



PRÁCTICA - UD1

LAURA BERENGUER
CETS 2023 - 2024

Tabla de contenido

Ejercicio 1.....3

Ejercicio 2.....3

Retos cripto.....4

 Básico.....4

 Cifrado por sustitución6

 Codificaciones6

 Avanzados.....7

 Avanzados II10

Ejercicio 1

Buscar y analizar dos ataques importantes que hayan sido realizados durante los años 2022-2023. Uno de ellos debe haber tenido por objetivo el sabotaje, espionaje o fines monetarios, y otro el despliegue de ransomware. En ambos casos se deberá analizar mediante fuentes técnicas y confiables la forma de actuación, impacto y como se resolvió el incidente.

Sabotaje a la red eléctrica de Ucrania en 2022

En febrero de 2022, antes del comienzo de la invasión de Ucrania por parte de Rusia, un ciberataque consiguió sabotear la red eléctrica de Ucrania, provocando apagones en varias zonas del país. El ataque fue reivindicado por el grupo Killnet.

El ataque se llevo a cabo mediante un DDoS (denegación de servicio distribuido), que consiste en saturar un servidor o red con solicitudes para sobrecargarlos y hacerlos inaccesibles. Los atacantes usaron botnets, es decir, redes de ordenadores infectados que se pueden controlar de forma remota.

El impacto fue considerable, ya que los apagones afectaron a servicios públicos, provocando pérdidas económicas.

El ataque fue resuelto por el gobierno ucraniano, logrando restaurar el servicio eléctrico.

Ataque de ransomware a Colonial Pipeline en 2021

En mayo del 2021, el oleoducto Colonial Pipeline, que se encarga de suministrar combustible a la costa este de Estados Unidos, fue atacado por el ransomware "DarkSide". Esto provocó el cierre del oleoducto durante varios días, provocando escasez de combustible y aumento de los precios del combustible.

Se llevó a cabo mediante un exploit de día cero, que se usó para instalar el ransomware en sus sistemas informáticos.

El ataque fue resuelto por Colonial Pipeline, que pagó un rescate de 4,4 millones de dólares a los atacantes.

Ejercicio 2

Buscar información sobre las acciones y programas de espionaje de la NSA. Analizar las técnicas, procedimientos y colaboraciones realizadas de forma breve, y posteriormente, analizar dos proyectos a elección del alumno que se encuentren dentro del catálogo ANT TAO de la NSA, destacando los detalles de los mismos.

El catálogo ANT TAO de la NSA contiene una lista de proyectos de tecnología de ataque. Estos se usan para desarrollar nuevas técnicas y herramientas de espionaje.

Proyecto Barnacle

Se utiliza para desarrollar malware que puede infiltrarse en otros sistemas para recopilar datos, controlar sistemas o realizar ataques.

Proyect QUANTUM

Se centra en el desarrollo de técnicas de ataque que son difíciles de detectar, pudiéndose usar para espiar otros sistemas sin ser detectados. Incluye el uso de técnicas de cifrado, ingeniería social y evasiones

Retos cripto

Básico

El alumno deberá obtener la clave para 'abrir' la caja.



A-1	J-10	S-19
B-2	K-11	T-20
C-3	L-12	U-21
D-4	M-13	V-22
E-5	N-14	W-23
F-6	O-15	X-24
G-7	P-16	Y-25
H-8	Q-17	Z-26
I-9	R-18	

9	23	14	14	18	5	(código proporcionado)
I	W	N	N	R	E	(código obtenido por sustitución)

0	1	0	1	0	1	(grupos de dos para hacer la transposición)
1	0	1	0	1	0	(código obtenido por transposicion)
W	I	N	N	E	R	(sustitución ordenada tras la transposision)

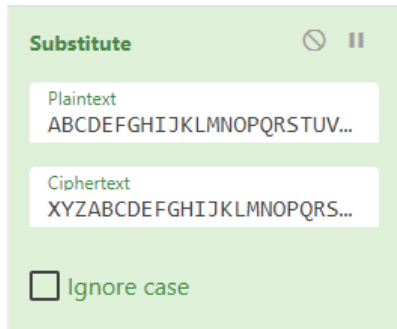
Cifrado por sustitución

Obtener el texto la clave y el texto en claro para el siguiente texto cifrado:

FRZDUGV GLH PDQB WLP HV EHIRUH WKHLU GHDWKV; WKH YDOLDQW QHYHU WDVWH RI
GHDWK

EXW RQFH.

Z. VKDNHVS HDUH, MXOLXV FDHVDU



The screenshot shows a web-based 'Substitute' cipher tool. It has a title 'Substitute' with a refresh icon and a pause icon. There are two input fields: 'Plaintext' containing 'ABCDEFGHIJKLMNOPQRSTUVWXYZ...' and 'Ciphertext' containing 'XYZABCDEFGHIJKLMNOPQRSTUVWXYZ...'. Below these fields is a checkbox labeled 'Ignore case' which is currently unchecked.

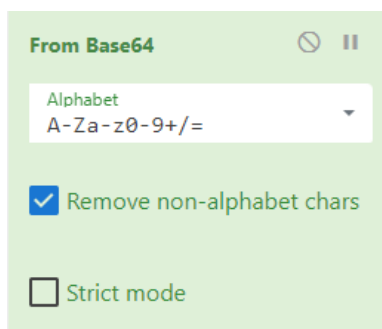
COWARDS DIE MANY TIMES BEFORE THEIR DEATHS; THE VALIANT NEVER TASTE OF DEATH
BUT ONCE.

W. SHAKESPEARE, JULIUS CAESAR

Codificaciones

El alumno deberá obtener el texto en claro para las siguientes codificaciones:



ZXN0byBlcyB1bmEgcHJ1ZWJhIGRlIGNyaXB0bwo=



The screenshot shows a web-based 'From Base64' decoding tool. It has a title 'From Base64' with a refresh icon and a pause icon. There is a dropdown menu labeled 'Alphabet' with the value 'A-Za-z0-9+/' selected. Below the dropdown is a checked checkbox labeled 'Remove non-alphabet chars'. At the bottom is an unchecked checkbox labeled 'Strict mode'.

esto es una prueba de cripto

*NjUgNzMgNzQgNmYgMjAgNjUgNzMgMjAgNzUgNmUgNjEgMjAgNzAgNzlgNzUgNjUgNjlgNjEg
MjAgNjUgNjUgMjAgNjMgNzlgNjkgNzAgNzQgNmYgMGE=*



From Base64  

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars

☐ Strict mode

65 73 74 6f 20 65 73 20 75 6e 61 20 70 72 75 65 62 61 20 64 65 20 63 72 69 70 74 6f 0a

From Hex  

Delimiter
Space

esto es una prueba de cripto

Avanzados

El alumno deberá descifrar los siguientes ejercicios, debiendo obtener la flag en formato "RS{flag}"

Ejercicio 1 (¿Sabemos las dos primeras letras?):

23[M/0TW%.T9?3)8?AR%.T?%N/UGH]



Rotacion de 32

RS{mOPtwENTY_SIX_arENT_EnOugh}

Ejercicio 2 (¿XOR?):

a1a088c08b90c28680c285c0acc381ac80c39ec0879bc29d948e

a1 a0 88 c0 8b 90 c2 86 80 c2 85 c0 ac c3 81 ac 80 c3 9e c0 87 9b c2 9d 94 8e

To Binary  

Delimiter
Space

Byte Length
8

01100001 00110001 00100000 01100001 00110000 00100000 00111000 00111000
00100000 01100011 00110000 00100000 00111000 01100010 00100000 00111001
00110000 00100000 01100011 00110010 00100000 00111000 00110110 00100000
00111000 00110000 00100000 01100011 00110010 00100000 00111000 00110101
00100000 01100011 00110000 00100000 01100001 01100011 00100000 01100011
00110011 00100000 00111000 00110001 00100000 01100001 01100011 00100000
00111000 00110000 00100000 01100011 00110011 00100000 00111001 01100101
00100000 01100011 00110000 00100000 00111000 00110111 00100000 00111001
01100010 00100000 01100011 00110010 00100000 00111001 01100100 00100000
00111001 00110100 00100000 00111000 01100101

Ejercicio 3 (¿Metadatos?):

MDEwMDAxMDAgMDExMDAxMDEgMDExMTAwMTEgMDExMDAwMTEgMDExMDAwMD
DEgMDExMTAwMTAgMDExMDAxMTEgMDExMDAwMDEgMDAxMDAwMDAgMDExMDE
xMDAgMDExMDAwMDEgMDAxMDAwMDAgMDExMDEwMDEgMDExMDExMDEgMDEx
MDAwMDEgMDExMDAxMTEgMDExMDAxMDEgMDExMDExMTAgMDAxMTEwMTAgMD
AxMDAwMDAgMDExMDEwMDAgMDExMTAxMDAgMDExMTAxMDAgMDExMTAwMDAg
MDExMTAwMTEgMDAxMTEwMTAgMDAxMDExMTEgMDAxMDExMTEgMDExMDExMDE
gMDExMDEwMDEgMDExMTAwMTAgMDExMDExMTEgMDAxMDExMTAgMDExMDExMD
EgMDExMDAxMDEgMDExMDAxMDAgMDExMDEwMDEgMDExMTAxMDEgMDExMDExM
DEgMDAxMDExMTAgMDExMDAwMTEgMDExMDExMTEgMDExMDExMDEgMDAxMDEx
MTEgMDExMDExMDEgMDExMDAwMDEgMDExMTEwMDAgMDAxMDExMTEgMDAxMTA
xMTEgMDAxMTAwMTAgMDAxMTAwMDAgMDAxMDExMTEgMDAxMTAwMDEgMDAxM
DEwMTAgMDAxMTEwMDEgMDExMTAwMDAgMDEwMDAwMDEgMDEwMDEwMTEgMD
ExMDAwMDEgMDEwMDAwMDEgMDAxMTAwMTAgMDAxMTAwMDEgMDExMTAxMDAg
MDExMDExMTEgMDEwMTAxMDAgMDExMDEwMTAgMDExMDExMDEgMDExMDAwMD
EgMDAxMTAxMTAgMDEwMTAwMDEgMDEwMTAxMTAgMDExMDEwMTEgMDEwMTEw
MDEgMDEwMTAwMDAgMDExMDExMTEgMDEwMDAwMDEgMDAxMDExMTAgMDExM
DEwMTAgMDExMTAwMDAgMDExMDAxMDEgMDExMDAxMTE=

From Base64

Alphabet

A-Za-z0-9+/=

☒ Remove non-alphabet chars

☐ Strict mode

01000100 01100101 01110011 01100011 01100001 01110010 01100111 01100001
00100000 01101100 01100001 00100000 01101001 01101101 01100001 01100111
01100101 01101110 00111010 00100000 01101000 01110100 01110100 01110000
01110011 00111010 00101111 00101111 01101101 01101001 01110010 01101111
00101110 01101101 01100101 01100100 01101001 01110101 01101101 00101110
01100011 01101111 01101101 00101111 01101101 01100001 01111000 00101111


```
00110111 00110010 00110000 00101111 00110001 00101010 00111001 01110000
01000001 01001011 01100001 01000001 00110010 00110001 01110100 01101111
01010100 01101010 01101101 01100001 00110110 01010001 01010110 01101011
01011001 01010000 01101111 01000001 00101110 01101010 01110000 01100101
01100111
```

From Binary⌵⏸

Delimiter
Space



Byte Length
8

Descarga la imagen:

https://miro.medium.com/max/720/1*9pAKaA21toTjma6QVkJYPoA.jpeg



Ejercicio 4:

From Morse Code  

Letter delimiter
Space

Word delimiter
Line feed

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.

R:S:F:I:N:D:I:N:G:_P:A:T:T:E:R:N:S:_I:S:_K:E:Y:_F:O:R:C:R:Y:P:O

Avanzados II

Se muestran a continuación los diferentes ejercicios planteados. Todos tendrán una flag del tipo "picoCTF{xxxxxx}"

Ejercicio 1: Take each number mod37 and map it to the following character set: 0-25 is the alphabet (uppercase), 26-35 are the decimal digits, and 36 is an underscore

54 211 168 309 262 110 272 73 54 137 131 383 188 332 39 396 370 182 328 327 366
70

17 26 20 13 3 36 13 36 17 26 20 13 3 36 2 26 0 34 32 31 33 33

A: 0
B: 1
C: 2
D: 3
E: 4
F: 5
G: 6
H: 7
I: 8
J: 9
K: 10
L: 11
M: 12
N: 13
O: 14
P: 15
Q: 16
R: 17
S: 18
T: 19
U: 20
V: 21
W: 22
X: 23
Y: 24
Z: 25
0: 26
1: 27
2: 28
3: 29
4: 30
5: 31
6: 32

7: 33
8: 34
9: 35
_: 36

R O U N D _ N _ R O U N D _ C O A 8 6 5 7 7

Ejercicio 2: Se adjunta el archivo que deberá ser descifrado/decodificado.

W H 4 7 H 4 7 H 9 0 D W 2 0 U 9 H 7

Ejercicio 3: ¿Rail Fence?

Ta _7N6DE7hlg:W3D_H3C31N__BD4ef sHR053F38N43D47 i33__NC

The flag is: WH3R3_D035_7H3_F3NC3_8361N_4ND_3ND_EB4C7D74

Ejercicio 4: Una palabra puede dar la clave...

UHQKRNWLFYJBTODCZVAXEGSMPuhqkrnwlfyjbtdczvaxegsmp

Lrxyzdot Jrwzutk uzovr, gfal u wzuer utk vauarjm ufz, utk hzoxwla br alr hrrajr
nzob u wjuvv quvr ft glfql fa guv rtqjovrk. Fa guv u hruxafnxj vquzuhurxv, utk, ua
alua afbr, xtytogt ao tuaxzujfvav—on qoxzvr u wzrua dzfpr ft u vqfrtafnfq dofta
on efrg. Alrzt grzt ago zoxtk hjuqy vdoav truz otr rsazrbfam on alr huqy, utk u
jotw otr truz alr oalrz. Alr vqujrv grzt rsqrrkftwjm luzk utk wjovvm, gfal ujj alr
uddruzutqr on hxztfvlrk wojk. Alr grfwla on alr ftrvqa guv erzm zrbuzuyhjr, utk,
auyftw ujj alftwv ftao qotvfrkzuafot, F qoxjk luzkjm hjubr lxdfarz noz lfv odftfot
zrvdrqaftw fa.

Alr njuw fv: dfqoQAN{5XH5717X710T_3E0JX710T_7H755H1U}

Substitute

Plaintext

UHQKRNWLF IYJBTODCZVAXE...

Ciphertext

ABCDEFGHIJKLMNOPQRSTUVWXYZ...

☐ Ignore case

Hereupon Legrand arose, with a grave and stately air, and brought me the beetle from a glass case in which it was enclosed. It was a beautiful scarabaeus, and, at that time, unknown to naturalists—of course a great prize in a scientific point of view. There were two round black spots near one extremity of the back, and a long one near the other. The scales were exceedingly hard and glossy, with all the appearance of burnished gold. The weight of the insect was very remarkable, and, taking all things into consideration, I could hardly blame Jupiter for his opinion respecting it.

The flag is: picoCTF{5UB5717U710N_3V0LU710N_7B755B1A}

Ejercicio 5: ¿Una transposicion manual que tal?

heTfl g as iicpCTo{7F4NRP051N5_16_35P3X51N3_VC85A020}E

Agrupamos los caracteres por grupos de 3, contando los espacios como un carácter mas.

La transposition seria de 012 a 201, quedandonos la siguiente frase.

The flag is picoCTF{7R4N5P051N6_15_3XP3N51V3_5C82A0E0}

Ejercicio 6: Se ha identificado que la clave del mensaje cifrado es "CYLAB" y que se debe usar un algoritmo que comienza por "V"...

rgnoDVD{O0NU_WQ3_G1G3O3T3_A1AH3S_a23a13a5}

Vigenère Decode  

Key
CYLAB

picoCTF{D0NT_US3_V1G3N3R3_C1PH3R_y23c13p5}