**Algoritmos**

Cifrado César (sustitución)

* Requiere de una clave (numérica) y se desplaza cada letra alfabéticamente según la clave

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

Ejemplo:

* Texto plano: “EL PRÓXIMO LUNES HAY EXAMEN DE SEGURIDAD”
* Clave: 9
* Texto cifrado: “NT YAXGQUX TDVNB PJH NGJUVNV MN BNODAQMJM”

Cifrado de la Cajas (transposición)

* Requiere una clave (una palabra) y se abre una tabla con la longitud de la palabra
* Luego se numera cada letra de la clave en orden alfabético y de izquierda a derecha

Ejemplo

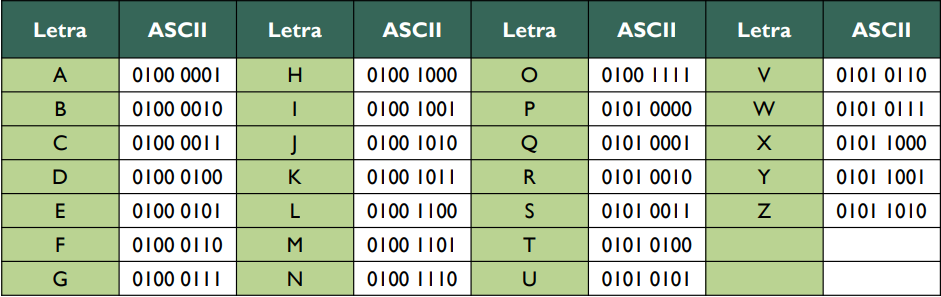
* Texto plano: “NO VAMOS A FALTAR NINGUN MIERCOLES A SEGURIDAD”
* Clave: “GOOGLE”
* Texto cifrado “OTGRAINSAUCSDAAIIEUMLNESROARNOEAVFNMLGD”

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| G | O | O | G | L | E   1. OTGRAI 2. NSAUCSD 3. AAIIEU 4. MLNESR 5. OARNOEA 6. VFNMLGD |
| 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 |  |  |  |

* Para descifrar se pone la clave y se numera igual que en el cifrado
* Tendremos que tener en cuenta la longitud del texto cifrado para saber cuantas letras van en cada columna

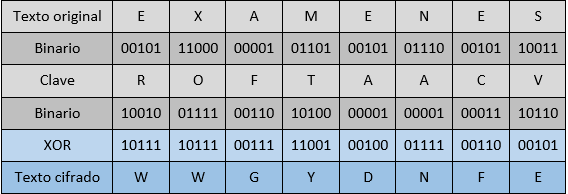
Cifrado de Vernam (simétrico y sustitución)

* Es necesario una clave de la misma longitud del texto plano
* Se realiza la operación XOR con los últimos 5 bits de la representación binaria de cada uno de los caracteres
* Para descifrar se realiza el mismo proceso con el texto cifrado y la clave



Ejemplo

* Texto plano: “EXAMENES”
* Clave: “ROFTAACV”
* Texto cifrado: “WWGYDNFE”



Cifrado RSA (asimétrico y sustitución)

* Se buscan dos primos diferentes (p, q)
* Se obtiene n = p \* q
* Se obtiene z = (p – 1) \* (q – 1)
* Se obtiene k que es un co-primo de z. Es decir, k tiene que ser primo y z no puede ser divisible por k
* Se obtiene j de la siguiente forma: (k \* j) mod z = 1

La clave pública es (k, n)

La clave privada es (j, n)

Cifrado

* Cada letra se pasa a un valor numérico
* C = M^k mod n

Descifrado

* M = C^j mod n
* Cada numero se pasa a una letra

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | Ñ | 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 |