**ACTIVIDAD 15:**

Descifrar con el método César el siguiente mensaje si la clave es 8:

“OIKMZ BWLWA SWA MQMZKPKPWA LM AMÑCZPLIL”

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| S | 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 |

* **El texto original es “HACER TODOS LOS EJERCICIOS DE SEGURIDAD”**

**ACTIVIDAD 16:**

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| G | O | O | G | L | E |
| 2 | 5 | 6 | 3 | 4 | 1 |
| 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 |  |  |  |

1. OTGRAI
2. NSAUCSD
3. AAIIEU
4. MLNESR
5. OARNOEA
6. VFNMLGD

* **El criptograma es “OTGRAINSAUCSDAAIIEUMLNESR**
* **OARNOEAVFNMLGD**

**ACTIVIDAD 17:**

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

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| U | N | I | V | E | R | S | I | D | A | D |
| 10101 | 01110 | 01001 | 10110 | 00101 | 10010 | 10011 | 01001 | 00100 | 00001 | 00100 |
| I | O | R | D | B | E | H | H | T | T | A |
| 01001 | 01111 | 10010 | 00100 | 00010 | 00101 | 01000 | 01000 | 10100 | 10100 | 00001 |
| 11100 | 00001 | 11011 | 10010 | 00111 | 10111 | 11011 | 00001 | 10000 | 10101 | 00101 |
|  | A |  | R | G | W |  | A | P | U | E |

* **El mensaje cifrado es “\_A\_RGW\_APUE”**

**Actividad 18:**

Cifrar el siguiente mensaje con el algoritmo rsa “flores”, p = 11 y q = 7.

p = 11

q = 7

n = 77

z = 60

k = 7

j = 43

n = p \* q → n = 11 \* 7 → n = 77

z = (p – 1) (q – 1) → z = (11 – 1) (6 – 1) → z = 60

k = co-primo no divisor de z → k = 7

(k \* j) mod z = 1 → (7 \* j) mod 60 = 1 → j = 43

Clave pública (k, n) → Clave pública (7,77)

Clave privada (j, n) → Clave privada (43,77)

C = M ^ K mod n

* F → 5 ^ 7 mod 77 → 47
* L → 11 ^ 7 mod 77 → 11
* O → 15 ^ 7 mod 77 → 71
* R → 18 ^ 7 mod 77 → 39
* E → 4 ^ 7 mod 77 → 60
* S → 19 ^ 7 mod 77 → 68
* **El mensaje cifrado es “47 11 71 39 60 68”**

**ACTIVIDAD 19:**

Descifrar el siguiente mensaje con el algoritmo RSA “21 00 03 05 18 15 00 06 01”, p = 11, q = 17 y k = 3.

p = 11

q = 17

n = 187

z = 160

k = 3

j = 107

n = p \* q → n = 11 \* 17 → n = 187

z = (p - 1) (q – 1) → z = (11 - 1) (17 – 1) → z = 160

(k \* j) mod z = 1 → (3 \* j) mod 160 = 1 → j = 107

Cave publica (k, n) → Clave pública (3, 187)

Clave privada (j, n) → Clave privada (107, 187)

M = C ^ J mod n

* 21 → 21^107 mod 187 → 98
* 00 → 0^107 mod 187 → 00
* 03 → 3^107 mod 187 → 75
* 05 → 5^107 mod 187 → 113
* 18 → 18^107 mod 187 → 171
* 15 → 15^107 mod 187 → 60
* 00 → 0^107 mod 187 → 00
* 06 → 6^107 mod 187 → 107
* 01 → 1^107 mod 187 → 01
* **El mensaje cifrado es “98 00 75 113 171 60 00 107 01”**