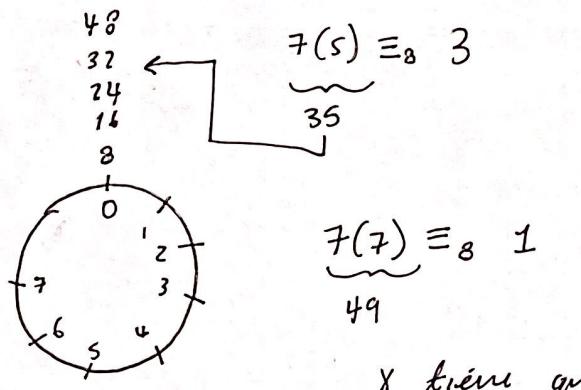


$$f_x = 1 \bmod(8)$$

$$f(1) \equiv_8 7$$



x tiene que ser 7

cap. 4 Rosen

neutro multiplicacion 1

neutro suma 0

32 · 41 Rosen

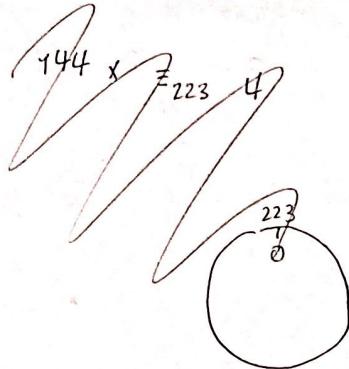
32) a)

$$(19^2 \bmod(41)) \bmod(9)$$

$$(19 \cdot 19 \bmod(41)) \bmod(9)$$

$$\underbrace{(361 \bmod(41))}_{\text{floor } \left(\frac{361}{41}\right) \approx 8} \bmod(9)$$

$$(361 - 8 \cdot 41) \bmod(9)$$

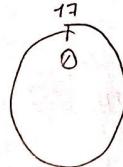


$$34 \times \equiv_{89} 77$$

$$77 \equiv_{89}$$

$$a = 2 \quad m = 17$$

$$a \cdot \bar{a}^1 \equiv_{17} 1$$



$$1 \equiv 18 \equiv 35$$

$$2 \cdot 9$$

$$\bar{a}^1 \equiv_{17} 9$$

$$a = 34 \quad m = 89$$

$$1 \equiv 90 \equiv$$

$$a = 4 \quad m = 9$$

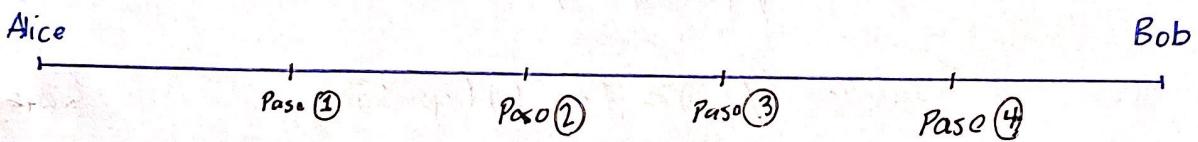
$$1 \equiv 10 \equiv 20 \quad 19 \equiv 28$$

$\swarrow 4 \cdot 5 \quad \nearrow 4 \cdot 7$

$$\bar{a}^1 \equiv 7$$

Sistema criptográfico RSA:

- Inventado en 1978
- Mas ampliamente utilizado
- Rivest, Shamir, Adleman



Paso 1: Generación de llaves

Paso 2: Distribución

Paso 3: Encriptación

Paso 4: Desencriptación

Generación de la llave:

- Elegimos dos números primos p & q .
Estos los elige Alice, solo ella lo sabe.
- Se mantienen en secreto. # Eligen numeros de 10^{24} bits.
- Calculamos: $n = p \cdot q$ (parte de la clave)
- Encontrar p & q a partir de n es computacionalmente inviolable.

- Calculamos $\phi(n) = (p-1)(q-1)$

totiente de Euler
[1]

- [1] devuelve el número de primos relativos con n menores que n .

$$\{1, 2, 3, 4\}$$

$$\phi(5) = 4$$

$$\phi(11) = 10$$

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$$

$$\therefore \phi(n) = (p-1)(q-1)$$

Elegimos un entero e :

$$1) e < \phi(n)$$

e & n es la llave pública.

$$2) \text{mcd}(e, \phi(n)) = 1$$

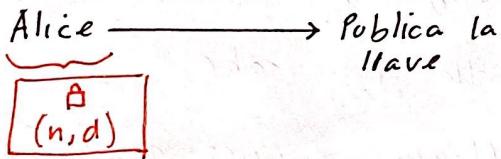
• La clave pública (n, e)

• Calculamos otro entero d :

$$e \cdot d \equiv 1 \pmod{\phi(n)}$$

! "d" es el inverso multiplicativo de $e \cdot \text{mod}(\phi(n))$.

• Clave privada (n, d) .



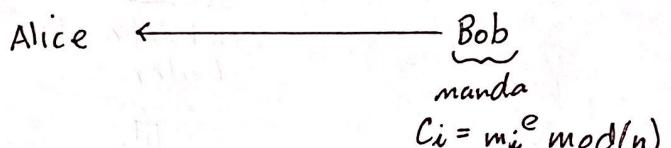
Encryptación:

$$\underbrace{M}_{\text{mensaje}} = m_1, m_2, m_3, m_4, \dots, m_K$$

Calcula (Bob):

$$C_i = (m_i)^e \pmod{n}$$

$$\underbrace{C = C_1, C_2, C_3, \dots, C_K}_{\text{Mensaje encriptado}}$$



Desencripta:

$$C = c_1 c_2 c_3 \dots c_k$$

Calculamos (Alice):

$$m_i = (c_i)^d \bmod(n)$$

$$M = m_1 m_2 m_3 \dots m_k$$

$$\# ed \equiv 1 \pmod{\phi(n)} \rightarrow ed \equiv 1 \pmod{n}$$

■ Dado un diccionario:

$$\Sigma = (0: \square, 1: A, 2: B \dots 27: Z)$$

- Si el mensaje M se descompone en monogramas (letra por letra) se escogen "p" y "q" de modo que $n = p \cdot q$ sea mayor que el monograma más grande en Σ .
- Si son bigramas $m_1 m_2$ (letras de dos en dos)

Z A N A H O R I A
 ↓
 →2701

El bigrama más grande será 2727.

Cifrado Vigenère

2019-10-30

Un sistema criptográfico polialfabético.

Def polialfabético: para cada letra se usa un alfabeto diferente.

Sistema criptográfico:

- Un diccionario: \sum
- Una clave: AGUACATE
- Un mensaje:

COMER FIAMBRE SIN JAMÓN
AGUACATE AGUA CAT EAGUA

- tabla recta:

	A	B	C	D	...	Z	mensaje
A							
B							
C							
:							
A							

Corto 2 Matemática Discreta

Miércoles, 4 de septiembre 2019

Nombre y Apellidos: David Gabriel Corzo Monasterio

Tema:	1	2	3	Total
Puntos:	40	45	15	100
Nota:	40	20	10	70

1. (40 pts.) ¿De cuántas maneras distintas pueden 5 corredores distintos terminar una carrera suponiendo que ninguno queda empatado?

* orden importa

$$\begin{array}{ccccc} X_1 & X_2 & X_3 & X_4 & X_5 \\ \hline 1 & 2 & 3 & 4 & 5 \end{array} \quad * \text{ si uno tiene el primer lugar es diferente por lo tanto me inclino por permutaciones}$$

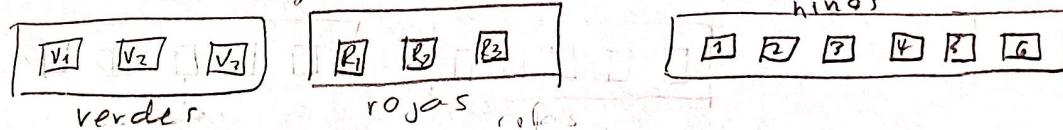
hay 5 lugares $\therefore 5^5 = 120$ ✓

5 jugadores

$$\frac{5!}{(5-5)!} = 5! = 120$$

2. (45 pts.) ¿De cuántas maneras distintas es posible distribuir 3 camisas idénticas verdes y 3 camisas idénticas rojas entre 6 niños tal que cada niño recibe únicamente una camisa?

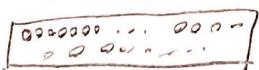
* relaciono a los regulares



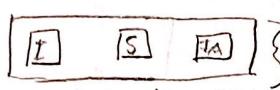
* lo cuenta como que si fueran distintos * importa el orden.
 $1V_1 + 2V_2 + 3V_3 + 4R_1 + 5R_2 + 6R_3$ pero cuenta toda primera
 $n=6 \quad r=6 \quad {}^n P_r = \frac{6!}{(6-6)!} = 720$ permutación

∴ de un conjunto de 6 camisas las puedo distribuir tal que cada uno solo tenga una 6 permutaciones

3. (15 pts.) Ingrid, Steven e Ian están jugando poker con una baraja de 52 cartas. Fabricio, el dealer, (quien no está jugando) reparte a cada jugador sus respectivas cartas; 5 a cada uno. ¿Cuántas jugadas posibles pueden existir en una ronda?



52 cartas



Jugadores

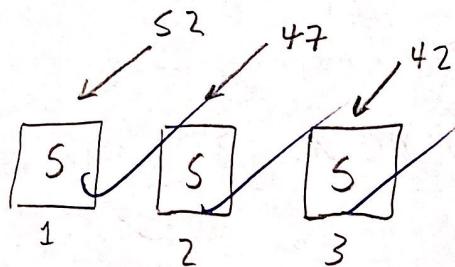
como una jugada son 5 cartas
15 en total se pretende usar 15 para cada jugada

* de un conjunto de 52 cartas cuántas veces puedo distribuir? El orden importa:



formas diferentes de distribuir 52 en 3 jugadores

en una jugada se deben distribuir 15 cartas para los tres jugadores, ¿Cuántas veces se pueden distribuir 52 cartas en conjuntos de 15? $52P_{15}$ veces, ese resultado ($\approx 5.810187598 \times 10^{24}$) dividido 3 es el número de



Por casos:

Primer jugador: ${}^{52}P_5 = 311875200$

Segundo jugador: ${}^{47}P_5 = 184072680$

Tercer jugador: ${}^{42}P_5 = 102080160$

{ combinaciones }

405947880

598028040.

CS041 Matemática Discreta Aplicada

Examen Parcial 2

Nombre: David Lora

Resumen:

Ejercicio:	1	2	3	4	5	6	7	8	Total
Puntos:	13	13	13	13	13	13	11	11	100
Resultado:									

Parte I: Resuelva los siguientes ejercicios de forma clara y ordenada, dejando constancia de todo su procedimiento.

1. (13 puntos) Encuentre el $\text{mcd}(2689, 1369)$.

2. (13 puntos) Manuel tiene dos contenedores. Un contenedor puede almacenar 23 ml y el otro 21 ml. Explique, ¿cómo puede usar Manuel estos contenedores para medir exactamente 1 ml? Justifique su respuesta usando un procedimiento no exhaustivo.

3. (13 puntos) Indique para qué valor (o valores) de k tiene solución la ecuación diofantina:

$$128x + 60y = k$$

4. (13 puntos) Si $a, b \in \mathbb{Z}^+$ con $a = 420$, $\text{mcd}(a, b) = 2$ y $\text{mcm}(a, b) = 5460$, determine el valor de b .

5. (13 puntos) Encuentre todas las soluciones de la ecuación diofantina:

$$121x + 74y = 208$$

6. (13 puntos) Usando el algoritmo de exponentiación modular, calcule:

$$9^{29} \in \mathbb{Z}_{13}$$

Parte II: Suponga que cada letra del alfabeto (y el espacio) se puede codificar con los dígitos según la siguiente tabla:

U = 00	D = 04	H = 08	L = 12	O = 16	S = 20	W = 24
A = 01	E = 05	I = 09	M = 13	P = 17	T = 21	X = 25
B = 02	F = 06	J = 10	N = 14	Q = 18	U = 22	Y = 26
C = 03	G = 07	K = 11	Ñ = 15	R = 19	V = 23	Z = 27

7. (11 puntos) Utilice el cifrado de César ponderado con clave $k = 5$ y $d = 11$ para encriptar el mensaje: ATACAR AL AMANECER.
8. (11 puntos) Se ha interceptado el siguiente mensaje UOWFGNFDNPNDKXNFOWPOWNWKN. Si se sabe que se ha utilizado el cifrado César ponderado con $k = 7$ y $d = 6$, descifre el mensaje.

$$a = 7 \mod(28) \quad \text{mcd}(28, 7)$$

$$a \cdot a^{-1} \equiv_2 1$$

$$7 \cdot a^{-1} \equiv_{28}$$

$$1 \equiv_{28} 29 \equiv_{28}$$

Parcial # 2

David Corzo 20140432

$$\textcircled{1} \quad \text{mcd}(2686, 1369)$$

$$2686 = 1369 \cdot \boxed{1} + 1317$$

$$\text{mcd}(1369, 1317)$$

$$1369 = 1317 \cdot \boxed{1} + 52$$

$$\text{mcd}(1317, 52)$$

$$1317 = 52 \cdot \boxed{25} + 17$$

$$\text{mcd}(52, 17)$$

$$52 = 17 \cdot \boxed{3} + 1$$

$$\text{mcd}(17, 1)$$

$$17 = 1 \cdot \boxed{17} + 0$$

$$\text{mcd}(1, 0)$$

$$\text{mcd}(2686, 1369) = 1 \quad \checkmark$$

$\textcircled{2}$ Contenedor₁ = 23 ml
 Contenedor₂ = 21
 # Primera saquemos el mcd de 23, 21

$$\text{mcd}(23, 21)$$

$$23 = 21 \cdot \boxed{1} + 2$$

$$\text{mcd}(21, 2)$$

$$21 = 2 \cdot \boxed{10} + 1$$

$$\text{mcd}(2, 1)$$

$$1 = 1 \cdot \boxed{1} + 0$$

$$\text{mcd}(1, 0)$$

$$23x + 21y = 1$$

$\textcircled{3}$ Encuentre valores de K.

$$128x + 60y = K$$

$$\text{mcd}(128, 60) \quad \text{Es correcto.}$$

La ecuación tiene $128 = 60 \cdot \boxed{2} + 8$ que 7 módulos
 solución si tal $\text{mcd}(60, 8)$ no puede tener
 K está representado inversa, pero a fuerza
 por múltiplos de 60 = $8 \cdot \boxed{7} + 4$ bruto es posible
~~4!~~ describirlo.

$$\text{mcd}(8, 4)$$

$$8 = 4 \cdot \boxed{2} + 0$$

$$\text{mcd}(4, 0)$$

$$\text{mcd}(128, 60) = 4$$

$\textcircled{4}$

$$a, b \in \mathbb{Z}^+ ; a = 420$$

$$\text{mcd}(a, b) = 2$$

$$\text{mcm}(a, b) = 5460$$

$$\text{mcd}(a, b) \text{ mcm}(a, b) = a \cdot b$$

$$\frac{(2)(5460)}{420} = b$$

$$\frac{2 \cdot 5460}{210} = b$$

$$\frac{5460}{210} = b$$

$$b = 26 \quad \checkmark$$

Ejercicio	1	2	3	4	5	6	7	8	Final
Puntos	13	13	13	13	13	13	11	5	94

⑥ Algoritmo de exponenteación modular:

$$9^{24} \in \mathbb{Z}_{13}$$

Escribir 29 en binario.

$$29_2 = \begin{array}{r} 1 & 1 & 1 & 0 & 1 \\ + & 3 & 2 & 1 & 0 \end{array}$$

$$29 = 2^4 + 2^3 + 2^2 + 2^0 \quad \checkmark$$

Bits	a^{2^n}	$a^2 \text{ mod}(n)$	
0 1	$9^{2^0} = 9 \equiv_{13} 9$	$9^2 = 81 \equiv_{13} 3$	
1 0	$9^{2^1} = 9^2 \equiv_{13} 3$	$3^2 \equiv_{13} 9$	
2 1	$9^{2^2} = 9^4 \equiv_{13} 9$	$9^2 \equiv_{13} 3$	
3 1	$9^{2^3} = 9^8 \equiv_{13} 3$	$3^2 \equiv_{13} 9$	
4 1	$9^{2^4} = 9^{16} \equiv_{13} 9$	$9^2 \equiv_{13} 3$	

$$\begin{aligned} \frac{29}{2} &= 14 + \frac{1}{2} \\ \frac{14}{2} &= 7 + \frac{0}{2} \\ \frac{7}{2} &= 3 + \frac{1}{2} \\ \frac{3}{2} &= 1 + \frac{1}{2} \\ \frac{1}{2} &= 0 + \frac{1}{2} \\ 11101 \end{aligned}$$

$$f_0(81 \div 13) = 6$$

$$13 \cdot 6 = 78$$

$$81 - 78 = 3$$

$$\begin{aligned} 9^{29} &= 9^4 \cdot 9^3 \cdot 9^2 \cdot 9^0 \\ &\equiv_{13} 9 \cdot 3 \cdot 9 \cdot 9 \\ &\equiv_{13} 9^2 \cdot 9 \cdot 3 \\ &\equiv_{13} 3 \cdot 9 \cdot 3 \equiv_{13} 3^2 \cdot 9 \\ &\equiv_{13} 9 \cdot 9 \equiv_{13} 9^2 \equiv_{13} \boxed{3} \end{aligned}$$

②

~~Res~~

$$\text{contenedor}_1 = 23$$

$$\text{contenedor}_2 = 21$$

$$\text{mcd}(23, 21)$$

$$23 = 21 \cdot \boxed{1} + 2$$

$$\text{mcd}(21, 2)$$

$$21 = 2 \cdot \boxed{10} + 1$$

$$\text{mcd}(2, 1)$$

$$2 = 1 \cdot \boxed{2} + 0$$

$$\text{mcd}(1, 0)$$

$$\# El \text{ mcd}(23, 21) = 1$$

$$23x + 21y = 1$$

Bézout reversible

$$21 - 2 \cdot 10 = 1$$

$$21 - (23 - 21) \cdot 10 = 1$$

$$21 - 10(23 - 21) = 1$$

$$21 - 10 \cdot 23 + 10 \cdot 21 = 1$$

$$-10 \cdot 23 + 11 \cdot 21 = 1$$

Manuel debe llenar 11 veces el de 21 ml & ~~después vaciar~~ 10 veces el de 23 ml.

La solución es $x = 7(47 - 47) - 4 \cdot 47 = 7$
en que $x \& y = 7 \cdot 47 - 7 \cdot 47 - 4 \cdot 47 = 1$

+ tienen que ser de la forma $7 \cdot 47 - 11 \cdot 47 = 1$

$$y = \frac{7 \cdot 47 - 11 \cdot 47}{11} + k$$

$$7 \cdot 74 - 11(121 - 74) = 1$$

$$7 \cdot 74 - 11 \cdot 121 + 11 \cdot 74 = 1$$

$$128 \cdot 74 - 11 \cdot 121 = 1$$

(5) \rightarrow supongo que es un 5...

$$121x + 74y = 208$$

$$\text{mcd}(121, 74)$$

$$121 = 74 \cdot \boxed{1} + 47$$

$$\text{mcd}(74, 47)$$

$$74 = 47 \cdot \boxed{1} + 27 \checkmark$$

$$\text{mcd}(47, 27)$$

$$47 = 27 \cdot \boxed{1} + 20 \checkmark$$

$$\text{mcd}(27, 20)$$

$$27 = 20 \cdot \boxed{1} + 7 \checkmark$$

$$\text{mcd}(20, 7)$$

$$20 = 7 \cdot \boxed{2} + 6 \checkmark$$

$$\text{mcd}(7, 6)$$

$$7 = 6 \cdot \boxed{1} + 1 \checkmark$$

$$\text{mcd}(6, 1)$$

$$6 = 1 \cdot \boxed{6} + 0$$

$$\text{mcd}(1, 0)$$

$$\text{mcd}(121, 74) = 1 \checkmark$$

$$7 - 6 = 1$$

$$7 - (20 - 7 \cdot 2) = 1$$

$$7 - 20 + 7 \cdot 2 = 1$$

$$3 \cdot 7 - 20 = 1$$

$$3(27 - 20) - 20 = 1$$

$$3 \cdot 27 - 3 \cdot 20 - 20 = 1$$

$$3 \cdot 27 - 4 \cdot 20 = 1$$

$$3 \cdot 27 - 4(47 - 27) = 1$$

$$3 \cdot 27 - 4 \cdot 47 + 4 \cdot 27 = 1$$

$$7 \cdot 27 - 4 \cdot 47 = 1$$

⑦ Cesar ponderado $k = 5$; $d = 11$
 "ATACAR AL AMANECER"

Original

$$E(x) = 5x + 11$$

$$\begin{aligned}
 A &= 1 \rightarrow 16 \equiv_{28} 16 \rightarrow 0 \\
 T &= 21 \rightarrow 116 \equiv 4 \rightarrow D \\
 A &= 1 \rightarrow 16 \equiv 16 \rightarrow 0 \\
 C &= 3 \rightarrow 26 \equiv 26 \rightarrow Y \\
 A &= 1 \rightarrow 16 \equiv 16 \rightarrow 0 \\
 R &= 19 \rightarrow 106 \equiv 22 \rightarrow U \\
 L &= 0 \rightarrow 11 \equiv 11 \rightarrow K \\
 A &= 1 \rightarrow 16 \equiv 16 \rightarrow 0 \\
 L &= 12 \rightarrow 71 \equiv 15 \rightarrow N \\
 L &= 0 \rightarrow 11 \equiv 11 \rightarrow K \\
 A &= 1 \rightarrow 16 \equiv 16 \rightarrow 0 \\
 M &= 13 \rightarrow 76 \equiv 20 \rightarrow S \\
 A &= 1 \rightarrow 16 \equiv 16 \rightarrow 0 \\
 N &= 14 \rightarrow 81 \equiv 25 \rightarrow X \\
 E &= 5 \rightarrow 36 \equiv 8 \rightarrow H \\
 C &= 3 \rightarrow 26 \equiv 26 \rightarrow Y \\
 E &= 5 \rightarrow 36 \equiv 8 \rightarrow H \\
 R &= 19 \rightarrow 106 \equiv 22 \rightarrow U
 \end{aligned}$$

$$U = 12$$

$$D = 16$$

$$W = 24$$

$$F = 6$$

$$G = 7$$

$$N = 14$$

$$P = 6$$

$$D = 4$$

$$N = 14$$

$$P =$$

$$N =$$

$$D =$$

$$K =$$

$$X =$$

$$N =$$

$$F =$$

$$D =$$

$$W =$$

$$P =$$

$$D =$$

$$W =$$

$$N =$$

$$W =$$

$$K =$$

$$N =$$

$$D(x) = (x - 6) \cdot 7^{-1}$$

Dado que 7 módulo 28 no tiene inversa
 \therefore no se puede desencriptar.

$$7 \in \mathbb{Z}_{28}$$

$$28 = 7 \cdot \boxed{4} + 0$$

$$\text{mcd}(7, 0)$$

No hay inversos

Trabajo en Clase

David Gabriel Corzo McMurt 20190432

2019-09-25

① $\text{mcd}(231, 1820)$

$$= \text{mcd}(1820, 231)$$

$$1820 = 7 \cdot 231 + 203$$

$$\text{mcd}(231, 203)$$

$$231 = 1 \cdot 203 + 28$$

$$\text{mcd}(203, 28) \checkmark$$

$$203 = 7 \cdot 28 + 7$$

$$\text{mcd}(28, 7)$$

$$28 = 4 \cdot 7 + 0$$

$$\text{mcd}(7, 0)$$

$$\text{mcd}(2597, 1369) \checkmark$$

$$2597 = 1 \cdot 1369 + 1228$$

$$\text{mcd}(1369, 1228)$$

$$1369 = 1 \cdot 1228 + 141$$

$$\text{mcd}(1228, 141)$$

$$1228 = 8 \cdot 141 + 100$$

$$\text{mcd}(141, 100)$$

$$141 = 1 \cdot 100 + 41$$

$$\text{mcd}(100, 41)$$

$$100 = 2 \cdot 41 + 18$$

$$\text{mcd}(41, 18)$$

$$41 = 2 \cdot 18 + 5$$

$$\text{mcd}(18, 5)$$

$$18 = 3 \cdot 5 + 3 \checkmark$$

$$\text{mcm}(5, 3)$$

$$5 = 1 \cdot 3 + 2$$

$$\text{mcd}(3, 2)$$

$$3 = 1 \cdot 2 + 1$$

$$\text{mcd}(2, 1)$$

$$2 = 1 \cdot 1 + 1$$

$$\text{mcd}(1, 1)$$

$$1 = 1 \cdot 1 + 0$$

$$\text{mcd}(1, 0)$$

$$c) \text{ mcd}(4001, 2689)$$

$$4001 = 1 \cdot 2689 + 1312$$

$$\text{mcd}(2689, 1312)$$

$$2689 = 2 \cdot 1312 + 65$$

$$\text{mcd}(1312, 65)$$

$$1312 = 20 \cdot 65 + 12$$

$$\text{mcd}(65, 12)$$

$$65 = 5 \cdot 12 + 5$$

$$\text{mcd}(12, 5)$$

$$12 = 2 \cdot 5 + 2$$

$$\text{mcd}(5, 2)$$

$$5 = 2 \cdot 2 + 1$$

$$\text{mcd}(2, 1)$$

$$2 = 1 \cdot 1 + 1$$

$$\text{mcd}(1, 1)$$

$$1 = 1 \cdot 1 + 0$$

$$\text{mcd}(1, 0)$$

$$\textcircled{2} \quad a) \text{mcd}(250, 111)$$

$$250 = 2 \cdot 111 + 28 \quad \textcircled{3}$$

$$\text{mcd}(111, 28)$$

$$111 = 3 \cdot 28 + 27 \quad \textcircled{2}$$

$$\text{mcd}(28, 27)$$

$$28 = 27 \cdot 1 + 1 \quad \textcircled{1}$$

$$\text{mcd}(27, 1)$$

$$\cancel{27 = 27 \cdot 1 + 0} \quad \square$$

$$b) 250x - 111y = 1$$

$$\cancel{28 - 27 \cdot 7 = 1}$$

$$\cancel{111 - 3 \cdot 28 = 27}$$

$$\cancel{250 - 2 \cdot 111 = 28}$$

$$28 = (111 - 3 \cdot 28) = 1 \quad \textcircled{3}$$

$$28 - 111 + 3 \cdot 28 = 1$$

$$4 \cdot 28 - 111 = 1$$

$$4(250 - 2 \cdot 111) - 111 = 1$$

$$4 \cdot 250 - 8 \cdot 111 - 111 = 1$$

$$4 \cdot 250 - 9 \cdot 111 = 1$$

$$x = 4$$

$$y = -9$$

Multizieren de $4, -9$. \square

$$1 \cdot 111 - (-9) \cdot 280 = 1$$

$$y = 1 \quad x = -2$$

$$c) \quad 250x + 111y = 19$$

Tomando en cuenta que $x = 4$ & $y = -9$ es una solución multiplicamos los mismos por 19.

$$\begin{array}{r} 3 \\ 19 \\ \times 4 \\ \hline 76 \end{array} \quad \begin{array}{r} 8 \\ 19 \\ \times 9 \\ \hline -171 \end{array}$$

\therefore todos los múltiplos de $x = 76$ & $y = -171$

comprobación:

$$250(76) + 111(-171) = 19$$

$$19,000 - 18,981 = 19$$

$$19 = 19 \quad \checkmark$$

③ Encontrar "c" para la ecuación diofantina:

$$12x + 16y = c$$

encontramos $\text{mcd}(12, 16)$

$$16 = 12 \cdot 1 + 4$$

$$\text{mcd}(12, 4)$$

$$12 = 3 \cdot 4 + 0$$

$$\text{mcd}(4, 0)$$

es $\frac{4}{\cancel{x}}$

\therefore la ecuación diofantina presentada anteriormente tiene una solución " c " tal que " c " será múltiplo de $\frac{14}{\cancel{x}}$.

$$\textcircled{4} \quad \text{mcd}(180, 162, 126)$$

$$\underbrace{\text{mcd}(180, \underbrace{\text{mcd}(162, 126)}_1)}_2$$

$$\textcircled{1} \quad \text{mcd}(162, 126)$$

$$162 = 1 \cdot 126 + 36$$

$$\text{mcd}(126, 36)$$

$$126 = 3 \cdot 36 + 18$$

$$\text{mcd}(36, 18)$$

$$36 = 2 \cdot 18 + 0$$

$$\text{mcd}(18, 0) \quad \cancel{x}$$

$$\textcircled{2} \quad \text{mcd}(180, 18)$$

$$180 = 10 \cdot 18 + 0$$

$$\text{mcd}(18, 0) \quad \cancel{x}$$

El mcd es 18

\textcircled{5} Si $a, b \in \mathbb{Z}^+$ con $a = 630$, $\text{mcd}(a, b) = 105$ & $\text{lcm}(a, b) = 242,550$, determine el valor de b .

$$\underbrace{\text{mcd}(a, b)}_{105} \cdot \underbrace{\text{lcm}(a, b)}_{242,550} = a \cdot b$$

$$105 \cdot 242,550 = 630 \cdot b$$

$$\frac{105 \cdot 242,550}{630} = b$$

$$b = \underbrace{40425}_{\cancel{x}}$$

$$\text{mcd}(630, 40425)$$

$$40425 = 64 \cdot 630 + 105$$

$$\text{mcd}(630, 105)$$

$$630 = 105 \cdot 6 + 0$$

$$\text{mcd}(105, 0) \quad \cancel{x} \quad \checkmark$$

⑥ Ganó Giarg \$1020 en 20, 50, si 50x > 20y
cuantas fichas de 20 & 50 puede tener?

$$1020 = 20 \cdot 50 + 20 \cdot 1$$

Podría tener 20 fichas de 50 &
1 de 20.

$$50x + 20y = 1020$$

$$\text{mcd}(50, 20)$$

$$50 = 20 \cdot 2 + 10$$

$$\text{mcd}(20, 10)$$

$$20 = 10 \cdot 2 + 0$$

$$x > y$$

$$102 + 2k > -204 - 5k$$

$$7k > -204 - 102$$

$$k > \frac{-306}{7} \approx -43 \quad \therefore t = -42$$

$$50x + 20y = 10 \quad \text{mcd}(50, 20) = 10$$

$$x=1$$

$$y=2$$

pero $x > y$ entonces
hay que encontrar

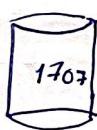
$$x = x_0 + \frac{b}{\text{mcd}(a,b)} \cdot k$$

$$y = y_0 - \frac{a}{\text{mcd}(a,b)} \cdot k$$

$$x = 102 + \frac{20}{10} k$$

$$y = -204 - \frac{50}{10} k$$

⑦



$$17x + 55y = 1$$

$$\text{mcd}(55, 17)$$

$$55 = 3 \cdot 17 + 4$$

$$\text{mcd}(17, 4)$$

$$17 = 4 \cdot 4 + 1$$

$$\text{mcd}(4, 1)$$

La respuesta es que
puede usarla de infinitas
maneras.

$$17 - 4 \cdot 4 = 1$$

$$17 - 4(55 - 3 \cdot 17) = 1$$

$$17 - 4 \cdot 55 + 12 \cdot 17 = 1$$

$$\underbrace{13 \cdot 17}_a - \underbrace{4 \cdot 55}_b = 1$$

$$x = 13 \quad y = -4$$

múltiplos de $x = 13$ & $y = -4$.

13 serridas del de 17 &
4 vaciadas del de 55,
quedará 1 onza en el
de 17.

Trabajo de repaso David Corzo

20190432

Se llaman divisores de cero a $a \neq 0 \neq b$, tales que $a \cdot b \equiv_n 0$. Encuentre los divisores de cero $\mathbb{Z}_6, \mathbb{Z}_7, \mathbb{Z}_8$ & \mathbb{Z}_{15} .

■ \mathbb{Z}_6 : residuos $\mod(6) = \{0, 1, 2, 3, 4, 5\}$

$$6 = 2 \cdot 3$$

descomposición prima de 6.

R// Todos los números múltiplos de dos & de tres menores que 6. $\{2, 4, 3\}$ son divisores de cero

■ \mathbb{Z}_7 :

R// todos los números son invertibles en este módulo, no hay divisores de cero.

■ \mathbb{Z}_8 :

$$8 = 2^3$$

R// todos los números múltiplos de dos menores a 8.

■ \mathbb{Z}_{15} :

$$15 = 3 \cdot 5$$

R// todos los números múltiplos de 3 & de 5 menores a 15.

2) Encuentre los inversos de:

a) $6 \in \mathbb{Z}_{17}$

$$a = 6 \quad n = 17$$

$$a \cdot a^{-1} \equiv_{17} 1$$

$$1 \equiv_{17} 18$$

$$\begin{array}{c} \wedge \\ 6 \cdot 3 \end{array}$$

$$6 \cdot 3 \equiv_{17} 1$$

$$\boxed{a^{-1} \equiv_{17} 3}$$

b) $3 \in \mathbb{Z}_{10}$

$$a = 3 \quad n = 10$$

$$a \cdot a^{-1} \equiv_{10} 1$$

$$1 \equiv_{10} 11 \equiv 21$$

$$\begin{array}{c} \wedge \\ 3 \cdot 7 \end{array}$$

$$3 \cdot 7 \equiv 1$$

$$\boxed{a^{-1} = 7}$$

c) $5 \in \mathbb{Z}_{12}$

$$a = 5 \quad n = 12$$

$$5 \cdot a^{-1} \equiv_{12} 1$$

$$1 \equiv_{12} 13 \equiv_{12} 25$$

$$\begin{array}{c} \wedge \\ 5 \cdot 5 \end{array}$$

$$5 \cdot 5 \equiv_{12} 1$$

$$\boxed{a^{-1} = 5}$$

$$1 \equiv_{16} 17 \equiv_{16} 33 \equiv_{16} 49$$

$$\begin{array}{c} \wedge \\ 7 \cdot 7 \end{array}$$

$$\boxed{a^{-1} = 7}$$

$$1002 = 125 \cdot 8 + 2 \quad 5 = 12 \cdot 3 + 2$$

$$\text{mod}(5, 2)$$

$$47 = 12 \cdot 4 + 1 \quad 2 = 12 \cdot 1 + 1$$

$$\text{mod}(2, 1)$$

$$8 = 12 \cdot 0 + 8 \quad 1 = 12 \cdot 0 + 1$$

$$\text{mod}(1, 1) = 1$$

$$e) 777 \in \mathbb{Z}_{1009}$$

$$\text{mcd}(1009, 777)$$

$$1009 = 777 \cdot \boxed{1} + 232 \quad \textcircled{7}$$

$$\text{mcd}(777, 232)$$

$$777 = 232 \cdot \boxed{3} + 81 \quad \textcircled{6}$$

$$\text{mcd}(232, 81)$$

$$232 = 81 \cdot \boxed{2} + 70 \quad \textcircled{5}$$

$$\text{mcd}(81, 70)$$

$$81 = 70 \cdot \boxed{1} + 11 \quad \textcircled{4}$$

$$\text{mcd}(70, 11)$$

$$70 = 11 \cdot \boxed{6} + 4 \quad \textcircled{3}$$

$$\text{mcd}(11, 4)$$

$$11 = 4 \cdot \boxed{2} + 3 \quad \textcircled{2}$$

$$\text{mcd}(4, 3)$$

$$4 = 3 \cdot \boxed{1} + 1 \quad \textcircled{1}$$

$$\text{mcd}(3, 1)$$

$$3 = 1 \cdot \boxed{0} + 0 \quad \textcircled{0}$$

$$\text{mcd}(1, 0) = 1$$

filtrar el módulo

$$\frac{211 \cdot 1009 - 274 \cdot 777 = 1}{211 \cdot 0 + 735 \cdot 777} \quad \mathbb{Z}_{1009}$$

El inverso es: 735

master

$$4 - 3 \cdot 1 = 1$$

master, \textcircled{2}

$$4 - (11 - 4 \cdot 2) = 1$$

$$4 - 11 + 4 \cdot 2$$

$$3 \cdot 4 - 11 = 1$$

master \textcircled{3}

$$3(70 - 11 \cdot 6) - 11 = 1$$

$$3 \cdot 70 - 18 \cdot 11 - 11 = 1$$

$$3 \cdot 70 - 19 \cdot 11 = 1$$

master \textcircled{4}

$$3 \cdot 70 - 19(81 - 70) = 1$$

$$3 \cdot 70 - 19 \cdot 81 + 19 \cdot 70 = 1$$

$$-22 \cdot 70 - 19 \cdot 81 = 1$$

master \textcircled{5}

$$22(232 - 81 \cdot 2) - 19 \cdot 81 = 1$$

$$22 \cdot 232 - 44 \cdot 81 - 19 \cdot 81 = 1$$

$$22 \cdot 232 - 63 \cdot 81 = 1$$

master \textcircled{6}

$$22 \cdot 232 - 63(777 - 232 \cdot 3) = 1$$

$$22 \cdot 232 - 63 \cdot 777 + 189 \cdot 232 = 1$$

$$211 \cdot 232 - 63 \cdot 777 = 1$$

master \textcircled{7}

$$211(1009 - 777) - 63 \cdot 777 = 1$$

$$211 \cdot 1009 - 211 \cdot 777 - 63 \cdot 777 = 1$$

$$\boxed{211 \cdot 1009 - 274 \cdot 777 = 1}$$

$$3) \text{ a). } 3^{15} \in \mathbb{Z}_{17}$$

Sacar 15 en binario

$$\begin{aligned} 15_2 &= 1111 \\ &= 2^3 + 2^2 + 2^1 + 2^0 \\ &= 3^2 \cdot 3^2 \cdot 3^1 \cdot 3^0 \end{aligned}$$

$$\begin{aligned} \frac{15}{2} &= 7 + \frac{1}{2} \\ \frac{7}{2} &= 3 + \frac{1}{2} \\ \frac{3}{2} &= 1 + \frac{1}{2} \\ \frac{1}{2} &= 0 + \frac{1}{2} \end{aligned} \quad \left. \begin{array}{c} 1111 \\ \hline \end{array} \right\}$$

Bits	a	$a^2 \bmod(n)$
1	$3^0 = 1$	$1 \equiv_{17} 1$
1	$3^1 = 9$	$9^2 = 81 \equiv_{17} 13$
1	$3^2 = 13$	$13^2 = 169 \equiv_{17} 16$
1	$3^3 = 27$	$27^2 = 729 \equiv_{17} 1$

$$3^{15} = \frac{3^2 \cdot 3^2 \cdot 3^1 \cdot 3^0}{\underbrace{13}_{\equiv_{17} 1} \cdot \underbrace{9}_{\equiv_{17} 3}} \in \mathbb{Z}_{17}$$

$$\textcircled{1} \quad 208 = 16 \cdot 13$$

$$12 \cdot 17 = 204$$

$$208 \equiv_{17} 4$$

$$\textcircled{2} \quad 27 = 9 \cdot 3$$

$$27 \equiv_{17} 10$$

$$\equiv_{17} \underbrace{4 \cdot 10}_{40} \equiv_{17} \boxed{6}$$

$$40 = 4 \cdot 10$$

$$2 \cdot 17 = 34$$

$$40 - 34 = 6$$

$$b) 125^{4577} \in \mathbb{Z}_{13}$$

$$4577_2 = \underbrace{1}_{12} \underbrace{0}_{11} \underbrace{0}_{10} \underbrace{1}_{9} \underbrace{1}_{8} \underbrace{1}_{7} \underbrace{1}_{6} \underbrace{1}_{5} \underbrace{0}_{4} \underbrace{0}_{3} \underbrace{0}_{2} \underbrace{1}_{10}$$

$$\frac{4577}{2} = 2288 + \frac{1}{2}$$

$$\sqrt{\frac{1}{125} 4577} = \underbrace{2^{12}}_{125} + \underbrace{2^8}_{725} + \underbrace{2^7}_{125} + \underbrace{2^6}_{125} + \underbrace{2^5}_{125} + \underbrace{2^0}_{125}$$

$$\frac{2288}{2} = 1144 + \frac{0}{2}$$

$$\frac{1144}{2} = 572 + \frac{0}{2}$$

$$\frac{572}{2} = 286 + \frac{0}{2}$$

$$\frac{286}{2} = 143 + \frac{0}{2}$$

$$\frac{143}{2} = 71 + \frac{1}{2}$$

$$\frac{71}{2} = 35 + \frac{1}{2}$$

$$\frac{35}{2} = 17 + \frac{1}{2}$$

$$\frac{17}{2} = 8 + \frac{1}{2}$$

$$\frac{8}{2} = 4 + \frac{0}{2}$$

$$\frac{2}{2} = 1 + \frac{0}{2}$$

$$MSB \quad \frac{1}{2} = 0 + \frac{1}{2}$$

1000 1111 0000 1

Bits	α^{2^n}	$\alpha^2 \text{ mod}(n)$
0 * 1	$125^{2^0} = 125 \equiv_{13} 8$	$8^2 = 64 \equiv_{13} 12$
1 0	$125^{2^1} = 125^2 \equiv_{13} 12$	$12^2 \equiv_B 1$
2 0	$125^{2^2} = 125^4 \equiv_{13} 1$	$1^2 \equiv_{13} 1$
3 0	$125^{2^3} = 125^8 \equiv_{13} 1$	$1^2 \equiv_{13} 1$
4 0	$125^{2^4} = 125^{16} \equiv 1$	$1^2 \equiv_{13} 1$
5 * 1	$125^{2^5} = 125^{32} \equiv 1$	$1^2 \equiv_{13} 1$
6 * 1	$125^{2^6} = 125^{64} \equiv 1$	$1^2 \equiv_{13} 1$
7 * 1	$125^{2^7} = 125^{128} \equiv 1$	$1^2 \equiv_{13} 1$
8 * 1	$125^{2^8} = 125^{256} \equiv 1$	$1^2 \equiv_{13} 1$
9 0	$125^{2^9} = 125^{512} \equiv 1$	$1^2 \equiv_{13} 1$
10 0	$125^{2^{10}} = 125^{1024} \equiv 1$	$1^2 \equiv_{13} 1$
11 0	$125^{2^{11}} = 125^{2048} \equiv 1$	$1^2 \equiv_{13} 1$
12 * 1	$125^{2^{12}} = 125^{4096} \equiv 1$	$1^2 \equiv_{13} 1$

$$125^{4577} = \underbrace{125^{2^{12}}}_{=1} \cdot \underbrace{125^{2^8}}_{=1} \cdot \underbrace{125^2}_{=1} \cdot \underbrace{125^6}_{=1} \cdot \underbrace{125^4}_{=1} \cdot \underbrace{125^0}_{=1} = 2 + \frac{0}{2}$$

$$= \boxed{8}$$

$$c) 11^{954} \in \mathbb{Z}_{20}$$

$$954 = \begin{array}{cccc} 1 & 1 & 1 & 0 \\ 9 & 8 & 7 & 6 \\ \hline 1 & 1 & 1 & 0 \end{array}$$

$$11^{954} = 11^9 \cdot 11^8 \cdot 11^7 \cdot 11^4 \cdot 11^3 \cdot 11^2$$

Bits	a	$a^2 \bmod(n)$
0 0	$11^2 = 11 \equiv_{20} 11$	$11^2 \equiv_{20} 1$
1 0	$11^2 = 11^2 \equiv_{20} 1$	$1^2 \equiv_{20} 1$
2 1	$11^2 = 11^4 \equiv_{20} 1$	$1^2 \equiv_{20} 1$
3 1	$11^2 = 11^8 \equiv_{20} 1$	$1^2 \equiv_{20} 1$
4 1	$11^2 = 11^{16} \equiv_{20} 1$	$1^2 \equiv_{20} 1$
5 0	$11^2 = 11^{32} \equiv_{20} 1$	$1^2 \equiv_{20} 1$
6 0	$11^2 = 11^{64} \equiv_{20} 1$	$1^2 \equiv_{20} 1$
7 1	$11^2 = 11^{128} \equiv_{20} 1$	$1^2 \equiv_{20} 1$
8 1	$11^2 = 11^{256} \equiv_{20} 1$	$1^2 \equiv_{20} 1$
9 1	$11^2 = 11^{512} \equiv_{20} 1$	$1^2 \equiv_{20} 1$

$$11^{954} = \underbrace{11^2}_1 \cdot \underbrace{11^2}_1 \cdot \underbrace{11^2}_1 \cdot \underbrace{11^2}_1 \cdot \underbrace{11^2}_1 \cdot \underbrace{11^2}_1 \rightarrow \mathbb{Z}_{20}$$

$$\equiv_{20} 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1$$

$$\equiv_{20} \boxed{1}$$

$$LSB \quad \frac{424}{2} = 462 + \frac{0}{2}$$

$$\frac{462}{2} = 231 + \frac{0}{2}$$

$$\frac{231}{2} = 115 + \frac{1}{2}$$

$$\frac{115}{2} = 57 + \frac{1}{2}$$

$$\frac{57}{2} = 28 + \frac{1}{2}$$

$$\frac{28}{2} = 14 + \frac{0}{2}$$

$$\frac{14}{2} = 7 + \frac{0}{2}$$

$$\frac{7}{2} = 3 + \frac{1}{2}$$

$$\frac{3}{2} = 1 + \frac{1}{2}$$

$$\frac{1}{2} = 0 + \frac{1}{2}$$

1110011100 100

$$d) 2^{340} \in \mathbb{Z}_{31}$$

$$LSB \quad \frac{340}{2} = 170 + \frac{0}{2}$$

$$\frac{170}{2} = 85 + \frac{0}{2}$$

$$\frac{85}{2} = 42 + \frac{1}{2}$$

$$\frac{42}{2} = 21 + \frac{0}{2}$$

$$\frac{21}{2} = 10 + \frac{1}{2}$$

$$\frac{10}{2} = 5 + \frac{0}{2}$$

$$\frac{5}{2} = 2 + \frac{1}{2}$$

$$\frac{1}{2} = 1 + \frac{0}{2}$$

$$MSB \quad \underbrace{\frac{1}{2}}_{101010100} = 0 + \frac{1}{2}$$

$$16^2 = 256$$

$$8^2 = 64$$

$$\text{floor}(256 \div 31) = 8$$

$$\text{floor}(64 \div 31) = 2$$

$$31 * 8 = 248$$

$$31 * 2 = 62$$

$$256 - 248 = 8$$

$$64 - 62 = 2$$

$$2^{340} = 2^{2^8} \cdot 2^{2^6} \cdot 2^{2^4} \cdot 2^{2^2} \mod 31$$

$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow$

$$\equiv_{31} 2 \cdot 16 \cdot 2 \cdot 16$$

$$\equiv_{31} 16^2 \cdot 2^2$$

$$\equiv_{31} 8 \cdot 4$$

$$\equiv_{31} 32 \equiv_{31} \boxed{1}$$

4) a. Cifrado caesar con clave $d = 7$ para cifrar y descifrar el mensaje "VAMOS A CENAR EN CASA"

Original	$E(x) = x + 7$	$D(x) = x - 7$	
$V = 23$	$\rightarrow 23 + 7 \bmod(26) \equiv 2$	$\rightarrow B$	$\rightarrow 2 - 7 \rightarrow 23 = V$
$A = 01$	$\rightarrow \equiv 8$	$\rightarrow H$	$\rightarrow 8 - 7 \rightarrow 1 = A$
$M = 13$	$\rightarrow \equiv 20$	$\rightarrow S$	$\rightarrow 20 - 7 \rightarrow 13 = M$
$O = 16$	$\rightarrow \equiv 23$	$\rightarrow V$	$\rightarrow 23 - 7 \rightarrow 16 = O$
$S = 20$	$\rightarrow \equiv 27$	$\rightarrow Z$	$\rightarrow 27 - 7 \rightarrow 20 = S$
$L = 00$	$\rightarrow \equiv 7$	$\rightarrow G$	$\rightarrow 7 - 7 \rightarrow 0 = L$
$A = 01$	$\rightarrow \equiv 8$	$\rightarrow H$	$\rightarrow 8 - 7 \rightarrow 1 = A$
$L = 00$	$\rightarrow \equiv 7$	$\rightarrow G$	$\rightarrow 7 - 7 \rightarrow 0 = L$
$C = 03$	$\rightarrow \equiv 10$	$\rightarrow T$	$\rightarrow 10 - 7 \rightarrow 3 = C$
$E = 05$	$\rightarrow \equiv 12$	$\rightarrow L$	$\rightarrow 12 - 7 \rightarrow 5 = E$
$N = 14$	$\rightarrow \equiv 21$	$\rightarrow T$	$\rightarrow 21 - 7 \rightarrow 14 = N$
$A = 01$	$\rightarrow \equiv 8$	$\rightarrow H$	$\rightarrow 8 - 7 \rightarrow 1 = A$
$R = 19$	$\rightarrow \equiv 26$	$\rightarrow Y$	$\rightarrow 26 - 7 \rightarrow 19 = R$
$L = 00$	$\rightarrow \equiv 7$	$\rightarrow G$	$\rightarrow 7 - 7 \rightarrow 0 = L$
$E = 05$	$\rightarrow \equiv 12$	$\rightarrow L$	$\rightarrow 12 - 7 \rightarrow 5 = E$
$N = 14$	$\rightarrow \equiv 21$	$\rightarrow T$	$\rightarrow 21 - 7 \rightarrow 14 = N$
$L = 00$	$\rightarrow \equiv 7$	$\rightarrow G$	$\rightarrow 7 - 7 \rightarrow 0 = L$
$C = 03$	$\rightarrow \equiv 10$	$\rightarrow T$	$\rightarrow 10 - 7 \rightarrow 3 = C$
$A = 01$	$\rightarrow \equiv 8$	$\rightarrow H$	$\rightarrow 8 - 7 \rightarrow 1 = A$
$S = 20$	$\rightarrow \equiv 27$	$\rightarrow Z$	$\rightarrow 27 - 7 \rightarrow 20 = S$
$A = 01$	$\rightarrow \equiv 8$	$\rightarrow H$	$\rightarrow 8 - 7 \rightarrow 1 = A$

b) Se ha interceptado "WSHC₁C₂GSLSD" $k=3$; $d=0$

ORIGINAL	$D(x)$
$W = 24$	$24 \cdot 19 - 0 = 8 \rightarrow H$
$S = 20$	$20 \cdot 19 - 0 = 16 \rightarrow O$
$H = 8$	$8 \cdot 19 - 0 = 12 \rightarrow L$
$C = 3$	$3 \cdot 19 - 0 = 1 \rightarrow A$
$L = 0$	$0 \cdot 19 - 0 = 0 \rightarrow L$
$C = 3$	$3 \cdot 19 - 0 = 1 \rightarrow A$
$L = 0$	$0 \cdot 19 - 0 = 0 \rightarrow L$
$G = 7$	$7 \cdot 19 - 0 = 21 \rightarrow T$
$S = 20$	$20 \cdot 19 + 0 = 16 \rightarrow O$
$L = 12$	$12 \cdot 19 + 0 = 4 \rightarrow D$
$S = 20$	$20 \cdot 19 - 0 = 16 \rightarrow O$
$D = 4$	$4 \cdot 19 - 0 = 20 \rightarrow S$

$$E(x) = 3x + 0$$

inversa de 3 mod 28

$$24 \cdot 19 = 456 \equiv_{28} 8$$

$$\text{floor}(456 \div 28) = 16$$

$$a \cdot a^{-1} \equiv_{28} 1$$

$$a = 3 \quad n = 28$$

$$\text{mcd}(28, 3)$$

$$28 = 3 \cdot 9 + 1$$

$$\text{mcd}(3, 1)$$

$$3 = 1 \cdot 3 + 0$$

$$\text{mcd}(1, 0)$$

At 8 zero out

$$28 - 3 \cdot 9 = 1$$

$$\begin{array}{r} 28 - 9 \cdot 3 \equiv_{28} 1 \\ \hline 0 + 19 \cdot 3 \equiv_{28} 1 \end{array}$$

$$a^{-1} = 19$$

c) Se ha interceptado "CKI₁TAJOEDB"; $K=3$; $d=1$

Original	$D(x)$
$C = 03$	$(3-1) \cdot 19 \equiv 10 \rightarrow J$
$K = 11$	$(11-1) \cdot 19 \equiv 22 \rightarrow U$
$I = 09$	$(9-1) \cdot 19 \equiv 17 \rightarrow L$
$U = 00$	$(0-1) \cdot 19 \equiv 9 \rightarrow I$
$T = 21$	$(21-1) \cdot 19 \equiv 16 \rightarrow O$
$A = 1$	$(1-1) \cdot 19 \equiv 0 \rightarrow U$
$J = 10$	$(10-1) \cdot 19 \equiv 3 \rightarrow C$
$O = 16$	$(16-1) \cdot 19 \equiv 5 \rightarrow E$
$E = 05$	$(5-1) \cdot 19 \equiv 20 \rightarrow S$
$D = 04$	$(4-1) \cdot 19 \equiv 1 \rightarrow A$
$B = 02$	$(2-1) \cdot 19 \equiv 19 \rightarrow R$

Tomando en cuenta la función de encriptado:

$$E(x) = 3 \cdot x + 1$$

La inversa de $3 \pmod{28} = 19$

$$D(x) = (x - 1) \cdot 19$$