.

**2. vernam vernam vernam vernam vernam vernam**

****

La cifra entre los dos es diferente

#### Apartado 2

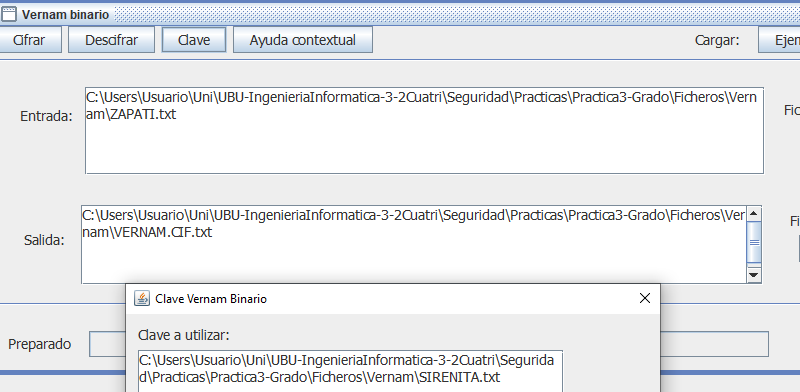
**a)Cifrar con el método de Vernam binario el fichero ZAPATI.DOC que tiene formato Microsoft Word. Use como clave un archivo de mayor longitud, por ejemplo SIRENITA.TXT. El fichero de salida se llamará VERNAM.CIF.**

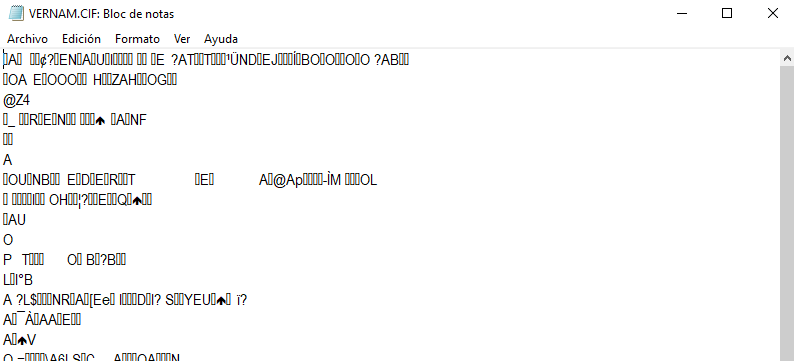
El programa de criptoclasicos no deja subir ficheros con formato Word, solo con formato txt, por lo que cambiaré el tipo del archivo.

No se puede hacer, porque la herramienta criptoclasicos solo admite ficheros Word.

Copiando el texto y pegándolo en un fichero txt, obtenemos los siguientes resultados:

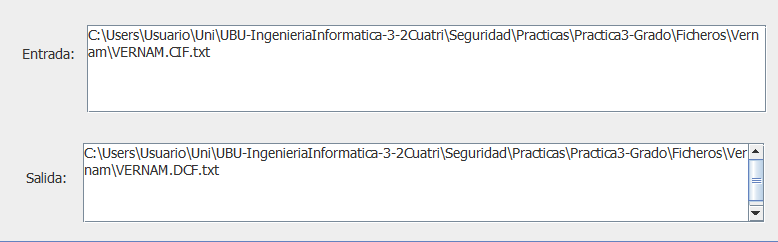
NOTA: La longitud de SIRENITA es menor que el de ZAPATI, por lo que he duplicado el texto

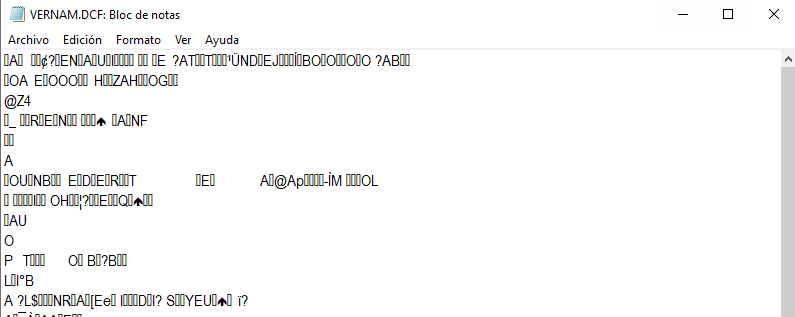




Como podemos observar, la mayoría de los caracteres son no imprimibles

**b)Descifrar el fichero VERNAM.CIF, guardándolo como VERNAM.DCF. Observe si se obtenido el mismo archivo.**

****

****

No, no se obtiene el mismo fichero

#### Informe

**1.Comente qué ha sucedido en las operaciones de cifra del apartado 1.**

**2.¿Daría el mismo resultado si se usará el método de Vernam orientado a caracteres en la cifra del apartado 2.a?**

No, no daría el mismo resultado

**3.Al descifrar el fichero VERNAM.CIF en el apartado 2.b, ¿se recupera el formato de Word 7.0. ¿Por qué?**

En nuestro caso no admitía ficheros Word, pero si el cifrador es lo suficientemente “inteligente” para leer archivos Word, seria capaz de recuperar la versión

## Cifradores polialfabeticos por sustitución: Cifradores de Transposición

### Cifradores por Transposición de Filas

#### Apartado 1

**a)Cifrar para valores distintos de filas (en concreto 1, 2, 3, 4 y 5) el siguiente mensaje:**

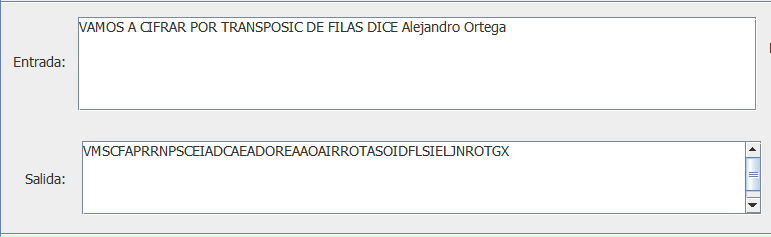
**VAMOS A CIFRAR POR TRANSPOSIC DE FILAS DICE <NombreAlumno/s>**

El proceso de cifrado es similar a los vistos, en la herramienta de criptoclasicos

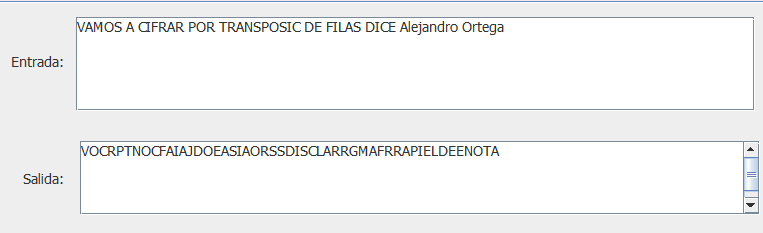
Con valor 1:

No nos deja el criptoclasicos, pero podemos intuir que el texto se queda igual a como estaba en un principio, porque hacemos columnas de un carácter, lo que se corresponde al texto en fila.

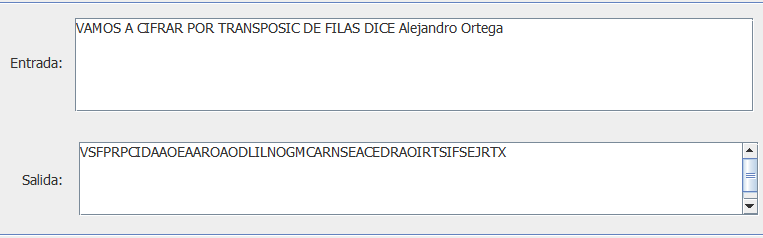
Con valor 2



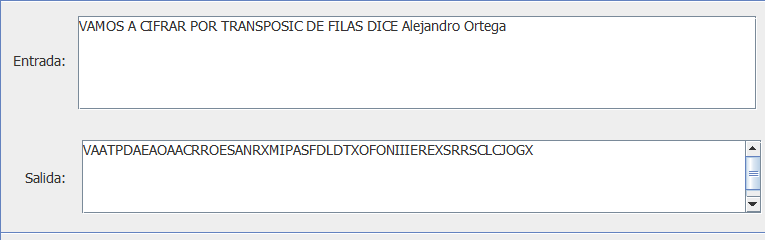
Con valor 3



Con valor 4



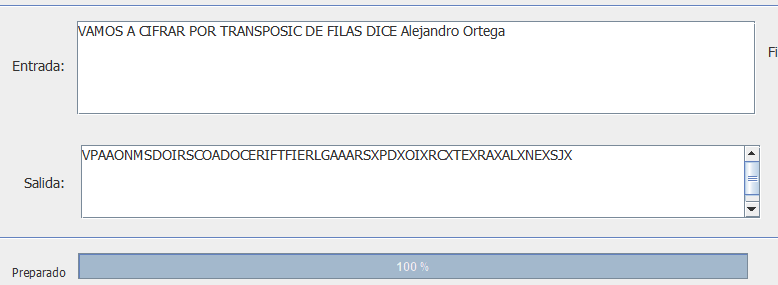
Con valor 5



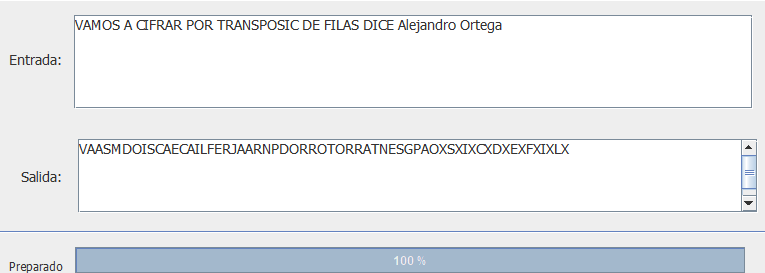
**b)Repetir cifrando con 20 y 30 filas.**

**Nota: Hemos puesto que el carácter de relleno sea X**

Con 20:

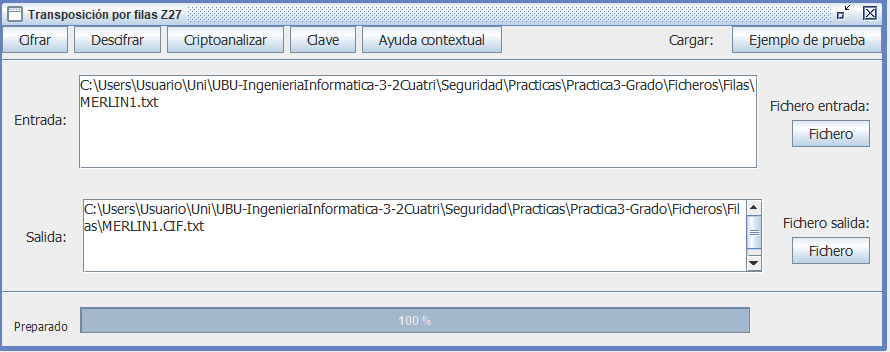
****

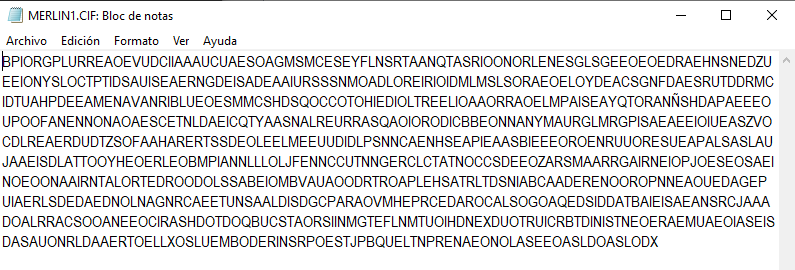
Con 30

****

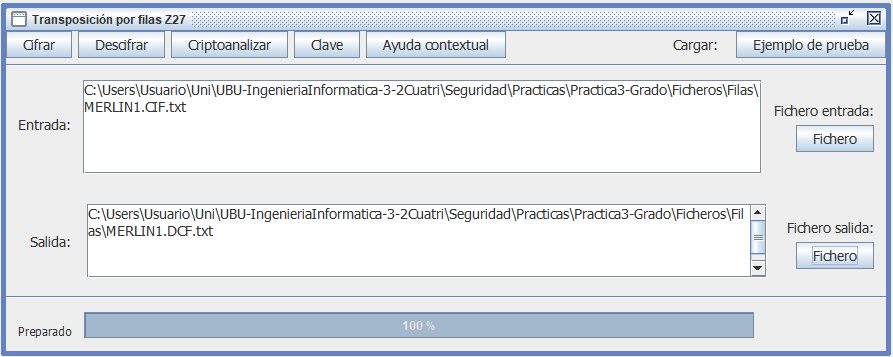
#### Apartado 2

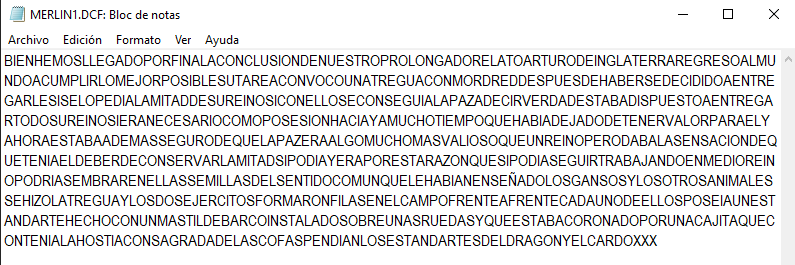
**a)Cifrar con un valor de 16 filas el fichero MERLIN1.TXT. El fichero de salida se llamará MERLIN1.CIF.**

****

****

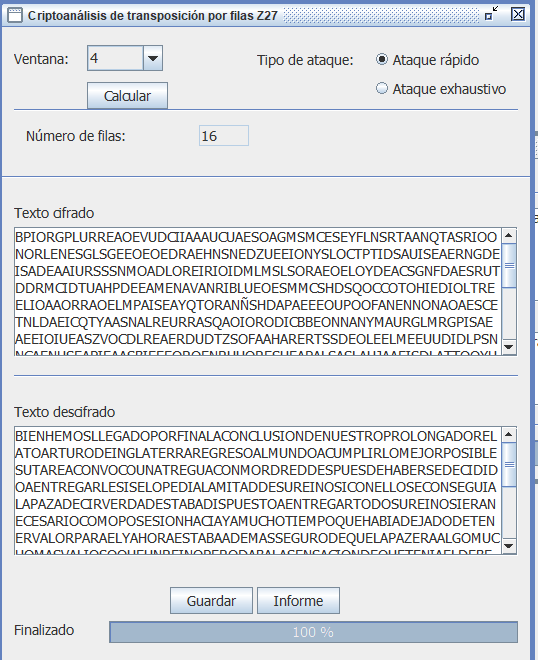
**b)Descifrar el fichero MERLIN1.CIF, guardándolo como MERLIN1.DCF.**

****

****

Podemos observar que se ha descifrado con éxito.

**c)Criptoanalizar el fichero MERLIN1.CIF, guardando el fichero como MERLIN1.CRI.**

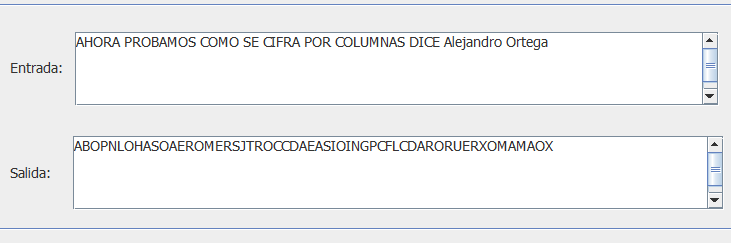
Al darle a calcular, rápidamente ha descifrado el texto y ha adivinado que se ha usado como numero de filas 16.

### Cifradores por Transposición de Columnas

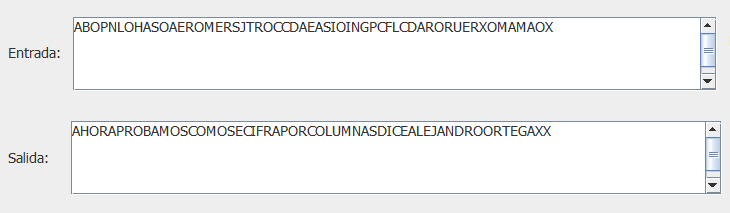
#### Apartado 1

**a)Cifrar con 8 columnas el siguiente mensaje:**

**AHORA PROBAMOS COMO SE CIFRA POR COLUMNAS DICE <NombreAlumno/s>**

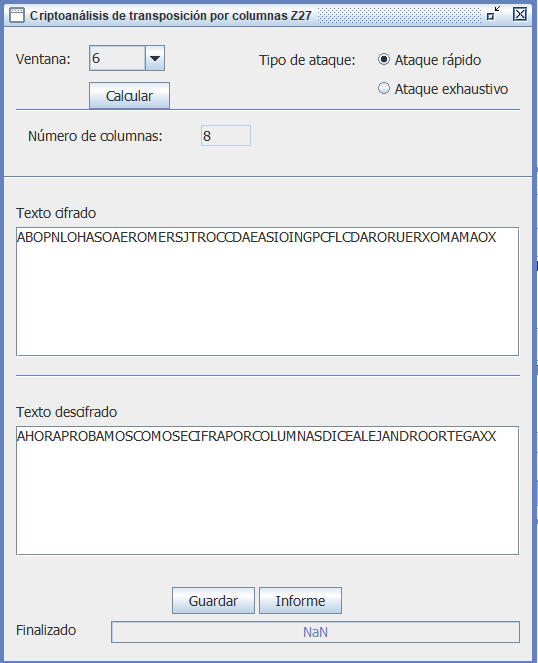
****

**b)Descifrar el criptograma obtenido.**

****

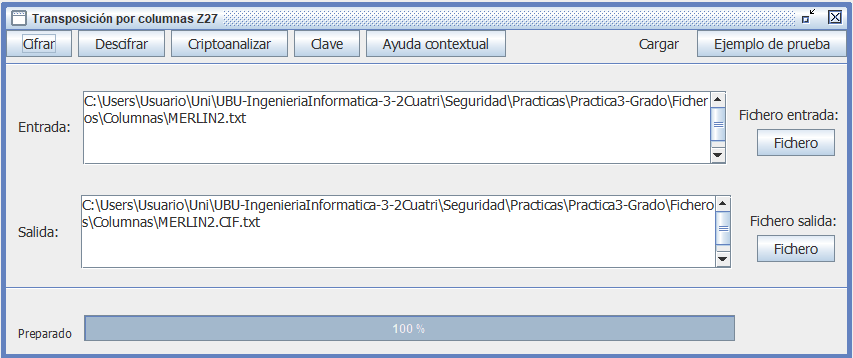
Observamos que ha añadido unas X al final del texto, esto es porque el numero de columnas no era exacto, y había que rellenar el mensaje.

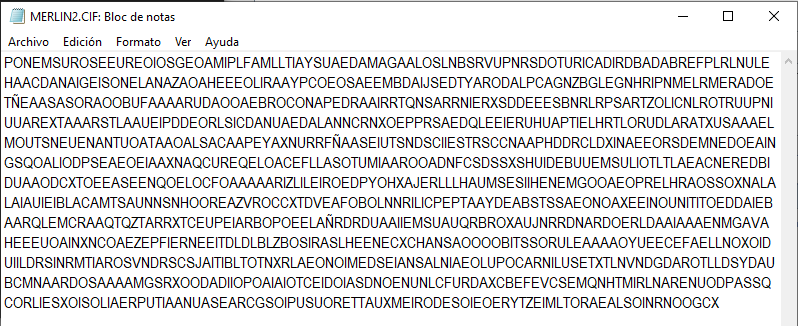
**c)Intente criptoanalizar el criptograma obtenido con un valor de ventana mayor que 5.**

Podemos observar que si que puede romper el cifrado, adivinando que se ha cifrado con un numero de columna de 8,aunque no debería.

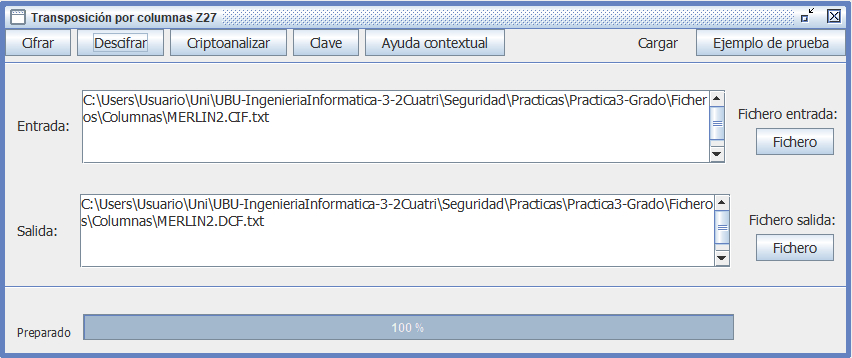
#### Apartado 2

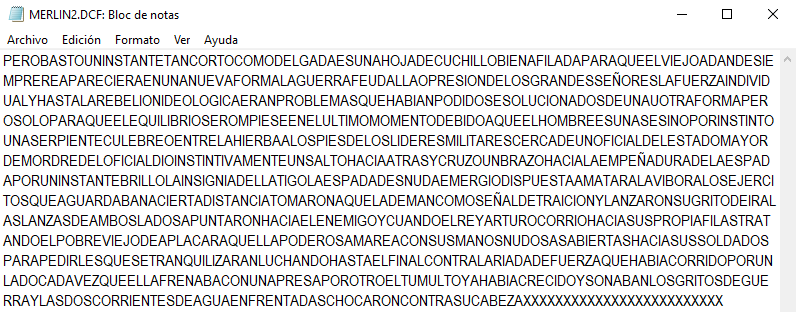
**a)Cifrar con una valor de 30 columnas el fichero MERLIN2.TXT. El fichero de salida se llamará MERLIN2.CIF.**

****

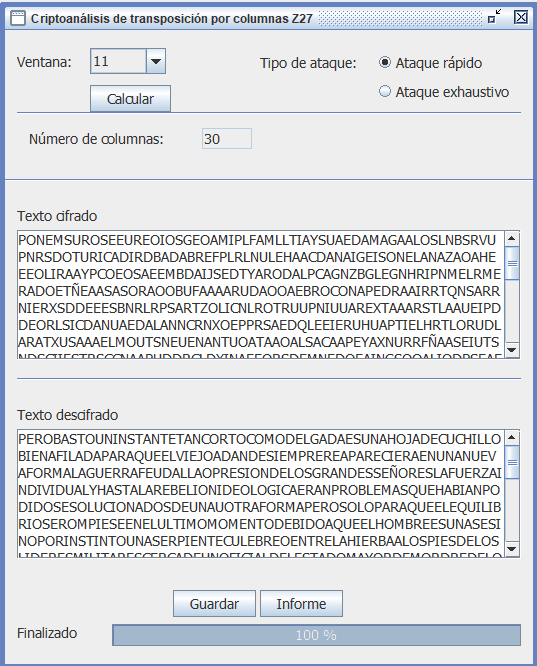
****

**b)Descifrar el fichero MERLIN2.CIF, guardándolo como MERLIN2.DCF.**

****

****

**c)Criptoanalizar el fichero MERLIN2.CIF, guardándolo como MERLIN2.CRI. Usar para ello distintas longitudes de ventana.**

Con una ventana de 11, ya es posible conseguir el texto original, adivinando que el numero de columnas utilizadas son 30.

#### Informe

**1.Indique por qué no se puede romper el cifrado en el apartado 1.c.**

En mi caso si que se ha podido descifrar

**2.Elija una ventana de tamaño 20 y demuestre que, según el método de anagramación, en el período de cifra se cumple que la media de los diagramas es un valor alto y la desviación estándar tiende a ser baja.**

el algoritmo utilizado para criptoanalizarlo, selecciona las iteraciones cuya media es más alta que la última seleccionada, por lo que la media crece, y que tengan una media alta unida a una desviación típica baja, señal de que podrían ser parte del texto en claro.

al usar más valores en la ventana, hay más posibilidades de esto.

# Conclusión

A lo largo de esta practica, he aprendido bastante sobre todo el mundo de criptografía, y he logrado entender los fundamentos teóricos de los algoritmos de criptografía básicos.

Me ha resultado bastante interesante, ya no solo relacionado con el temario de la asinatura, sino orientado a mi futuro laboral.

# Bibliografía

XOR calculator. (s.f.). Obtenido de http://www.xor.pw/#