Tarea 1 - Criptografía

Emmanuel Peto Gutiérrez Lisandro Vázquez Aguilar

November 2020

1.

a) Sea $\mathbb{Z}_n$ y $a, b \in \mathbb{Z}_n$. Mostrar que $(-a)b = -ab \mod n$.

Solución:

Se tiene que:

$0 = ab - ab = (-1)ab - (-1)ab = (-a)b - (-ab)$

Luego, como $n|0$, entonces $n|(-a)b - (-ab)$

Por lo tanto $(-a)b \cong -ab \mod n$. ■

b) Si $a \in \mathbb{Z}_n^*$ y $ax \cong b \mod n$ implica que $x \cong ba^{-1} \mod n$.

Solución:

Por hipótesis se sabe que $n|ax - b$, entonces n divide a cualquier múltiplo de $(ax - b)$, en particular, $n|a^{-1}(ax - b) = a^{-1}ax - ba^{-1}$. Así, $a^{-1}ax \cong ba^{-1} \mod n$.

Por definición $a^{-1}a \cong 1 \mod n$

$\Rightarrow n|a^{-1}a - 1$

$\Rightarrow n|a^{-1}ax - x$

$\Rightarrow a^{-1}ax \cong x \mod n$

Se tiene que $a^{-1}ax \cong x \mod n$ y $a^{-1}ax \cong ba^{-1} \mod n$, y como la congruencia módulo n es una relación de equivalencia, entonces $x \cong ba^{-1} \mod n$. ■

c) Si $a \cong b \mod n$ entonces $a^n \cong b^n \mod n$.

Solución:

Se demostrará por inducción que $a^n \cong b^n \mod m$ para cualquier m, así que en particular se cumplirá cuando $m = n$.

• Caso base $(n = 0)$.

Se tiene que $m|0 = 1 - 1 = a^0 - b^0$. Por lo que $a^0 \cong b^0 \mod m$.

• H.I. Supóngase que $a^n \cong b^n \mod m$ para alguna $n \in \mathbb{N}$. Se demostrará que $a^{n+1} \cong b^{n+1} \mod m$.

Por hipótesis se tiene que $m|a - b$ y $m|a^n - b^n$, lo cual hace que divida a la multiplicación de ambos. Así, $m|(a - b)(a^n - b^n) = a^{n+1} - ab^n - a^nb + b^{n+1} = (a^{n+1} - b^{n+1}) - (a - b)b^n - (a^n - b^n)b$. Como $m| - (a - b)b^n - (a^n - b^n)b$ entonces $m|a^{n+1} - b^{n+1}$ y así $a^{n+1} \cong b^{n+1} \mod m$ ■.

2.

a) Resolver paso a paso la siguiente congruencia: $8x \cong 2 \mod 26$
Primero verificamos que la congruencia lineal tenga solución, para esto es verificamos que $2 = (8, 26)|2$, como se cumple, entonces significa que sí tiene solución. Ahora dividimos toda la congruencia entre el **mcd** y obtenemos:

$$4x \cong 1 mod(13)$$

Entonces tenemos que calcular el inverso multiplicativo de 4 modulo 13, esto lo hacemos con el algoritmo de euclides extendido:

$$13 = 4 * 3 + 1$$

$$\Rightarrow 1 = 13(1) + 4(-3)$$

Por lo tanto el inverso multiplicativo de 4 es -3, que es congruente a su vez con 10 módulo 13, por lo tanto tenemos que el inverso multiplicativo es **10**. Entonces si multiplicamos la congruencia por 10:

$$4(10)x \cong 1(10) mod(13)$$
$$x \cong 10 mod(13)$$

b) Resolver el siguiente sistema de congruencias de ser posible. De lo contrario, dé una razón específica de por qué no se puede resolver.

$$x \cong 4 \mod 11 \quad (1)$$
$$x \cong 25 \mod 35 \quad (2)$$
$$x \cong 15 \mod 22 \quad (3)$$
$$x \cong 5 \mod 10 \quad (4)$$

Primero verificamos que el sistema tenga solución usando $(m_i, m_j)|a_i - a_j$ para cualesquiera i,j :

$1 = (11, 35)| - 21$✓ $\quad 1 = (10, 11)| - 1$✓ $\quad 5 = (35, 10)|20$✓
$11 = (11, 22)| - 11$✓ $\quad 1 = (35, 22)|10$✓ $\quad 2 = (22, 10)|10$✓

Ahora que sabemos que el sistema de congruencias podemos comenzar a resolverlo. Comenzamos por resolver las primeras 2, para obtener una sola congruencia que las contenga a las dos:

$$x \cong 4 \mod 11$$

$$x \cong 25 \mod 35$$

De las cuales obtenemos la siguiente congruencia a resolver:

$$11 * x_0 + 4 \cong 25 mod(35)$$

$$\Rightarrow 11 * x_0 \cong 21 mod(35)$$

Ahora utilizando el algoritmo extendido de euclides:

$$35 = 11 * 3 + 2$$
$$11 = 2 * 5 + 1$$
$$2 = 1 * 2$$

Ahora expresamos 1 como combinación lineal de 11 y 35:

$$1 = 11 - 2 * 5$$
$$1 = 11 - (35 - 11 * 3) * 5$$
$$1 = 11(16) + 35(-5)$$
$$1(21) = 11(16 * 21) + 35(-5 * 21)$$

Entonces el inverso multiplicativo de 11 es 16 modulo 35. $X_0 = 16 * 21$ y se obtiene:

$$x \cong 4 + 11(16 * 21) mod([11, 35])$$
$$x \cong 235 mod(385)$$

Ahora resolvemos la congruencia obtenida junto con la congruencia 3):

$$x \cong 235 \quad \text{mód } (385) \tag{5}$$
$$x \cong 15 \quad \text{mód } (22) \tag{6}$$

Entonces se tiene la siguiente congruencia:

$$15 + 22 * x_1 \cong 235 mod(385)$$

$$\Rightarrow 22 * x_1 \cong 220 mod(385)$$

Aplicando el algoritmo extendido de euclides:

$$385 = 22 * 17 + 11$$

Espresando como combinación lineal:

$$11 = 22(-17) + 385(1)$$

$$11(20) = 22(-17 * 20) + 385(20)$$

Entonces:

$$\begin{aligned} x_1 &= -17 * 20 mod 385 \\ &= -340 mod 385 \\ &= 45 mod 385 \end{aligned}$$

Por lo que se obtiene la nueva congruencia:

$$x \cong 15 + 22(45) mod([385, 22])$$

$$\Rightarrow x \cong 235 mod(770)$$

Por último resolveremos la congruencia que se acaba de obtener con la 4):

$$x \cong 385 mod 770$$

$$x \cong 5 mod 10$$

Entonces se tiene la congruencia:

$$5 + 10 * x_2 \cong 235 mod 770$$

$$\Rightarrow 10 * x_2 \cong 230 mod 770$$

Una solución particular es $x_2 = 23$, entonces:

$$x \cong 5 + 10 * 23 mod([770, 10])$$

$$\Rightarrow x \cong 235 mod(770)$$

Por lo tanto la solución del sistema es:

$$x \cong 235 mod(770)$$

c) Resolver el siguiente sistema de congruencias de ser posible. De lo contrario, dé una razón específica de por qué no se puede resolver.

$$x \cong 4 \quad \text{mód } 7$$

$$x \cong 5 \quad \text{mód } 33$$

$$x \cong 6 \quad \text{mód } 14$$

$$x \cong 10 \quad \text{mód } 22$$

Primero verificamos que el sistema tenga solución usando $(m_i, m_j)|a_i - a_j$ para cualesquiera i,j:

$1 = (7, 33)| - 1$✓ $\quad$ $1 = (7, 22)|6$✓ $\quad$ $11 = (33, 22)|5$✗

$2 = (7, 14)|2$✓ $\quad$ $1 = (33, 14)|1$✓

La última no se cumple, por lo tanto el sistema **no tiene solución**.

3.

a) Sea $\Phi(x)$ la función de Euler, mostrar que $\Phi(p^n) = p^n - p^{n-1}$

Solución:

Todos los números positivos menores o iguales a p^n son (evidentemente) p^n. Ahora, la cantidad de elementos que son primos relativos con p^n son p^n menos el número de elementos que no son primos relativos con p^n, así que sólo hay que encontrar la cantidad c de elementos $x < p^n$ tales que $\text{mcd}(p^n, x) > 1$ y se obtiene $\Phi(p^n) = p^n - c$.

Primero, nótese que $\text{mcd}(p^n, x) = p^i$ donde $0 \leq i \leq n$, ya que los únicos divisores de p^n son precisamente las potencias de p donde el exponente es menor o igual a n.

Luego, si $\text{mcd}(p^n, x) > 1$ significa que x es múltiplo de p. Pero todos los múltiplos de p menores o iguales a p^n son: $1p, 2p, 3p, ..., p^{n-1}p$; es decir, todos los números de la forma mp, donde $m \in \mathbb{Z}$ y $1 \leq m \leq p^{n-1}$. Y precisamente, la cantidad de m's que cumplen esa condición son p^{n-1}, y por lo tanto hay p^{n-1} múltiplos de p menores o iguales a p^n.

Así, $\Phi(p^n) = p^n - p^{n-1}$. ■

b) Dar la cardinalidad de $\mathbb{Z}^*_{129}$ y dar los elementos listados de la forma (a, a^{-1}).

Solución

Para resolver el problema se utilizó ayuda de un programa en C. El primer paso es usar el algoritmo de Euclides extendido para obtener todas las combinaciones lineales de la forma $129x + a(y) = \text{mcd}(129, a)$ con $0 < a < 129$. Si el mcd(129,a) = 1 significa que a es primo relativo con 129 y por lo tanto tiene inverso multiplicativo módulo 129.

Para todos los a que sean primos relativos con 129:

$129x + a(y) = 1$

$\Rightarrow a(y) - 1 = 129(-x)$

$\Rightarrow 129 | a(y) - 1$

$\Rightarrow a(y) \cong 1 \mod 129$

Es decir, y es inverso multiplicativo de a módulo 129. Como y puede ser negativo, se le suma 129 en ese caso para que $y > 0$.

La cardinalidad de $\mathbb{Z}^*_{129}$ es 84. La lista de elementos (a, a^{-1}) es la siguiente:

(1,1), (2,65), (4,97), (5,26), (7,37), (8,113), (10,13), (11,47), (13,10), (14,83), (16,121), (17,38), (19,34), (20,71), (22,88), (23,101), (25,31), (26,5), (28,106), (29,89), (31,25), (32,125), (34,19), (35,59), (37,7), (38,17), (40,100), (41,107), (44,44), (46,115), (47,11), (49,79), (50,80), (52,67), (53,56), (55,61), (56,53), (58,109), (59,35), (61,55), (62,77), (64,127), (65,2), (67,52), (68,74), (70,94), (71,20), (73,76), (74,68), (76,73), (77,62), (79,49), (80,50), (82,118), (83,14), (85,85), (88,22), (89,29), (91,112), (92,122), (94,70), (95,110), (97,4), (98,104), (100,40), (101,23), (103,124), (104,98), (106,28), (107,41), (109,58), (110,95), (112,91), (113,8), (115,46), (116,119), (118,82), (119,116), (121,16), (122,92), (124,103), (125,32), (127,64), (128,128).

4. Descifrar el siguiente mensaje codificado en monoalfabetico explicando paso a paso como lo descifras. No se tomara en cuenta si no se explica cómo se obtiene la clave.

Este cripto análisis se tuvo que hacer de manera más analítica, apoyandonos de la estructura del español, por ejemplo primero observamos que la letra que más se repetía era la P entonces a esta le asignamos la A, y una vez que tuvimos la A, pudimos descubrir la silaba 'LA' y por sonsiguiente supimos que la G era la L en el criptograma, y asi sucesivamente, fuimos sustituyendo en el texto las letras que ibamos encontrando, para así ir intentando descubrir las demás de manera que tuviera sentido el texto. Para hacer más rapido el proceso de sustitución hicimos un programa que fuera haciendo las sustituciones:

```
f = open("encrypted-monoalphabet.txt", "r")
cryptogram = f.read()
f.close()

original_alph = "abcdefghijklmnopqrstuvwxyz"
associat_alph = "PRIMOABCDEFGHJKLNQSTUVWXYZ"#<----
for i in range(len(original_alph)):
    cryptogram = cryptogram.replace(associat_alph[i],original_alph[i])

fw = open("answer.txt","w")
fw.write(cryptogram)
fw.close();
```

Finalmente obtuvimos que la clave es **PRIMO** y el texto descifrado es:

dogma central las principales funciones del dna se resumen en el llamado dogma central de la genetica molecular. el dna sempena tanto una funcion

autocatalitica como una funcion heterocatalitica transcripcion en rna la traduccion a proteinas se lleva a cabo con moldes o patrones de rnam, nunca con

los moldes o patrones de dna. los genes llegan a expresarse fenotipicamente debido a su capacidad para especificar las estructuras de las proteinas

biologicamente activas.

codigo genetico las reacciones bioquimicas son medidas por enzimas, las cuales son todas proteinas. las proteinas son polimeros se subunidaddes monomeros denominados aminoacidos, a menudo llamados residuos. cada aminoacido

tiene un grupo amino nhsubindicedos en uno de sus extremos y un grupo carboxilo cooh en el otro. normalmente, se pueden encontrar veinte diferentes tipos de aminoacidos, en una secuencia especificamente ordenada. en la secuencia de nucleotidos del dna se codifica la clave negativo para la produccion de

proteinas. al numero de nucleotidos que para un solo aminoacido se le denomina codon. hay veinte aminoacidos comunes, pero solo cuatro nucleotidos

diferentes. obviamente, un simple codon un nucleotido que codifica para un aminoacido puede codificar solo para cuatro aminoacidos. un doble codigo dos nucleotidos que codifican para un aminoacido permite solo dieciseis combinaciones. por lo tanto y desde el punto de vista matematico, un triple codigo tres nucleotidos que codifican para un aminoacido es la unidad de codificacion mas pequena codon capaz de ajustarse a los veinte aminoacidos.

la evidencia experimental que apoya el concepto del triple codigo fue proporcionada por el estudio de la adicion de un solo par de bases sencillas

al grupo de enlace sencillo de un bacteriografo. si la transcripcion de una unidad genetica funcional cistron de dna en rnam siempre se lee desde una posicion fija, entonces los primeros seis codones de una cadena de un cistron de dna podria ser la siguiente:

tiaminacitosinaadenina guaninaguaninacitosina tiaminaadeninaadeina adeinaguaninatiamina citosinaguaninaguanina tiaminacitosinaguanina

la adicion de una sola base por ejemplo guanina al final del segundo codon podria desviar o alterar todos los demas codones de un nucleotido furea del registro e impedir la lectura correcta de todos los codones situados a la derecha de la base anadida.

tiaminacitosinaadenina guaninaguaninacitocina guaninatiaminaadenina adeinaadeinaguanina tiaminacitosinaguanina guaninatiaminacitosina guanina

de manera analoga con la eliminacion de nucleotidos. tres eliminaciones o multiplos de tres pueden corregir la lectura en la sintesis de una proteina

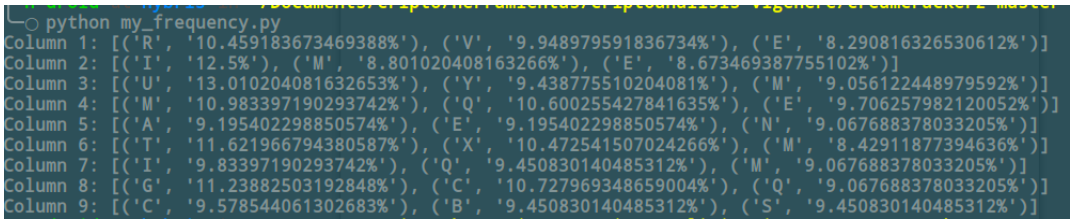
activa. otras evidencias indican que el codon es una secuencia de tres mucleotidos y de aqui que al codigo genetico se le conoca como un triplete o una tercia.

5. Dado el siguiente texto cifrado en vinage hacer la prueba de Kasiski, explicar detalladamente como se obtien la clave y descifrar el mensaje. Sin clave no hay puntos.

Primero encontramos las secuencias más largas que se repitan, calculamos la distacia de cada repetición y descomponemos esta distancia en factores:

Secuencia	Posiciones	Distancias	Factores
WCZTXAKGQIJDOMMKBNW	1018, 6444	5426	2, 2713
UYOEMEIYEXQRGIVQ	4727, 4745	18	2, 3, 3
TWOSHGCEMQHVHIE	25, 736	711	3, 3, 79
UYOEMEIYEXQRGIV	2486, 4727	2241	3, 3, 3, 83
FMSBVVSFMMPEEI	497, 5680	5183	71, 73
AEWUFVFIEOFIU	1219, 1291	72	2, 2, 2, 3, 3
TCWAJIDMTKKCA	1681, 2230	549	3, 3, 61
GNTAGQHIHOITL	1696, 2956	1260	2, 2, 3, 3, 5, 7
FWNSPYFMDXZPO	2508, 2850	342	2, 3, 3, 19
SBBKCCIJFIWIN	3915, 4050	135	3, 3, 3, 5
CTOPMFSUTVKBN	1262, 5617	4355	5, 13, 67
OLIOWASUOIWWU	3132, 4887	1755	3, 3, 3, 5, 13

Ahora que tenemos los factores de las distancias, observamos que el factor que más se repite es **3*3=9**, entonces tomaremos esta como la posible distancia para la palabra clave. Después dividimos todo nuestro texto en 9 columnas, y por cada columna calculamos cuántas veces aparece cada letra y calculamos el porcentaje de cada letra. Para esto se hizo un programa que regresara las 3 palabras más comunes de cada columna.



Una vez que tenemos los porcentajes de cada columna, comparamos con el porcentaje de las letras más usadas en el español Y a partir de aquí es intentar con varias combinaciones, intentando asociar cada columna con el porcentaje que más se asemeje en la tabla de frecuencias del español. La técnica que nos funcionó en general fue asociar la letra que más se repetia de cada columna con la A, y si no tenia sentido, luego se intentaba con la E y así sucesivamente usando la tabla de frecuencias como referencia. Asi fue como obtuvimos la clave:

$$clave = NEUMATICO$$

Texto descifrado:

LASALTASCONCENTRACIONESDERIBONUCLEOTIDOSENPRESENCI
ADELAENZIMAPOLINUCLEOTIDOFOSFORILASAPUEDENGENERAR
MOLECULASDERNAMSINTETICASINVITROALFORMARUNENLACEI
NTERNUCLEOTIDOFOSFODIESTERDEESTAMANERAPUEDENUNIRS
EUNASCONOTRASUNNUMERODEMOLECULASDEURACILOYASIFOR
MARUNAMOLECULASINTETICADEPOLIURACILOCONLAACTIVIDAD
DERNAMALAGREGARPOLIURACILOALOSEXTRACTOSDECELULASB
ACTERIANASSEPRODUCEUNASINTESISLIMITADADEPOLIPEPTIDO
SQUESOLOCONTIENENALAMINOACIDOFENILALANINAESPORESTO
QUEESPROBABLEQUESEANTRESURACILOSLOSQUECODIFIQUENPA
RALASINTESISDELAFENILALANINALASMEZCLASDEDIFERENTESRI
BONUCLEOTIDOSTAMBIENPUEDENFORMARMOLECULASSINTETIC
ASDERNAMCONLOSNUCLEOTIDOSDISPUESTOSENUNORDENALAZA
RPUEDEEMPLEARSEUNACOMBINACIONDETECNICASQUIMICOORG
ANICASOENZIMATICASPARALAPREPARACIONDEPOLIRRIBONUCL
EOTIDOSSINTETICOSSONSECUENCIASDEREPETICIONCONOCIDASC
OMOPOREJEMPLOADENINAURACILADENINAURACILADENINAURA
CILQUECODIFICAALTERNATIVAMENTEPARALOSAMINOACIDOSISO
LEUSINAYTIROSINACITOCINAURACILCITOCINAURACILQUECODIFI
CAPARALALEUCINAYSEINAENFORMAALTERNAETCETERAINCLUS
OENAUSENCIADERNAMYDESINTESISDEPROTEINASUNTRINUCLEO
TIDOSEFIJARAAUNRIBOSOMAPORLOTANTOINVITROPUEDENUTILI
ZARSETRINUCLEOTIDOSDESECUENCIACONOCIDAPARAFIJARSEES
PECIFICAMENTECONUNODEUNAMEZCLADEVEINTEDIFERENTESA
MINOACIDOSYASIUNIRSEALOSRIBOSOMASPOREJEMPLOURACILUR
ACILGUANINASOLOFIJAELRNATCARGADODELEUCINAALOSRIBOS
OMASURACILGAUNINAURACILSOLOFIJAELRNATCARGADODECIST

EINAETCETERAELCODIGOGENETICOESDEGENERADODEBIDOAQU
EEXISTEMASDEUNCODONPARALASINTESISDELAMAYORPARTEDE
LOSAMINOACIDOSELCODIGOESBASICAMENTEELMISMOPRATODO
SLOSORGANISMOSALPARECERDELOSSESENTAYCUATROPOSIBLES
CODONESDELETRASSOLOTRESSONINCAPACESDECODIFICARPARA
CUALQUIERAMINOACIDOAESTOSCODONESSELESDENOMINATRIPL
ETESSINSENTIDOSINTESISDEPROTEINASLAINFORMACIONENUNAS
ECUENCIADESOXIRRIBONUCLEOTIDAESTRANSCRITAOTRADUCID
AENLASECUENCIARIBONUCLEOTIDADEUNAMOLECULADERNAPOR
UNAENZIMAESPECIFICARNAPOLIMERASAENLADOBLEHELICEINTA
CTAESTAENZIMARECONOCECOMOSITIODEINICIACIONCIERTASSE
CUENCIASDEPARESCONABUNDANTEADENAINAYTIAMINAYCOMIE
NZALATRANSCRIOPCIONDEUNADELASDOSCADENASENLAREGION
ADYACENTELASREGIONESPROMOTORASENSINOSONTRANSCRITA
SDENTRODEUNAREGIONESPECIFICADELDNASOLOUNADELASDOSC
ADENATIENESENTIDOESDECIRESTRANCRITAENRNAPEROENOTRA
REGIONDISTINTADEESAMISMAMOLECULADEDNALAOTRACADENA
SERALAQUETENGASENTIDOAPESARDEESTOLAINFORMACIONPAR
AELABORARCUALQUIERMOLECULADADADERNAOCADENAPOLIPE
PTIDICARESIDEEXCLISIVAMENTEENUNADELASDOSCADENASESDE
CIRQUELARNAPOLIMERASANOSALTADEUNACADENADEDNAALAO
TRADURANTEELPRODESODETRANSCRIPCIONDEUNGENENPARTIC
ULAROGRUPODEGENESADYACENTESPARALASINTESISDEUNAMOL
ECULADERNATANTOLAMOLECULADERNAMCOMOLADERNARSEAS
OCIANCONPROTEINASFORMANDOPRECURSORESYQUEENTONCES
SEDIRIGENDELNUBLEOALCITOPLASMAAHIELMENSAJEESLEIDOUN
IDIRECCIONALMENTEPORUNOOMASRIBOSOMASPOLISOMASCOME
NZANDOENELEXTREMOSICADAUNODELOSVEINTEAMINOACIDOSS
ERECONOCEPORSUPROPIOTIPODERNATENTONCESENELCITOPLA
SMAEXISTENUNMINIMODEVEINTEESPECIESDERNATLAUNIONDEU
NAMINOACIDOCONSUMOLECULADERNATESMEDIADAPORUNENZI
MAESPECIFICAENUNPRODESODENOMINADOACTIVACIONOCARGA
DOENALGUNAPARTEDELRNATHAYUNASECUENCIADETRESNUCLE
OTIDOSELANTICODONQUEESELCOMPLEMENTODELCODONDERNA
MLAAFINIDADDELASTERNASCOMPLEMENTARIASLLEVAACADAAM
INOACIDOARELACIONARSEADECUADAMENTECONLOSOTROSAMIN
OACIDOSDELACADENAPOLIEPTIDICAENSINTESISUNAENZIMARIBO
SOMALUNEELGRUPOAMINOYELGRUPOCARBOXILODELOSAMINOA
CIDOSADYACENTESFORMANDOELENLACEPEPTIDICODESPUESDL
AMOLECULADERNATSELIBERADESUAMINOACIDODELRNAMDELRI
BOSOMAQUEDANDOLIBREPARAACTIVARSEOUNIRSECONOTROAM
INOACIDOTAMBIENLIBREDELMISMOTIPOCUANDOELRIBOSOMALL
EGAALFINALDELMENSAJESECOMPLETALATRADUCCIONDELCODI
GONUCLEOTIDOENUNASECUENCIADEAMINOACIDOSLOSRIBOSOM
ASBACTERIANOSESTANCOMPUESTOSDEDOSSUBUNIDADESPRINCI
PALESUNASUBUNIDADGRANDEDECINCUENTASYUNASUBUNIDADD

ETREINTASDONDESESUNIDADSVEDBERGDEFLOTACIONUNCOEFIC
IENTEDESEDIMENTACIONMOLECULARENULTRACENTRIFUGAMAS
DETREINTAPROTEINASDIFERENTESESTANASOCIADASCONELRNA
RENLOSRIBOSOMASPEROAUNNOSEHAELUCIDADOLAFUNCIONESP
ECIFICAQUELLEVAACABOALPARECERCUANDOMENOSHAYDOSSIT
IOSFUNCIONALESENELRIBOSOMAELPRIMEROUNSITIOPEPTIDALY
SEGUNDOUNSITIOAMINACILDURANTELASINTESISDEPROTEINASEL
RNAMSEUNAALASUBUNIDADDETREINTASLAPRIMERAMOLECULAD
ERNATACTIVADAENTRAALSITIOPEPTIDALQUIZAPASANDOATRAV
EZDELSITIOAMINOACILLASIGUIENTEMOLECULADERNATCARGAD
AENTRAALSITIOAMINOACILYENCIMATICAMENTESEFORMAUNENL
ACEPEPTIDICOENTRELOSDOSAMINOACIDOSADYACENTESELRNAT
NOACTIVADOESELSITIOPEPTIDALDEJAAHORAELRIBOSOMAYPUE
DERESULTARENZIMATICAMENTEACTIVADOUNAVEZMASCONTRA
OTRAMOLECULADEMINOACIDODESUMISMAESPECIEELCOMPLEJO
RESTANTERNATDIPEPTIDOPASADELSITIOAMINOACILALSITIOPEP
TIDALCONICIDIENDOCONUNMOVIMIENTODELRIBOSOMAJUNTOCO
NELMENSAJEROQUEEXPONEELSIGUIENTECODONDERNAMENELSI
TIOVACANTEAMINOACILESTEPROCESOSEREPITEHASTAQUESECO
MPLETAELMENSAJESEPIENSAQUECIERTASPROTEINASESPECIFICA
SESDECIRFACTORESDELIBERACIONRECONOCENESTOSCODONESD
ETERMINACIONYSEPARANLADCADENAPOLIPEPTIDICAYACOMPL
ETADELAULTIMAMOLECULADERNATCADAMOLECULADERNATCO
NTIENEDESETENTAYCINCOAOCHENTANUCLEOTIDOSENUNORDEN
ESPCIFICOLATERMINACIONTRESDETODASLASMOLECULASDERNA
TQUESEUNENALOSAMINOACIDOSALPARECERTERMINANENCITOC
INA-CITOCIANADEINAELEXTREMOCINCOTERMINAENUNRESIDUO
DEGUANINAENELRNATSUELENPRESENTARSEBASESPODWALLDW
GVDGADCQUWWDJEDLTGFKPXUKZSGOVXXAHEEKCGXWAXFJJC
LAUEOFHUWHCYECVHFOMICQMVDMBTTMFQLSLIKPBQKZSGWW
PFRNICSRTEIDDCFDWXVOQCVBSQTSYZZJUFQBAFMRFRJSLDVDD
JYEWLBUONEKFOIPLQZDYWBMDXQARIWGVDGBKVCWBMPLUZJU
FQBTLFZJHWUBDHQRCYEWMPXMRJUZOGELAOLUKHHKUDHFIEC
WTFARKHARBBYZRZEFOETMGMFTWZHHWGZCUKGXBOQRKHSSG
AURHXKJOVPNAQTUYIBDHOTRJJCXHJDNSQTZXFOQTEQJSZXIZM
FQHOKTUPZVDMBTSYXZJQKOLSYDMRJUCGIYZFRBSHXGHMZEJA
QHSIZPLYRONCUPDCQKCMGUEZJQKRXALZZKIWOXAMUSZEVSKT
WAMFSAABTHFNLDGRHCXQRVKFOEPYZYZCSSLEYOHWYUOJJYM
BKYNWKPFMLZDGOVXXADJFWQBUCONGQJOXAUZKRSWSGAUFDI
CABTRCAMKHWGIGCYZCEKQHSIZDJIABLTHFHUEMFTRCXZUUFW
GPUPDZDSIKPWUKRTWWGPAGZEYFORJLMBZBYITCCZZRTWWGP
HABFTATBRUZORHSBBCAGMRCABHPWUCFFGFEDNMMKEKSVGY
QPLULSKBCZZEBSGBCNQRZIVSEPJDNKUABTAUEOIELSBCUEARSL
SKXUZZJQESGJXASZUFSGCZAQDYDAXICAMZDSSGTFQWKHWAHC
NQQDYFOEXHUBZQDAXCNQDJFJCUPVXDHKWSERIPNEQVSGXHM
TIQUWEVOMMZDSMJJCLZXKSBBCUGQRSAZZJUZHEQUITSIEDRFSF

XPUXOIYFQBECACVKFOFDFQBLBSAXCMMIVHSOVIOQBFCGSEPW
FHMQVCKSYXZJYFHXHCECVBSDKDNQHEQWBXALZZDFGZBRCESI
EFWVDKGDTEVWYXWMORHSATHXQTEJADHSYBNCYHSIICPNJUD
QHSIZZUUFWGPODZTYDUNPHUMRGMSVDXUEZSSDTGUXZWEJAB
AGQSZEFWGPJGDUULSKBCZZIBSGBCNQRZIVSNCJAKZFWDMXXAD
ZDAQBPLQKJYYIBTHFDUUTWWDUCTVUDUKJJAMWEJATAYZTEQ
EWGDUOHUEWJBIUXZWEJATRCAMUUWBEPWQRGUHHBSCONJFM
SWTBMAVHMBTTHLHDQVSTYOESVGMSLTJMQVBSTHTGUKDULW
HCCZZUUDCLTMJSIUECLSYXZJFJCMTCZZJSGAIAYFZJQDUNCIEBF
TGBXHJGDUUFHXCYDCZVWFXCNQRJYYBBUCOZUEKRXEYZCZUF
RHSYETGEKWVXIZDEBSAHAYOTCQESGHUVDIQKWLTYZBVDLFTP
FONUEFOWTHUMRKJOVXFSTRDABTPFONDYWBSDXQKIDSAIJYPD
ZDAQBPLXZJYFHXHCECVFJCMTCZZJIAGXTHOTVDLFTPFRHEQDR
XTMFZDEDSVJFMLVDKOCTLMOLUVSTRNGZISGAHUOXZCYROWD
LPDCQUOWTHMOVFLWWXWMOLUVSVPGNHRHKSEPYEOVSATBR
CPZUTWZVDXUFFWWBXICONRBSZMTLZZISMOEFOUDISGAIDHQM
KUVSEPGMPLYFOKXUPDCUUHNGUUMTBMMXCXAKRIWBSXGMRI
YTCLDGMRIDSHRGHMLRBYCWTUOKRHSQBDHQRJETFXAUZNKQU
WHCHDZDUKBKPGUSFSGBWGCMKEHSHXHHDZKHSBLRLUOKEJZT
UCSTIQWGEPZUFLHSQTIIDBVSMOMGIPDVBDWUGISDEULWVPMO
GRKEGXVOZCRUVWVXIZORWABTILQBZUFHHHXARCEKSKGIDDJG
MSAPSQMVBLSQIIYDJYJJXCXQQVVWFGRCMOFHGHKDFMCFUKDX
GIPDJFWFMPLETZDLSKTMQMVILCLIYJSFIQOJJYGRKUVSLHIZMLU
KHKPMUFLUFHXVYZDIQUWHCSFHVDWBNCUSQRDJSLEIZRRRAZB
SUPOFHVSEPHFDRIAENTHABFFASGWUSZEBSHTGYMMNWG

6. Cifrado de Hill.

Primero se encontró la relación entre los textos:

`1) CU AL ES SE DE RI VA ND EE ST RU CT UR AS AL GE BR AI CA SD EC OD IG` y

`2) CM WH MK EW DS FG RQ TJ KU IP DQ AJ SN KC WH YY PB QY OE CT GO AL QI`

Se sabe que aplicando el cifrado a 1) se obtiene 2). La relación, cambiando las letras por números, es la siguiente: (2,20) → (2,12), (0,11) → (22,7), (4,18) → (12,10), (18,4) → (4,22), (3,4) → (3,18), (17,8) → (5,6), (21,0) → (17,16), (13,3) → (19,9), (4,4) → (10,20), (18,19) → (8,15), (17,20) → (3,16), (2,19) → (0,9), (20,17) → (18,13), (0,18) → (10,2), (0,11) → (22,7), (6,4) → (24,24), (1,17) → (15,1), (0,8) → (16,24), (2,0) → (14,4), (18,3) → (2,19), (4,2) → (6,14), (14,3) → (0,11), (8,6) → (16,8).

Estratégicamente se eligieron las relaciones (0,11) → (22,7) y (21,0) → (17,16). La razón de esto es porque (0,11) tiene 0 en la primera entrada, (21,0) tiene 0 en la segunda entrada; y además, 11 y 21 son primos relativos con 26, y por lo tanto tienen inversos multiplicativos módulo 26.

Se tienen las siguientes ecuaciones:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 \\ 11 \end{bmatrix} = \begin{matrix} 0a + 11b = 11b \cong 22 \mod 26 \\ 0c + 11d = 11d \cong 7 \mod 26 \end{matrix} \tag{7}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 21 \\ 0 \end{bmatrix} = \begin{matrix} 21a + 0b = 21a \cong 17 \mod 26 \\ 21c + 11d = 21c \cong 16 \mod 26 \end{matrix} \tag{8}$$

Primero, encontremos los valores b y d. Se tiene que $11b \cong 22 \mod 26$
$\Rightarrow b \cong 22(11^{-1}) \mod 26$. El inverso multiplicativo de 11 módulo 26 es 19.
$\Rightarrow b \cong 22(19) = 418 \cong 2 \mod 26$.

Luego, para d se tiene que $11d \cong 7 \mod 26$.
$\Rightarrow d \cong 7(19) = 133 \cong 3 \mod 26$.

Se usa un procedimiento similar para encontrar a y c. El inverso multiplicativo de 21 módulo 26 es 5.
$\Rightarrow a \cong 17(5) = 85 \cong 7 \mod 26$
$\Rightarrow c \cong 16(5) = 80 \cong 2 \mod 26$

Por lo tanto, la matriz usada para cifrar es:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 7 & 2 \\ 2 & 3 \end{bmatrix} \tag{9}$$

La determinante de la matriz es 7(3) - 2(2) = 17, que es primo relativo con 26, y por lo tanto es invertible. El inverso multiplicativo de 17 módulo 26 es 23.

La matriz inversa es la siguiente:

$$23 \begin{bmatrix} 7 & -2 \\ -2 & 3 \end{bmatrix} \mod 26 = \begin{bmatrix} 161 & -46 \\ -46 & 69 \end{bmatrix} \mod 26 = \begin{bmatrix} 17 & 6 \\ 6 & 5 \end{bmatrix} \tag{10}$$

Y es la que se usó para descifrar el criptograma.

El texto original obtenido es el siguiente:

MO DE LO TE OR IC OE LE SP AC IO VE CT OR IA LD EL CO DI GO GE NE
TI CO ES PR ES EN TA DO EN EL CA MP OD EG AL OI SD EC UA TR OB AS ES
SO BR EZ ET AD OS EL PU NT OD EP AR TI DA ES LA BI YE CC IO ND AD AP
OR LA FU NC IO NF QU EM AN DA AL CO NJ UN TO QU EC ON TI EN EA LO SE
LE ME NT OS AD EN IN AC IT OC IN AG UA NI NA UR AC IL AL CO NJ UN TO
DE PA RE JA SO RD EN AD AS LA PA RE JA CE RO CE RO LA PA RE JA CE RO
UN OL AP AR EJ AU NO CE RO YL AP AR EJ AU NO UN OR ES PE CT IV AM EN
TE RE SP ET AN DO EL OR DE NE LC RI TE RI OB IO LO GI CO PA RA ES TA
BL EC ER UN AB IY EC CI ON EN TR EE LC ON JU NT OB AS EY LA SP AR EJ
AS OR DE NA DA SB IN AR IA SE NE LC AM PO DE GA LO IS DE CU AT RO EL
EM EN TO SE SE LC OM PL EM EN TO BA SE EN DN AM OL EC UL AD OB LE PO
RD EC IR UN EJ EM PL OF DE AE SL AP AR EJ AC ER OC ER OF DE CE SC ER
OU NO FD EG ES UN OC ER OY FD EU ES UN OU NO CO MO RE SU LT AD OL AS
UM AD EN UM ER OS BI NA RI OS CO RR ES PO ND IE NT ES AB AS ES CO MP
LE ME NT AR IA SD ED NA ES SI EM PR EL AP AR EJ AO RD EN AD AU NO UN
OE NE ST EC RI TE RI OT EN EM OS OC HO CO NJ UN TO SD EB AS ES OR DE
NA DA SL AP RI ME RB AS EE SG AU CL AS EG UN DA BA SE ES GU AC LA TE
RC ER AB AS EE SC SU GL AC UA RT AE SC UA GL AQ UI NT AE SA CG UL AS
EX TA ES AC GA LA SE PT IM AU GC AY LA QU EF AL TA PA RA CO ME NZ AR
NU ES TR OE ST UD IO SE LE CC IO NA MO SL AS BA SE SO RD EN AD AS GU
AC YA CG UL AS CU AL ES SE DE RI VA ND EE ST RU CT UR AS AL GE BR AI

CA SD EC OD IG OG EN ET IC OP RE VI OA PA RT IR DE LA TI CE SB OL EA
NA SD EL CU AD RO DE BA SE SD ED NA EL OR DE NP RI MA RI OE SG UA CF
UE EL QU ES EC ON SI DE RO DE SP UE SL AS OP ER AC IO NE SB AS IC AS
SU MA YP RO DU CT OE NE LC ON JU NT OD EB AS ES FU ER ON IN TR OD UC
ID AS EN LA DE FI NI CI ON BA SI CA ES TR UC TU RA DA DE LC AM PO DE
GA LO IS SI UN AE ST RU CT UR AD EC AM PO DE GA LO IS EN EL CO NJ UN
TO DE BA SE SO RD EN AD AS GU AC ES SU PU ES TA EN TO NC ES UN AC OR
RE SP ON DE NC IA BI YE CT IV AC ON EL CA MP OD EG AL OI SD EC UA TR
OE LE ME NT OS DE TE RM IN AU NA UN IC AD EF IN IC IO ND ES UM AY PR
OD UC TO RE SU LT AN DO CO MO ID EN TI DA DE SA GC OM OL AI DE NT ID
AD DE LA SU MA YU CO MO ID EN TI DA DD EL PR OD UC TO CO NE ST AS OP
ER AC IO NE SS EV EE LI SO MO RF IS MO CO MO CO NS EC UE NC IA DE ES
TE IS OM OR FI SM OH AY UN IS OM OR FI SM OE NT RE ES TE CO NJ UN TO
YE LC ON JU NT OD EC OO RD EN AS EQ UI SU NO CO MA PU NT OS SU SP EN
SI VO SC OM AE QU IS EN ED ON DE EQ UI SI ES TA EN EL ES PA CI OV EC
TO RI AL CO NL AS UM AC GE LC UA LS EE XP AN DE AL CO NJ UN TO ES EP
AR AT OD AS LA SE NE CO OR DE NA DA SD IC HO DE OT RA FO RM AE LC ON
JU NT OE SE ES LA SU MA DI RE CT AD EE NE GR UP OS EN CG AS IC AD AC
OD ON SE PU ED EV ER CO MO UN EL EM EN TO TR ID IM EN SI ON AL CO NC
OO RD EN AD AS EN EL CA MP OD EG AL OI SD EC UA TR

Donde los espacios correctos serían los siguientes:

"modelo teorico el espacio vectorial del codigo genetico es presentado en el campo de galois de cuatro bases sobre zeta dos el punto de partida es la biyeccion dada por la funcion f que manda al conjunto que contiene a los elementos adenina citocina guanina uracil al conjunto de parejas ordenadas la pareja cero cero la pareja cero uno la pareja uno cero y la pareja uno uno respectivamente respetando el orden el criterio biologico para establecer una biyeccion entre el conjunto base y lasparejas ordenadas binarias en el campo de galois de cuatro elementos es el complemento base en dna molecula doble por decir un ejemplo f de a es la pareja cero cero f de c es cero uno f de g es uno cero y f de u es uno uno como resultado la suma de numeros binarios correspondientes a bases complementarias de dna es siempre la pareja ordenada uno uno en este criterio tenemos ocho conjuntos de bases ordenadas la primer base es g a u clase g u n d a base es g u a c la tercera base es c s u g la cuarta es c u a g la quinta es a c g u la sexta es a c g a la septima u g c a y la que falta para comenzar nuestro estudio seleccionamos las bases ordenadas g u a c y a c g u las cuales se derivan de estructuras algebraicas de codigo genetico previo a partir de la tices boleanas del cuadro de bases de dna el orden primario es g u a c fue el que se considero despues las operaciones basicas suma y producto en el conjunto de bases fueron introducidas en la definicion basica estructurada del campo de galois si una estructura de campo de galois en el conjunto de bases ordenadas g u a c es supuesta entonces una correspondencia biyectiva con el campo de galois de cuatro elementos determina una unica definicion de suma y producto resultando como identidades a g como la identidad de la suma y u como identidad del producto con estas operaciones se ve el isomorfismo como consecuencia de este isomorfismo hay un isomorfismo entre este conjunto y el conjunto de coor-

denas equis uno coma puntos suspensivos coma equis ene donde equis i esta en el espacio vectorial con la suma c g el cual se expande al conjunto ese para todas las ene coordenadas dicho deo traforma el conjunto ese es la suma directa de ene grupos en c g asi cada codon se puede ver como un elemento tridimensional con coordenadas en el campo de galois de cuatro elementos por lo que har sesenta y cuatro codones diferentes"