**ACTIVIDAD 5:**

Cifrar el siguiente mensaje con el cifrado de Vernam “EXAMENES”, la clave es “ROFTAACV”.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Texto original | E | X | A | M | E | N | E | S |
| Binario | 00101 | 11000 | 00001 | 01101 | 00101 | 01110 | 00101 | 10011 |
| Clave | R | O | F | T | A | A | C | V |
| Binario | 10010 | 01111 | 00110 | 10100 | 00001 | 00001 | 00011 | 10110 |
| XOR | 10111 | 10111 | 00111 | 11001 | 00100 | 01111 | 00110 | 00101 |
| Texto cifrado | W | W | G | Y | D | N | F | E |

* El criptograma es WWGYDNFE.

**ACTIVIDAD 6:**

Descifrar el siguiente mensaje con el cifrado de Vernam “FFNEJWCHGR”, la clave es “RILDFTBACW”.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Texto cifrado | F | F | N | E | J | W | C | H | G | R |
| Binario | 00110 | 00110 | 01110 | 00101 | 01010 | 10111 | 00011 | 01000 | 00111 | 10010 |
| Clave | R | I | L | D | F | T | B | A | C | W |
| Binario | 10010 | 01001 | 01100 | 00100 | 00110 | 10100 | 00010 | 00001 | 00011 | 10111 |
| XOR | 10100 | 01111 | 00010 | 00001 | 01100 | 00011 | 00001 | 01001 | 00100 | 00101 |
| Texto original | T | O | B | A | L | C | A | I | D | E |

* El texto plano es TOBALCAIDE.

**ACTIVIDAD 7:**

Cifrar el siguiente mensaje con el algoritmo RSA “TOBALCAIDE”, p = 5 y q = 23.

* n = p \* q → n = 5 \* 23 → n = 115

p = 5

q = 23

n = 115

z = 88

k = 3

j = 59

* z = (p – 1) (q – 1) → z = (5 – 1) (23 – 1) → z = 88
* k → z % k != 0 → 88 % 3 != 0 → k = 3
* La clave pública es (k,n) → (3, 115)
* K \* j = 1 (mod z) → 3 \* j = 1 (mod 88) → j = 59
* La clave privada es (j,n) → (59, 115)

Cifrado:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| 0 | 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 |

C = MK mod n

* T = 20 → 203 mod 115 → 65
* O = 15 → 153 mod 115 → 40
* B = 1 → 13 mod 115 → 1
* A = 0 → 03 mod 115 → 0
* L = 11 → 113 mod 115 → 66
* C = 2 → 23 mod 115 → 8
* A = 0 → 03 mod 115 → 0
* I = 8 → 83 mod 115 → 52
* D = 3 → 33 mod 115 → 27
* E = 4 → 43 mod 115 → 64
* El criptograma es 65 40 1 0 66 8 0 52 27 64

**ACTIVIDAD 8:**

Descifrar el siguiente mensaje con el algoritmo RSA “15 21 15 16 04 13 05 26 05 19 15”, p = 2, q = 17 y k = 5.

p = 2

q = 17

n = 34

z = 16

k = 5

j = 13

* n = p \* q → n = 2 \* 17 → n = 34
* La clave pública (k,n) → (5,34)
* z = (p – 1) (q -1) → z = (2 – 1) (17 - 1) → z = 16
* (k \* j) % z = 1 → (5 \* j) % 16 = 1 → (5 \* 13) % 16 = 1 → j = 13
* La clave privada (j,n) → (13,34)

Descifrado

* 15 → 1513 mod 34 → 19
* 21 → 2113 mod 34 → 21
* 15→ 1513 mod 34 → 19
* 16→ 1613 mod 34 → 16
* 04 → 0413 mod 34 → 4
* 13 → 1313 mod 34 → 13
* 05 → 0513 mod 34 → 3
* 26 → 2613 mod 34 → 8
* 05 → 0513 mod 34 → 3
* 19 → 1913 mod 34 → 15

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 19 | 21 | 19 | 16 | 4 | 13 | 3 | 8 | 3 | 15 |
| S | U | S | P | E | N | D | I | D | O |

* El texto plano es SUSPENDIDO