Universidad Nacional de San juan

Facultad de Ciencias Exactas, Físicas y Naturales

Licenciatura en Ciencias de la Computación

Teoría de la información 2025

Integrantes:

-Lucero Matías

-Moya Lisandro

Práctico Criptografía Software: Criptool2, OpenPGP

1. *Cifrar con sustitución monoalfabética de Cesar (generalizada) el texto*

   AL PAN PAN, Y AL VINO...

   a) Para k=4

   Cifrando con un desplazamiento k=4, y utilizando el alfabeto de 27 símbolos, obtenemos:

   A -> E

   L -> O

   P -> T

   N -> Q

   Y -> C

   V -> Z

   I -> M

   O -> S

   Cifrando el texto original con estos desplazamientos:

   EO TEQ TEQ, C EO ZMQS

   b) Para k=18

   Realizando lo mismo con un desplazamiento 18, obtenemos:

   A -> R

   L -> C

   P -> H

   N -> E

   Y -> P

   V -> N

   I -> Z

   O -> G

   Cifrando el texto original con estos desplazamientos:

   RC HRE HRE, P RC NZEG

   ¿Este algoritmo presenta una estructura de grupo? Justifique su respuesta.

Sí. El conjunto de todas las transformaciones “desplazar k” (para k∈{0,…,m−1}, con m=27 si incluimos Ñ) bajo la **composición** de funciones forma un **grupo abeliano cíclico** isomorfo a (Zm,+):

- **Clausura:** componer dos desplazamientos Ea∘Eb da otro desplazamiento Ea+bmodm.
- **Asociatividad:** la composición de funciones es asociativa.
- **Identidad:** E0 (desplazamiento 0) deja todo igual.
- **Inverso:** el inverso de Ek es Em−k (desplazar m−k deshace k).
- **Conmutatividad:** Ea∘Eb=Eb∘Ea porque a+b≡b+a(modm).

Por lo tanto, las cifras de César con todas las claves forman un grupo (cíclico) y, en particular, un subgrupo del grupo simétrico de permutaciones sobre el alfabeto.

2. Dado el siguiente criptograma YAMNMYOAYPY, descifrarlo, sabiendo que fue cifrado con una sustitución monoalfabética de César cuya clave k es 12. Mantenga la misma estructura del algoritmo, es decir para descifrar utilice la fórmula Dk(mi)=ci-k-1mod(27).
Hallar el criptograma que se obtiene al aplicar el cifrado por el método de transposición de bloques de longitud n=7 y clave k=(3 7 2 6 4 1 5).

NO POR MUCHO MADRUGAR...

Descifrando con la fórmula $Mi = (Ci - k)\ mod\ 27$,

Reemplazando en la fórmula para cada caracter:

$$My = (Cy - k)\ mod\ 27 = (25 - 12)\ mod\ 27 = 13 =$$

Es decir $Y \rightarrow N$

Así con cada letra:

$$Ma = (0 - 12)\ mod\ 27 = 15, A \rightarrow O$$

$$Mm = (12 - 12\ )\ mod\ 27 = 0, M \rightarrow A$$

$$Mn = (13 - 12)\ mod\ 27 = 1, N \rightarrow B$$

$$Mo = (15 - 12)\ mod\ 27 = 3, O \rightarrow D$$

$$Mp = (16 - 12)\ mod\ 27 = 4, P \rightarrow E$$

Ahora descifrando el criptograma:

YAMNMYOAYPY → NOABANDONEN

Ahora aplicando transposición de bloques, primero, eliminamos los espacios del texto, y luego, dividimos el texto en bloques de longitud 7.

$$NO\ POR\ MUCHO\ MADRUGAR \rightarrow NOPORMUCHOMADRUGAR$$

1er bloque:

$$NOPORMU$$

2do bloque:

$$CHOMADR$$

3er bloque:

$$UGAR\ (En\ este\ caso, rellenamos\ con\ X\ para\ que\ alcance\ la\ longitud\ 7) = UGARXXX$$

Ahora realizando las transposiciones con la clave k:

1er bloque: $NOPORMU \rightarrow PUOMONR$

2do bloque: $CHOMADR \rightarrow ORHDMCA$

3er bloque: $UGARXXX \rightarrow AXGXRUX$

Obteniendo el criptograma:

$$PUOMONRORHDMCAAXGXRUX$$

3. Para el ejercicio anterior encuentre la clave de descifrado y aplíquela al texto cifrado para volver al texto en claro

Para encontrar la clave de descifrado, debemos invertir la clave original, es decir, devolver a las posiciones originales los caracteres transpuestos:

Tal que:

$$Código\ original \rightarrow k = (3\ 7\ 2\ 6\ 4\ 1\ 5)$$

Así, en k original, la primera posición se transponía a la tercera, la segunda a la séptima, y así sucesivamente hasta completar el bloque.

Entonces invirtiendo la transposición:

$$Clave\ de\ descifrado \rightarrow k = (6\ 3\ 1\ 5\ 7\ 4\ 2)$$

Realizando el mismo procedimiento que antes, de dividir el bloque en longitudes de n=7, y aplicar la clave:

$$PUOMONRORHDMCAAXGXRUX$$

1er bloque: $PUOMONR \rightarrow NOPORMU$

2do bloque: $ORHDMCA \rightarrow CHOMADR$

3er bloque: $AXGXRUX \rightarrow UGARXXX$

Obteniendo: $NOPORMUCHOMADRUGAR \rightarrow (Colocando\ espacios\ y\ borrando\ las\ X) \rightarrow NO\ POR\ MUCHO\ MADRUGAR$

4. Un sistema de cifrado que usa el método de sustitución polialfabética de Vigenère, es vulnerado, interceptando un mensaje del que se dispone el criptograma y el mensaje en claro. Sabiendo que la clave tiene longitud 8 y que la pareja mensaje en claro y criptograma son los siguientes: Mensaje en claro:

ESLOINESPERADOLOQUESIEMPREOCURRE

Criptografía:

GHVDAFYLRSCOVHFHSJOHAWGITSZQNKMW

5. Encontrar la clave de cifrado y verificarla para todo el mensaje.

Primero, debemos separar y comparar los textos, en bloques de longitud 8, utilizando la fórmula tal que para cifrar con k es:

$$Ci = (Mi + Ki)\ mod\ 27$$

Entonces para obtener Ki es:

$$Ki = (Ci - Mi)\ mod\ 27$$

Aplicando en cada bloque para cada símbolo, obtenemos:

1er bloque: $\frac{ESLOINES}{GHVDAFYL} \rightarrow COLOSSUS$

2do bloque: $\frac{PERADOLO}{RSCOVHFH} \rightarrow COLOSSUS$

3er bloque: $\frac{QUESIEMP}{SJOHAWGI} \rightarrow COLOSSUS$

4to bloque: $\frac{REOCURRE}{TSZQNKMW} \rightarrow COLOSSUS$

Así, nuestro K final es K=COLOSSUS, de tal forma que, si dividimos el mensaje en bloques de longitud 8, y lo sumamos con la palabra COLOSSUS, obtendremos el mensaje encriptado.

6. ¿Una transposición de una transposición es más segura que una transposición sola?

Sí, es más segura ya que requerirá, descifrar dos claves para poder llegar al mensaje original desde el mensaje encriptado, por lo que es más laborioso de realizar que descifrar únicamente una única clave. Por lo tanto, la complejidad aumentaría exponencialmente.

7. Un criptoanalista intercepta un mensaje cifrado MXDQLWR, y sabe que el emisor solo puede haber enviado uno de los siguientes mensajes: JORGITO, JUANITO o JAIMITO. También sabe que para cifrar, sumó el mismo número a todas las letras del texto en claro (no utilizó la letra Ñ).

Como vemos, se utilizó un Sistema César, para cifrar el mensaje original, por lo que se basa en un desplazamiento de un número en todas las letras.

Para llevar a cabo el descifrado, y al saber el posible mensaje original, debemos desplazar el mensaje encriptado hasta encontrar el mensaje original correspondiente.

Así, probamos con hacer concordar el primer caracter del encriptado con la J, ya que los posibles mensajes, todos comienzan con J, y obtenemos:

$$Mi = (Ci - b)\ mod\ 27$$

Reemplazando para J

$$Mj = (Cj - b)\ mod\ 27 = (12 - 3)\ mod\ 27 = 9$$

Así obtenemos J el primer caracter, y obtenemos que el desplazamiento es 3.

Realizando el desplazamiento inverso para el resto de letras:

$$MXDQLWR \rightarrow JUANITO$$

Así, el mensaje original es $JUANITO$

8. El siguiente sistema es una variante del sistema de César, para cifrar un mensaje, que lo divide en bloques de k caracteres, cada bloque lo transforma en un número x y el mensaje encriptado está dado por la sucesión de los números EK(mi)=ami+bmod(N), donde N debe ser mayor que el más grande valor posible de mi y a debe tener inverso módulo N. La clave es el par (a,b). N lo consideramos fijo. Alternativamente, en lugar de los números ci, estos pueden codificarse otra vez como bloques de caracteres que se envían en forma de un mensaje sin sentido. Esto presenta la dificultad de que algunos códigos pueden no tener representación escrita, como sucede en ASCII.

a. Para N fijo, ¿cuántas claves diferentes pueden hallarse si N es un número primo?

Se pueden hallar n*(N-1) claves diferentes, siendo n la cantidad de números a, tal que a sea coprimos de N, entonces b puede tomar cualquier valor entre 0 y N.

b. Se considera N=131, a=3 y b=7. Codificar el siguiente mensaje donde los bloques son formados con un solo caracter sin tener en cuenta espacios en blanco: ***HAY GENTE QUE DE SU CIENCIA TIENE LA CABEZA LLENA***

Primero, borramos los espacios en blanco y obtenemos:

HAYGENTEQUEDESUCIENCIATIENELACABEZALLENA

Aplicamos el sistema de cifrado:

$$Ek(mi) = 3 * mi + 7\ mod(131)$$

Donde mi va a ser el código de la letra en el alfabeto.

$$H \rightarrow Ch = 3 * 7 + 7\ mod(131) = 28$$

$$A \rightarrow Ca = 3 * 0 + 7\ mod(131) = 7$$

$$Y \rightarrow Cy = 3 * 25 + 7\ mod(131) = 82$$

$$G \rightarrow Cg = 3 * 6 + 7\ mod(131) = 25$$

$$E \rightarrow Ce = 3 * 4 + 7\ mod(131) = 19$$

$$N \rightarrow Cn = 3 * 13 + 7\ mod(131) = 46$$

$$T \rightarrow Ct = 3 * 20 + 7\ mod(131) = 67$$

$$Q \rightarrow Cq = 3 * 17 + 7\ mod(131) = 58$$

$$U \rightarrow Cu = 3 * 21 + 7\ mod(131) = 70$$

$$D \rightarrow Cd = 3 * 3 + 7\ mod(131) = 16$$

$$S \rightarrow Cs = 3 * 19 + 7\ mod(131) = 64$$

$$C \rightarrow Cc = 3 * 2 + 7\ mod(131) = 13$$

$$I \rightarrow Ci = 3 * 8 + 7\ mod(131) = 31$$

$$L \rightarrow Cl = 3 * 11 + 7\ mod(131) = 40$$

$$B \rightarrow Cb = 3 * 1 + 7\ mod(131) = 10$$

$$Z \rightarrow Cz = 3 * 26 + 7\ mod(131) = 85$$

Codificando el mensaje:

28 7 82 25 19 46 67 19 58 70 19 16 19 64 70 13 31 19 46 13 31 7 67 31 19 46 19 40 7 13 7 10 19 85 40 40 7

c. Hallar la función inversa Dk(mi)=a-1ci-d mod(N) de Ek(mi)=ami+b mod(N) que permita el desencriptado del mensaje anterior.

Primero, debemos buscar el inverso a^{-1}, tal que:

El inverso de a * a^{-1} = 1 (mod N) = 1 (mod 131)

Siendo a = 3, entonces:

3 * a^{-1} = 1 (mod 131)

a^{-1} = 44

Tal que:

$$3 * 44\ (mod\ 131) = 1$$

Así con la fórmula del descifrador, como d=7, obtenemos:

$$Di(mi) = a^{-1} * (ci - d)\ mod(131)$$

Reemplazando para cada número:

$$28 \rightarrow M28 = 44 * (28-7)\, mod(131) = 7 \rightarrow H$$
$$7 \rightarrow M7 = 44 * (7-7)\, mod(131) = 0 \rightarrow A$$
$$82 \rightarrow M82 = 44 * (82-7)\, mod(131) = 25 \rightarrow Y$$
$$25 \rightarrow M25 = 44 * (25-7)\, mod(131) = 6 \rightarrow G$$
$$19 \rightarrow M19 = 44 * (19-7)\, mod(131) = 4 \rightarrow E$$
$$46 \rightarrow M46 = 44 * (46-7)\, mod(131) = 13 \rightarrow N$$
$$67 \rightarrow M67 = 44 * (67-7)\, mod(131) = 20 \rightarrow T$$
$$19 \rightarrow M19 = 44 * (19-7)\, mod(131) = 4 \rightarrow E$$
$$58 \rightarrow M58 = 44 * (58-7)\, mod(131) = 17 \rightarrow Q$$
$$70 \rightarrow M70 = 44 * (70-7)\, mod(131) = 21 \rightarrow U$$
$$19 \rightarrow M19 = 44 * (19-7)\, mod(131) = 4 \rightarrow E$$
$$16 \rightarrow M16 = 44 * (16-7)\, mod(131) = 3 \rightarrow D$$
$$19 \rightarrow M19 = 44 * (19-7)\, mod(131) = 4 \rightarrow E$$
$$64 \rightarrow M64 = 44 * (64-7)\, mod(131) = 19 \rightarrow S$$
$$70 \rightarrow M70 = 44 * (70-7)\, mod(131) = 21 \rightarrow U$$
$$13 \rightarrow M13 = 44 * (13-7)\, mod(131) = 2 \rightarrow C$$
$$31 \rightarrow M31 = 44 * (31-7)\, mod(131) = 8 \rightarrow I$$
$$19 \rightarrow M19 = 44 * (19-7)\, mod(131) = 4 \rightarrow E$$
$$46 \rightarrow M46 = 44 * (46-7)\, mod(131) = 13 \rightarrow N$$
$$13 \rightarrow M13 = 44 * (13-7)\, mod(131) = 2 \rightarrow C$$
$$31 \rightarrow M31 = 44 * (31-7)\, mod(131) = 8 \rightarrow I$$
$$7 \rightarrow M7 = 44 * (7-7)\, mod(131) = 0 \rightarrow A$$
$$67 \rightarrow M67 = 44 * (67-7)\, mod(131) = 20 \rightarrow T$$
$$31 \rightarrow M31 = 44 * (31-7)\, mod(131) = 8 \rightarrow I$$
$$19 \rightarrow M19 = 44 * (19-7)\, mod(131) = 4 \rightarrow E$$
$$46 \rightarrow M46 = 44 * (46-7)\, mod(131) = 13 \rightarrow N$$
$$19 \rightarrow M19 = 44 * (19-7)\, mod(131) = 4 \rightarrow E$$
$$40 \rightarrow M40 = 44 * (40-7)\, mod(131) = 11 \rightarrow L$$
$$7 \rightarrow M7 = 44 * (7-7)\, mod(131) = 0 \rightarrow A$$
$$13 \rightarrow M13 = 44 * (13-7)\, mod(131) = 2 \rightarrow C$$
$$7 \rightarrow M7 = 44 * (7-7)\, mod(131) = 0 \rightarrow A$$
$$10 \rightarrow M10 = 44 * (10-7)\, mod(131) = 1 \rightarrow B$$
$$19 \rightarrow M19 = 44 * (19-7)\, mod(131) = 4 \rightarrow E$$
$$85 \rightarrow M85 = 44 * (85-7)\, mod(131) = 26 \rightarrow Z$$
$$7 \rightarrow M7 = 44 * (7-7)\, mod(131) = 0 \rightarrow A$$
$$40 \rightarrow M40 = 44 * (40-7)\, mod(131) = 11 \rightarrow L$$
$$40 \rightarrow M40 = 44 * (40-7)\, mod(131) = 11 \rightarrow L$$
$$19 \rightarrow M19 = 44 * (19-7)\, mod(131) = 4 \rightarrow E$$
$$46 \rightarrow M46 = 44 * (46-7)\, mod(131) = 13 \rightarrow N$$
$$7 \rightarrow M7 = 44 * (7-7)\, mod(131) = 0 \rightarrow A$$

Recuperando el mensaje:

HAY GENTE QUE DE SU CIENCIA TIENE LA CABEZA LLENA

d. Desencriptar el mensaje siguiente encriptado en dicho sistema por bloques de un caracter, sabiendo que N=131, el último número corresponde a un símbolo de puntuación y que los caracteres más frecuentes en idioma Castellano son, por su orden: e, a, o, l, s. No se consideran espacios en blanco. Se trabaja en ASCII. 42, 109, 49, 100, 19, 69, 99, 89, 129, 100, 60, 79, 99, 100, 59, 90, 100, 99, 49, 129, 80, 130, 69, 100, 39, 60, 79, 99, 100, 59, 90, 100, 99, 80, 69, 109, 60, 109, 70, 129, 100, 59, 60, 109, 74

Primero, calculamos la frecuencia de cada número y ordenamos por frecuencia:

100 → 7 veces

99 → 5 veces

60 → 4 veces

109 → 4 veces

59 → 3 veces

69 → 3 veces

129 → 3 veces

49 → 2 veces

79 → 2 veces

80 → 2 veces

90 → 2 veces

19, 39, 42, 70, 74, 89, 130 → 1 vez cada uno

Tomando en cuenta que el último número, 74, representa un símbolo de puntuación, el cual, probablemente, al ser el final del mensaje, represente un ".".

Y suponiendo que, el número 100 representa E:

Buscamos el descifrador:

$$Di = a^{-1} * (ci - d)\ mod\ (131) = mi$$

Reemplazando:

$$Di = a^{-1} * (74 - d)\ mod\ (131) = 46$$

$$Di = a^{-1} * (100 - d)\ mod (131) = 101$$

Despejando de la fórmula de codificación:

$$m = a - 1(c - b)\ mod\ 131$$

Reemplazando:

$$74 = a * 46 + b\ mod\ (131)$$

$$100 = a * 101 + b\ mod\ (131)$$

Así, obtenemos dicho sistema, restando entre ambos elementos:

$$100 - 74 = a(101 - 46)\ mod\ 131$$

$$26 = 55a\ mod\ 131$$

$$a = 26 * 55^{-1}\ mod\ 131$$

Calculando 55^{-1}

Obteniendo $55 * x$ tal que su módulo de 131, de 1, es decir, el resto es 1.

Así, x resulta en 81, volviendo al cálculo original:

$$a = 26 * 81 \; mod \; 131$$

$$a = 10$$

Ahora reemplazando en cualquier fórmula para obtener b:

$$100 = 10 * 101 + b \; mod \; 131$$

Entonces:

$$b = 7$$

Y calculamos el a^{-1}:

$$a * a^{-1} = x \; mod \; 131 = 1$$

$$10 * 118 \; mod \; 131 = 1$$

$$a^{-1} = 118$$

Así, obtenemos el descifrador:

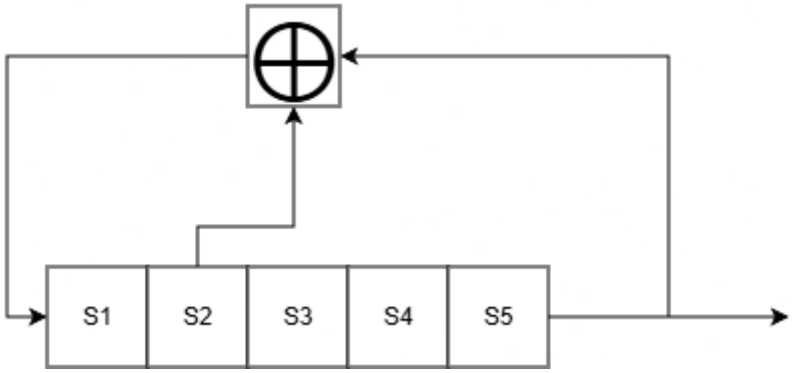
$$Di = 118 * (ci - 7) \; mod \; 131$$

Descifrando el mensaje, recuperamos el mensaje:

$$Es \; mejor \; que \; aprender \; mucho \; el \; aprender \; cosas \; buenas.$$

9. Para el polinomio primitivo f(x) = x5 + x2 + 1, se pide:

a. Dibujar el registro de desplazamientos LSFR



b. Si la semilla es S=10000, encontrar la secuencia cifrante. ¿Cuál es su período?

Empezando a partir de la semilla S=10000, a realizar la retroalimentación para obtener toda la secuencia cifrante:

Registro → Bit Si

$10000 \rightarrow 0$	$10111 \rightarrow 1$	$11110 \rightarrow 0$	$01011 \rightarrow 1$
$01000 \rightarrow 0$	$11011 \rightarrow 1$	$11111 \rightarrow 1$	$00101 \rightarrow 1$
$10100 \rightarrow 0$	$01101 \rightarrow 1$	$01111 \rightarrow 1$	$10010 \rightarrow 0$
$01010 \rightarrow 0$	$00110 \rightarrow 0$	$00111 \rightarrow 1$	$01001 \rightarrow 1$
$10101 \rightarrow 1$	$00011 \rightarrow 1$	$10011 \rightarrow 1$	$00100 \rightarrow 0$
$11010 \rightarrow 0$	$10001 \rightarrow 1$	$11001 \rightarrow 1$	$10000 \rightarrow 0$
$11101 \rightarrow 1$	$11000 \rightarrow 0$	$01100 \rightarrow 0$	$00010 \rightarrow 0$
$01110 \rightarrow 0$	$11100 \rightarrow 0$	$10110 \rightarrow 0$	$00001 \rightarrow 1$
			$10000 \rightarrow 0$

Así, la secuencia se repite de vuelta en el estado 31.

Tal que su período máximo, T, es:

$$Tmax = 2^n - 1 = 2^5 - 1 = 31$$

c. Con la secuencia cifrante, cifrar ENIGMA (considere el alfabeto ASCII para la representación del mensaje).

Para empezar, obtenemos cada letra del mensaje en binario, tal que:

“ENIGMA” → códigos ASCII decimales:

- $E = 69 \rightarrow 01000101$
- $N = 78 \rightarrow 01001110$
- $I = 73 \rightarrow 01001001$
- $G = 71 \rightarrow 01000111$
- $M = 77 \rightarrow 01001101$
- $A = 65 \rightarrow 01000001$

Son 6 caracteres × 8 bits = 48 bits.

Necesitamos 48 bits de secuencia cifrante, así que repetimos el LFSR y tomamos los primeros 48 bits que genera:

Keystream (48 bits):

K= **00001010 11101100 01111100 11010010 00010101 11011000**

Hacemos C=P⊕K carácter por carácter:

1. **E**
    - PE=01000101

- K1=00001010
- CE=01001111 → **79**

2. **N**
   - PN=01001110
   - K2=11101100
   - CN=10100010 → **162**
3. **I**
   - PI=01001001
   - K3=01111100
   - CI=00110101 → **53**
4. **G**
   - PG=01000111
   - K4=11010010
   - CG=10010101 → **149**
5. **M**
   - PM=01001101
   - K5=00010101
   - CM=01011000 → **88**
6. **A**
   - PA=01000001
   - K6=11011000
   - CA=10011001 → **153**

Entonces el texto cifrado en:

- **Decimal ASCII**:

(79, 162, 53, 149, 88, 153)

- **Hex**:

(4F, A2, 35, 95, 58, 99)

10. Para un sistema de cifra RSA con p=97 y q=31, se nos dice que podemos usar cualquiera de las siguientes claves públicas.
a) e=24, b) e=33, c) e=45, d) e=49
¿Cuáles de ellas son válidas y cuáles no? Justifique su respuesta.

En este caso, se debe elegir una clave pública e, tal que cumpla:

$$mcd\ [e, \varphi(n)]\ =\ 1$$

Verificando para cada e elegido:

$$\varphi(n) = \varphi(97 * 31) = (97 - 1) * (31 - 1) = 2880$$

a) $mcd\ [e, \varphi(n)] = mcd\ [24, 2880] = 24$
b) $mcd\ [e, \varphi(n)] = mcd\ [33, 2880] = 3$
c) $mcd\ [e, \varphi(n)] = mcd\ [45, 2880] = 45$
d) $mcd\ [e, \varphi(n)] = mcd\ [49, 2880] = 1$

Tal así, quedando que la única opción que cumple dicha condición, es el d) e=49.

11. Paco y Lola se envían mensajes por correo electrónico que desean se mantengan en secreto. Además, para evitar los malentendidos y una que otra sorpresa desagradable, todos los mensajes los firman digitalmente. Para todo el proceso utilizan el alfabeto de 28 elementos constituidos por las letras A=0, B=1, ..., Ñ=14, ..., Z=26, y el espacio en blanco (Blanco=27). El sistema de cifra que utilizan en RSA. El grupo de trabajo de cada uno de ellos es:
*PACO: ℤnP= 7 * 5 = 35 ϴp=11*
*LOLA: ℤnP= 3 * 11 = 33 ϴp=7*

12. Después de una fuerte discusión, Paco envía a Lola el mensaje "SI", a lo que Lola contesta con el mensaje "NO". Ambos firman el primer carácter enviado, es decir la letra S para Paco, y la letra N para Lola. Se pide:

a. Enviar los dos mensajes cifrados. Paco: MPaco=M1Paco,M2Paco y Lola: MLola=M1Lola,M2Lola.

Dado el grupo de trabajo de cada uno, podemos con los datos brindados, cifrar el mensaje:

$$Paco: n = 35, p = 7, q = 5, Clave\ pública\ de\ Paco = 11$$

$$Lola: n = 33, p = 3, q = 11, Clave\ pública\ de\ Lola = 7$$

Mensaje de Paco: SI

$$S \rightarrow 19$$

$$I \rightarrow 8$$

Ciframos utilizando la clave pública de Lola.

Aplicando la fórmula:

$$C = M^{clave\ pública\ de\ Lola}\ mod\ n_{de\ Lola}$$

$$Cs =\ 19^7\ mod\ 33 =\ 13$$

$$Ci = 8^7 \ mod \ 33 = 2$$

Entonces, SI quedaría cifrado:

$$S\ (19) \rightarrow 13, I\ (8) \rightarrow 2$$

$$SI \rightarrow 13\ 2$$

Realizando lo mismo para Lola: NO

$$N \rightarrow 13$$

$$O \rightarrow 15$$

Ciframos con la clave pública de Paco:

$$C = M^{clave\ pública\ de\ Paco} \ mod \ n_{de\ Paco}$$

$$Cn = 13^{11} \ mod \ 35 = \ 27$$

$$Co = 15^{11} \ mod \ 35 = \ 15$$

$$N(13) \rightarrow 27, \qquad O(15) \rightarrow 15$$

$$NO \rightarrow 27\ 15$$

b. Firmar cada uno de los mensajes.

Ahora, si deseamos firmar cada uno de los mensajes, tal que la primera letra esté firmada digitalmente por cada uno.

Debemos firmar la primera letra con la clave privada de cada uno.

Tal que para Paco:

Utilizamos su clave privada para el primer carácter:

$$Firma = \ M^d \ mod \ n$$

Entonces, debemos obtener la clave privada de paco, tal que:

$$\varphi(n) = \varphi(7 * 5) = (7 - 1)(5 - 1) = 24$$

$$mcd\ [e, \varphi(n)] = mcd\ [11, 24] = 1$$

$$d = inv(11{,}24) = 11$$

$$S \rightarrow 19$$

$$Firma\ Paco = 19^{11} \ mod \ 35 = 24$$

Realizando lo mismo para Lola:

$$\varphi(n) = \varphi(3 * 11) = (3 - 1)(11 - 1) = 30$$

$$mcd\ [e, \varphi(n)] = mcd\ [7, 30] = 1$$

$$d = inv(7{,}30) = 13$$

$$N \rightarrow 13$$

$$Firma\ Lola = 13^{13}\ mod\ 33 = 19$$

Así, quedaría cada mensaje cifrado con firma:

Mensaje de Paco:

$$SI \rightarrow (24, 13, 2)$$

Y de Lola:

$$NO \rightarrow (19, 27, 15)$$

c. *Descifrar los criptogramas y comprobar la firma en cada caso*

Ahora, procedemos a descodificar el mensaje, y a verificar la firma.

A Lola, le llega el mensaje de Paco $(24, 13, 2)$:

Entonces, utilizando su clave privada, puede desencriptar el mensaje:

Recordando que la clave privada de Lola es d=13.

$$Tal\ que\ M = C^{clave\ privada\ de\ Lola}\ mod\ n_{de\ Lola} \rightarrow M = 13^{13}\ mod\ 33 = \ 19$$

$$19 \rightarrow S$$

$$M = 2^{13}\ mod\ 33 = 8$$

$$8 \rightarrow I$$

Y ahora verificamos la firma de Paco, utilizando su clave pública:

$$M = C^{clave\ pública\ de\ Paco}\ mod\ n_{de\ Paco} = 24^{11}\ mod\ 35 = \ 19$$

$$19 \rightarrow S$$

Entonces, como la firma concuerda con el carácter firmado, se confirma que el mensaje es de Paco.

Realizamos lo mismo para Paco:

A Paco, le llega el mensaje de Lola $(19, 27, 15)$:

Entonces, utilizando su clave privada, puede desencriptar el mensaje:

Recordando que la clave privada de Paco es d=11.

$$Tal\ que\ M = C^{clave\ privada\ de\ Paco}\ mod\ n_{de\ Paco} \rightarrow M = 27^{11}\ mod\ 35 = \ 13$$

$$13 \rightarrow N$$

$$M = 15^{11}\ mod\ 35 = 15$$

$$15 \rightarrow O$$

Y ahora verificamos la firma de Lola, utilizando su clave pública:

$$M = C^{clave\ pública\ de\ Lola}\ mod\ n_{de\ Lola} = 19^7\ mod\ 33 = \ \text{^}13$$

$$13 \rightarrow N$$

Entonces, como la firma concuerda con el carácter firmado, se confirma que el mensaje es de Lola.

13. Si la clave pública del receptor de un criptosistema RSA es el par (n, e) = (2291; 17), el mensaje capturado por el intruso es: 575, encontrar la clave para descifrar el mensaje, par (n, d) = (2291, d), descifrar el mensaje. Indique a qué letra del ASCII corresponde el valor encontrado.

*Pista: busque en internet el algoritmo de Fermat para encontrar los factores primos p y q, esto es n=p*q. Codifique en un lenguaje de programación a su elección, el algoritmo de Fermat.*

Algoritmo de Fermat:

```python
import math

def fermat_factor(n):
    if n % 2 == 0:
        return 2, n // 2

    a = math.isqrt(n)
    if a * a < n:
        a += 1

    while True:
        b2 = a * a - n
        b = int(math.isqrt(b2))
        if b * b == b2:
            return (a - b, a + b)
        a += 1



if __name__ == "__main__":
    n=int(input("Ingrese el valor de n\n"))
    p, q = fermat_factor(n)
    print("p =", p, "q =", q)
```

Lo primero que debemos obtener es la clave privada del receptor, para así, poder decodificar el mensaje del emisor.
Así, utilizando el algoritmo de Fermat, podemos obtener p y q:

$$n = p * q$$
$$2291 = 29 * 79$$

Ahora, con los datos obtenidos, calculamos la clave privada del receptor:

$$\varphi(n) = \varphi(29 * 79) = (29 - 1)(79 - 1) = 2184$$

$$mcd\,[e, \varphi(n)] = mcd\,[17, 2184] = 1$$

$$d = inv(17{,}2184) = 257$$

Ahora con la clave privada del receptor, desciframos el mensaje del emisor:

$$M = C^d\ mod\ n_{del\ receptor} = 575^{257}\ mod\ 2291 = 65$$

$$Tal\ que\ 65 \rightarrow A\ en\ ASCII$$

14. Intente romper el criptosistema RSA con clave pública (n, e) = (536813567; 3602561), con el software que escribió en el ejercicio anterior. Para romperlo, encuentre la clave d, que permita descifrar todo mensaje cifrado con la clave pública.

Utilizando el algoritmo anterior, podemos obtener n = p*q, así utilizando el código, obtenemos:

$$n = p * q$$

$$536813567 = 8191 * 65537$$

$$\varphi(n) = \varphi(8191 * 65537) = (8191 - 1)(65537 - 1) = 536739840$$

$$mcd\,[e, \varphi(n)] = mcd\,[3602561, 536739840] = 1$$

$$d = inv(17{,}2184) = 201934721$$

15. INVESTIGACIÓN:

a. Investigue algún algoritmo para el cálculo rápido de potencias, para usar en expresiones xm mod(n).

Un algoritmo bueno para calcular potencias enteras de un número x dado, de manera rápida, es la exponenciación binaria, la cual se basa en las tres propiedades de la potencia:

$$x^1 = x$$

$$x^{a+b} = x^a x^b$$

$$x^{a*b} = (x^a)^b$$

Usando a = n-1 y b=1 en la ecuación, se sigue que $x^n = x^{n-1}x$. Tomando a = n/2 y b/2 en la ecuación se obtiene que $x^n = (x^{\frac{n}{2}})$^2

De manera que, el algoritmo calcula x^n para un natural n dado:

$$x^n = \begin{cases} x & \text{si } n = 1 \\ x^{\frac{n}{2}} \times x^{\frac{n}{2}} & \text{si } n \text{ es par} \\ x \times x^{n-1} & \text{si } n \text{ es impar} \end{cases}$$

Comparado con el método original de multiplicar por sí mismo veces, este algoritmo sólo utiliza *O(log n)* multiplicaciones y acelera el cálculo de tremendamente; más o menos de la misma forma que el algoritmo de la *multiplicación* acelera una multiplicación sobre el método más lento de realizar una suma repetida.

b. *Investigue algún algoritmo para factorizar un número natural N.*

Un algoritmo de factorización en números primos es un algoritmo que dado un número natural mayor que 1 genera la lista de números primos que componen la factorización del mismo. El más sencillo de entender e implementar en una computadora es el algoritmo de división por tentativa y sus variantes.

El algoritmo más sencillo y común para la factorización de enteros es la **división por tentativa**. Consiste en intentar dividir *n* entre todo número primo menor o igual a *n*. Si se encuentra un primo que es divisor de *n*, en división entera, ese número es un factor de *n*.

Si *n* es el número a factorizar, el algoritmo devuelve una lista de números primos factores de *n*. Si *n* = 1, entonces el número no es factorizable por ningún número primo (es 1).

```
algoritmo factorización (n)
  si n = 1
     devolver n
  sino
     i ← 2
     mientras n ≠ 1 hacer
        si i ∈ ℙ y i | n
           {lista factores n} ← i
           n ← n/i
        sino
           i ← i + 1
  devolver {lista factores n}
```

Con respecto a la notación:

- $i \in \mathbb{P}$ significa que *i* pertenece al conjunto de los números primos
- $i \mid n$ significa que *i* divide a *n*.