**ACTIVIDAD 9:**

Descifrar con el método César el siguiente mensaje si la clave es 7:

“ñhjly avkvz rvz lplyjojovz zot wyvalzahy”

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | Ñ | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | Ñ | O | P | Q | R | S |

* **El texto original es “HACER TODOS LOS EJERCICIOS SIN PROTESTAR”**

**ACTIVIDAD 10:**

Cifrar con el método de las cajas el siguiente mensaje “NO VAMOS A FALTAR NINGUN MIERCOLES A SEGURIDAD” la palabra clave es APROBAR.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| A | P | R | O | B | A | R |
| 1 | 5 | 6 | 4 | 3 | 2 | 7 |
| N | O | V | A | M | O | S |
| A | F | A | L | T | A | R |
| N | I | N | G | U | N | M |
| I | E | R | C | O | L | E |
| S | A | S | E | G | U | R |
| I | D | A | D |  |  |  |

* **El mensaje cifrado es “NANISIOANLYMTUOGALGCEDOFIEADVANRSASRMER”**

1. NANISI
2. OANLU
3. MTUOG
4. ALGCED
5. OFIEAD
6. VANRSA
7. SRMER

**ACTIVIDAD 11:**

Descifrar con el método de las cajas el siguiente mensaje “EVESDNNMULQHNIAUADDAEAGMIXESEYEAAEER” la palabra clave es INTERNET.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **I** | **N** | **T** | **E** | **R** | **N** | **E** | **T** |
| **3** | **4** | **7** | **1** | **6** | **5** | **2** | **8** |
| **L** | **A** | **S** | **E** | **M** | **A** | **N** | **A** |
| **Q** | **U** | **E** | **V** | **I** | **E** | **N** | **E** |
| **H** | **A** | **Y** | **E** | **X** | **A** | **M** | **E** |
| **N** | **D** | **E** | **S** | **E** | **G** | **U** | **R** |
| **I** | **D** | **A** | **D** |  |  |  |  |

* **“LA SEMANA QUE VIENE HAY EXAMEN DE SEGURIDAD”**

**ACTIVIDAD 12:**

Cifrar el siguiente mensaje con el cifrado de Vernam “UNIVERSIDAD”, la clave es “ERDAAEDTGRA”.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| U | N | I | V | E | R | S | I | D | A | D |
| 10101 | 01110 | 01001 | 10110 | 00101 | 10010 | 10011 | 01001 | 00100 | 00001 | 00100 |
| E | R | D | A | A | E | D | T | G | R | A |
| 00101 | 10010 | 00100 | 00001 | 00001 | 00101 | 00100 | 10100 | 00111 | 10010 | 00001 |
| 10000 | 11100 | 01101 | 10111 | 00100 | 10111 | 10111 | 11101 | 00011 | 10011 | 00101 |
| P |  | M | W | D | W | W |  | C | S | E |

* **El mensaje cifrado es “P\_MWDWW\_CSE”**

**ACTIVIDAD 13:**

Cifrar el siguiente mensaje con el algoritmo RSA “FLORES”, p = 3 y q = 7.

* N = P \* Q → N = 3 \* 7 → N = 21

P = 3

Q = 7

N = 21

Z = 12

K = 5

J = 5

* Z = (P – 1) (Q – 1) → Z = 2 \* 6 → Z = 12
* K = coprimo no divisor de z → K = 5
* (K \* J) mod z = 1 → (5 \* J) mod 12 = 1 → k = 5
* Clave pública (k,n) → Clave pública (5, 21)
* Clave privada (j,n) → Clave privada (5,5)

C = M^k mod n

* F → 55 mod 21 → 17
* L → 115 mod 21 → 2
* O → 155 mod 21 → 15
* R → 185 mod 21 → 9
* E → 45 mod 21 → 16
* S → 195 mod 21 → 10
* **Mensaje cifrado “17 2 15 9 16 10”**

**ACTIVIDAD 14:**

Descifrar el siguiente mensaje con el algoritmo RSA “78 00 71 64 72 43 32 00”, con p = 5, q = 17 y k=7.

P = 5

Q = 17

N = 85

Z = 64

K = 7

J = 55

* N = P \* Q → N = 5 \* 17 → N = 85
* Z = (P – 1) (Q – 1) → Z = 4 \* 16 → Z = 64
* (J \* K) mod z = 1 → (J \* 7) mod 64 → J = 43
* Clave pública (k,n) → Clave pública (7,85)
* Clave privada (j,n) → Clave priva (43,85)

M = Cj mod 85

* 78 → 7855 mod 85 → 22 → V
* 00 → 0055 mod 85 → 00 → A
* 71 → 7155 mod 85 → 11 → L
* 64 → 6455 mod 85 → 04 → E
* 72 → 7255 mod 85 → 13 → N
* 43 → 4355 mod 85 → 02 → C
* 32 → 3255 mod 85 → 08 → I
* 00 → 0055 mod 85 → 00 → A
* **El texto original es “VALENCIA”**