Universidad Nacional Autónoma de México

Facultad de Ciencias

Criptografía y Seguridad

Tarea 2: Cifrados monoalfabéticos

Fecha de entrega: 05/09/2023

Equipo:

Criptonianos

Acosta Arzate Rubén - 317205776

Bernal Marquez Erick - 317042522

Deloya Andrade Ana Valeria - 317277582

Gutiérrez Medina Sebastián Alejandro - 318287021

Rivera Silva Marco Antonio - 318183583

Inversos Multiplicativos

1. Investiga o desarrolla el algoritmo para encontrar los inversos multiplicativos módulo n. El algoritmo debe ser capaz de decidir si existe o no dicho inverso. No lo implementes, solo reporta el pseudocódigo. Explica tu respuesta y añade un ejemplo de cómo funciona. Si no es de tu autoría, debes incluir las fuentes bibliográficas.

Para saber si existe el inverso multiplicativo debemos saber si el módulo m y el número al cual queremos obtener inverso n son coprimos, es decir que *MCD(m,n)=1*, en caso de no tener inverso quiere decir que no existe dicho inverso. Así el primer paso de nuestro algoritmo es saber si *MCD(m,n)=1*

Para saber si son coprimos basta aplicar algoritmo de Euclides: escribimos nuestro módulo m en términos de n más un residuo r, como queremos un residuo entonces $0 \leq r < n$, es decir $m = nq + r$, donde $q, r \in Z$

Luego el número que está multiplicando pasa a ser el número que queremos expresar con suma y producto; y el residuo pasa a ser el multiplicador de dicha expresión, es decir queremos a n en términos del residuo r más otro residuo r_1, esto es $n = rq_1 + r_1$

Siguiendo esta misma idea expresamos a r en términos de r_1 más un residio r_3, es decir $r = r_1q_2 + r_2$. Así hasta que ya no podamos expresar la r en términos de una multiplicación más un residuo r'. El último residuo no cero es nuestro *MCD(m,n)*, que recordemos debe ser 1 para encontrar nuestro inverso módulo n.

Suponiendo que el *MCD(m,n)* sí es igual a 1. Despejamos todas las expresiones que no dio el algoritmo de Euclides en terminos de los residuos.

$$m = nq + r \rightarrow r = nq + mq'$$

$$n = rq_1 + r_1 \rightarrow r_1 = rq_1 + nq'$$

$$r = r_1q_2 + r_2 \rightarrow r_2 = r_1q_2 + rq''$$

Para nuestros propósitos es muy conveniente que todas nuestras *q's* primas sean igual a 1.

Como son numeros coprimos el último residuo no cero es igual 1, así nuestra nuestra ultima expresión tiene forma $1 * r_f = r_{f-1}q_f + r' * 1$, llamaremos a esta expresión *e*.

Luego sustituiremos en la expresión *e* la expresión *e-1* y resolvemos la expresión, de tal manera que podamos sustituir en esta la expresión *e-2* luego la *e-3*, *e-4*, así hasta la última expresión y de tal manera que tengamos la siguiente expresión $1 = ms + nt$, donde recordemos que m es nuestro módulo y n el número que queremos obtener su inverso, además s y t las obtenemos justo de hacer las sustituciones. Como m es nuestro módulo entonces podemos escrbir $1 = nt\ mod_{26}$

Cómo ya sabemos que n es el número a cual obtener inverso y que al multiplicarlo por t nos da como resultado 1, entonces t es justo nuestro inverso.

El código en python es el siguiente

```
def find_mod_inv(a,m):
    for x in range(1,m):
        if((a%m)*(x%m) % m==1):
            return x
    raise Exception('El inverso no existe')
```

Donde podemos observar que justo las operaciones las hace desde 1 hasta el módulo, pues no tendría sentido que fueran "mas allá" del rango del módulo; notemos también que hacemos una comprobación para saber si el MCD es igual 1 y en caso de no serlo le arrojamos una excepción de que no existe tal inverso, por último damos como resultado la x que justamente el inverso en el módulo.
*Código en las referencias

Ejemplo hecho a mano

Sea la ecuación $17\alpha \cong 11\ mod_{26}$, entonces queremos saber α^{-1}, primero obtenemos MCD(17,26) con el algoritmo de Euclides.

$$26 = 17 * 1 + 9$$

$$17 = 9 * 1 + 8$$

$$9 = 8 * 1 + 1$$

$$8 = 8 * 1 + 0$$

Despejamos las expresiones respecto al residuo

$$9 = 17 * (-1) + 26 * 1 \tag{A}$$

$$8 = 17 * 1 + 9 * (-1) \tag{B}$$

$$1 = 9 * 1 + 8 * (-1) \tag{C}$$

Sustituimos B en C

$$1 = 9 * 1 + 8 * (-1)$$

$$1 = 9 * 1 + [17 * 1 + 9 * (-1)] * (-1)$$

$$1 = 9 * 2 + 17 * (-1)$$

Sustituimos con A

$$1 = [17 * (-1) + 26 * 1] * 2 + 17 * (-1)$$

$$1 = 26 * 2 + 17 * (-3)$$

Como es módulo 26 entonces podemos aplicar la siguiente igualdad

$$1 = 26 * 2 + 17 * (-3)$$

$$1 = 17 * (-3) \quad mod_{26}$$

$$1 = 17 * 23 \quad mod_{26}$$

De esta manera sabemos que le inverso de 17 con mod_{26} es 23, ya que al multiplicarlos nos da el elemento neutro. $\alpha^{-1} = 23$

Criptograma

2. Descifra el mensaje del criptograma.

GK NKNIMUK F LKHPFO UH AUKHQJ UH AUKHQJ MUK LUNIKPK OIVFCIZFO AJH CJP MUK HJP TFRIFH IGLUCPFNJ F KPF QFOKF UH AUKHQJ MUK TFRCFOF NK CJP GIPQKOIJPJP QKOOJOKP NK HUKPQOF HFQUOFCKZF Y NKPLKOQFPK GIKNJP KPQOKGKAKNJOKP MUK NKBFPK FC CKAQJO AJH QKGJO NK GIOFO TFAIF PU FCOKNKNJO MUK LFOFCIZFPK CF PFHSOK Y FAKCKOFOF CJP CFQINJP NKC AJOFZJH PI HJ PK AJHPKSUIF KPJP OKPUCQFNJP GI AUKHQJ NK EFHQFPGFP PKOIF IHNISHJ NK PU HJGROK PKHQIF CF VFAIF IHAFLFAINFN NK IHVKHAIJH CF GFYJO NKPSOFAIF MUK LUKNK FEKAQFO F UH CKAQJO AUFHNJ F PUP FHPIJPFP IHVJFAIJHKP OKPLJHNK PJCJ CF HFNF GFOY W PTKCCKY

Procedimiento:

La estrategia que usamos para descifrar el criptograma fue comenzar por las letras más repetidas que son la K y F que se repetían 67 y 64 veces respectivamente. Con ese dato y sabiendo que el mensaje está en español, sabemos que las letras más usadas en este idioma son A y E, con esto y un hint de la profesora de que la letra más repetida es la E pudimos obtener nuestro primer avance. La letra K corresponde a la letra E

Después nos fijamos en las palabras cortas en el cifrado, como las letras Y, F y W, las cuales pueden ser las letras A, O, Y, de nuevo, se debe a que en el idioma español estas letras suelen ir aisladas y no existe alguna otra letra que caiga en este caso. La letra F es la que más se repite, correspondiendo a la letra A en el texto descrifrado, no puede ser la letra E ya que en el texto cifrado no la encontramos sola, la E no aparece en el idioma español de manera aislada (salvo muy pequeñas excepciones).

Luego analizamos las palabras que contiene dos letras, destacamos en especial FC y CF por dos motivos: el primero es que ya sabemos que la F corresponde a la A y porque las letras se pueden voltear formando alguna palabra en español que haga sentido al voltearlas. Las únicas palabras que cumplen esto son AL y LA, por lo tanto la C corresponde a la L

De la misma manera destacamos la palabra PUP y PU siendo la primera un palíndromo como OSO, OJO, ORO, etc, pero no harían sentido con la PU, ya que no hay palabras en español como OS, OJ, OR. Los posibles candidatos son SUS y SU, y también ESE y ES, pero ya vimos que la K corresponde a la E, por descarte nos quedamos con que la letra P corresponde a la S y la letra U corresponde a la U.

Ahora podemos empezar a sustituir algunas letras en el texto cifrado para que hagan sentido en español, por ejemplo la palabra CJP sabemos que, sustituyendo las letras descifradas, corresponde a la palabra LJS, la letra J podría ser A o la letra O, pero no puede ser la A porque ya sabemos que la letra F corresponde a esta, por lo tanto la letra J es la letra O.

Otro ejemplo son las palabras HJP y las palabras juntas $PI\ HJ\ PK$, que sustituyendo las letras ya descifradas corresponden a HOS y $SI\ HO\ SE$, puede que la H sea la L pero esto no es posible porque ya sabemos que la C es la L, de igual manera puede que la I sea la E o la U pero ya sabemos cual es el cifrado de cada una de estas, por lo cual la letra I corresponde a la letra I y la H corresponde a la N, siendo así el texto descifrado NOS y $SI\ NO\ SE$.

Así mismo la palabra cifrada AJH corresponde a AON, esto nos dice que la A es la letra C, ya que no hay ninguna palabra que termine en "on" de 3 letras, (y si acaso las hay, no son comunes).

Siguiendo este mismo razonamiento de sustituir las letras que ya desciframos en el texto cifrado para ver con qué palabra haría "match" en el idioma español es que pudimos descifrar el resto de la letras, y por lo tanto el texto.

En la siguiente tabla se muestran las letras originales en el texto cifrado junto con a qué letra corresponde en el descifrado.

Original	Descifrado	Original	Descifrado	Original	Descifrado
A	C	J	O	S	G
B	J	K	E	T	H
C	L	L	P	U	U
D	no aparece	M	Q	V	V
E	F	N	D	W	W
F	A	O	R	X	no aparece
G	M	P	S	Y	Y
H	N	Q	T	Z	Z
I	I	R	B		

Criptograma Descifrado:

Me dedique a pensar un cuento un cuento que pudiese rivalizar con los que nos habían impulsado a esa tarea un cuento que hablara de los misteriosos terrores de nuestra naturaleza y despertase miedos estremecedores que dejase al lector con temor de mirar hacia su alrededor que paralizase la sangre y acelerara los latidos del corazón si no se conseguía esos resultados mi cuento de fantasmas seria indigno de su nombre sentía la vacía incapacidad de invención la mayor desgracia que puede afectar a un lector cuando a sus ansiosas invoaciones responde solo la nada mary W shelley.

Cifrado afín

3. Cifra el enunciado: "Por mi raza hablará el espíritu" usando una transformación afín. Investiga a quién se le atribuye la frase.

Mensaje original:"Por mi raza hablará el espíritu"

Formula: $\alpha x + \beta$ con $\alpha = 3$ y $\beta = 5$

En la siguiente tabla se muestra la posición a la cual pertenece la letra, la operación y a qué letra pertenece de manera ya cifrada.

Letra	Número	Número Cifrado	Letra Cifrada
P	15	((3*15)+5) mod_{26}=24	Y
O	14	(((3*14)+5) mod_{26}=21	V
R	17	((3*17)+5) mod_{26}=4	E
M	12	((3*12)+5) mod_{26}=15	P
I	8	((3*8)+5) mod_{26}=3	D
A	0	((3*15)+0) mod_{26}=5	F
Z	25	((3*25)+5) mod_{26}=2	C
H	7	((3*7)+5) mod_{26}=0	A
B	1	((3*1)+5) mod_{26}=8	I
L	11	((3*11)+5) mod_{26}=12	M
E	4	((3*4)+5) mod_{26}=17	R
S	18	((3*18)+5) mod_{26}=7	H
T	19	((3*19)+5) mod_{26}=10	K
U	20	((3*20)+5) mod_{26}=13	N

Mensaje cifrado: "YVE PD EFCF AFIMFEF RM RHYDEDKN"

El mensaje se le atribuye a José Vasconcelos Calderón un abogado, político, escritor, educador, funcionario público, pedagogo y filósofo mexicano. Es también el nombre que lleva la Escuela Nacional Preparatoria No. 5 (ENP 5).

Fue nombrado primer Secretario de Educación Pública del país y rector de la Universidad Nacional condecorado como Doctor Honoris Causa por la misma institución y por las de Chile, Guatemala y otras latinoamericanas.

*Según wikipedia

Referencias

- Sandoval, L. I. M. (2023). Álgebra superior II: El algoritmo de Euclides. El blog de Leo. https://blog.nekomath.com/algebra-superior-ii-el-algoritmo-de-euclides/
- El algoritmo de Euclides (Artículo) | Khan Academy. (s. f.). Khan Academy. https://es.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/the-euclidean-algorithm
- Joshi, S. (2023, 30 enero). Calcular el inverso multiplicativo modular en Python. Delft Stack. https://www.delftstack.com/es/howto/python/mod-inverse-python/
- Fletcher Pratt, Secret and Urgent: The Story of Codes and Ciphers Blue Ribbon Books, 1939, pp. 254-255
- Colaboradores de Wikipedia. (2023). José Vasconcelos. Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/José_Vasconcelos
- Scribbr. (2022, 31 agosto). Formato con el generador de Scribbr. https://www.scribbr.es/citar/generador