Sobre la construcción de algoritmos de cifrado por desplazamiento

Adriana Gómez – Orlando Hernández
Educación **M**edia **T**ecnológica en Informática
CETP

Sylvia da Rosa – Federico Gómez
Instituto de **Co**mputación, **F**acultad de **Ing**eniería
UDELAR

Introducción

Las transformaciones criptográficas pueden describirse mediante una **función matemática**.

Introducción

Las transformaciones criptográficas pueden describirse mediante una **función matemática**.

Esto permite automatizar las operaciones de cifrado y descifrado mediante la **programación de algoritmos**.

Introducción

Las transformaciones criptográficas pueden describirse mediante una **función matemática**.

Esto permite automatizar las operaciones de cifrado y descifrado mediante la **programación de algoritmos**.

Propuesta coordinada entre las asignaturas Introducción a la Computación y Programación I para los estudiantes de Primer Año de Bachillerato en Informática de Escuela Técnica Atlántida.

Objetivos

Introducir al tema de criptosistemas sencillos para que nuestros alumnos logren **formalizar un algoritmo de cifrado** por desplazamiento.

Objetivos

Introducir al tema de criptosistemas sencillos para que nuestros alumnos logren **formalizar un algoritmo de cifrado** por desplazamiento.

Obtener información acerca de la construcción del concepto, que posibilite **aportar a una didáctica** de introducción al concepto **a nivel preuniversitario.**

Objetivos

Introducir al tema de criptosistemas sencillos para que nuestros alumnos logren **formalizar un algoritmo de cifrado** por desplazamiento.

Obtener información acerca de la construcción del concepto, que posibilite **aportar a una didáctica** de introducción al concepto **a nivel preuniversitario.**

Elaborar **nuevas propuestas pedagógicas** en atención a los resultados observados.

Marco Teórico

Epistemología Genética de Jean Piaget.

- Provee fundamentos para la investigación en didáctica de la informática.

Marco Teórico

Epistemología Genética de Jean Piaget.

- Provee fundamentos para la investigación en didáctica de la informática.

A partir de un contexto de trabajo:

- Curso de Epistemología Genética y aplicaciones a la Didáctica de la. Informática.
  - Centrado en el cómo enseñar informática:
    - » ¿Cómo aprenden los estudiantes?
    - » ¿Cuál es el rol del docente?

Metodología

Basada en la resolución de problemas.

Metodología

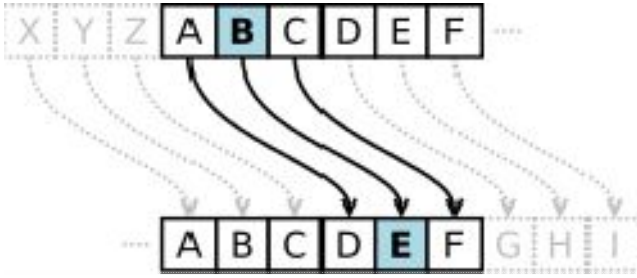
Basada en la resolución de problemas.

El problema dividido en subproblemas.

- Varias y sucesivas instancias.
  - 3 instancias en Introducción a la Computación.
  - 3 instancias en Programación.

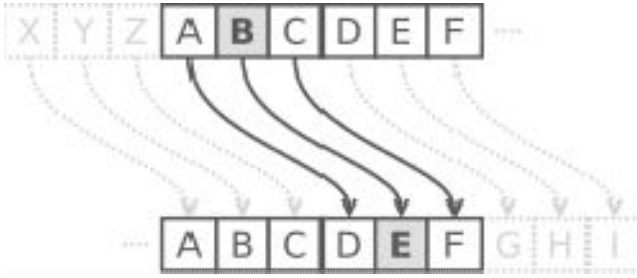
Instancia #1

a Introducción al cifrado de César.



Instancia #1

a Introducción al cifrado de César.

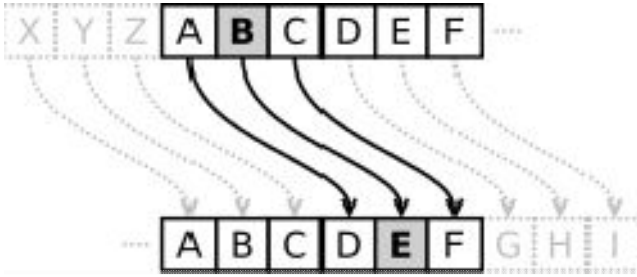


b Construcción de una tabla.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

Instancia #1

a Introducción al cifrado de César.



b Construcción de una tabla.

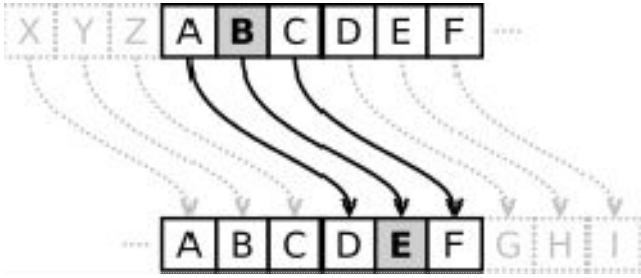
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

c Un asunto de… ***espías!***

Ñ	D	U	J	D	W	H	C	V	L	J	X	H	P	C	W	X	V	C	S	D	V	R	V

Instancia #1

a Introducción al cifrado de César.



b Construcción de una tabla.

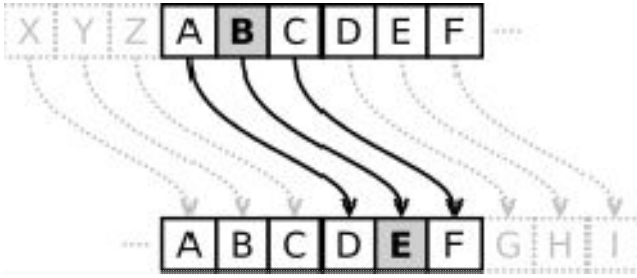
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	0	1	2
	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

c Un asunto de… ***espías!***

Ñ	D	U	J	D	W	H	C	V	L	J	X	H	P	C	W	X	V	C	S	D	V	R	V

Instancia #1

a Introducción al cifrado de César.



b Construcción de una tabla.

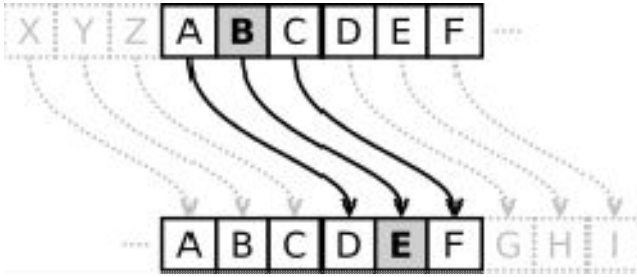
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
D	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27			
	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z			

c Un asunto de… ***espías!***

Ñ	D	U	J	D	W	H	C	V	L	J	X	H	P	C	W	X	V	C	S	D	V	R	V

Instancia #1

a Introducción al cifrado de César.



b Construcción de una tabla.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	0	1	2
C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z		A	B

c Un asunto de… ***espías!***

Ñ	D	U	J	D	W	H	C	V	L	J	X	H	P	C	W	X	V	C	S	D	V	R	V

L	A	R	G	A	T	E		S	I	G	U	E	N		T	U	S		P	A	S	O	S

Instancia #2

a ¿Qué pasos siguió la Agente 99 para ocultar el mensaje secre

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	0	1	2
C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z		A	B

b ¿
llega?

c U

Ñ	D	U	J	D	W	H	C	V	L	J	X	H	P	C	W	X	V	C	S	D	V	R	V

¿Pue que
has e
lógico-matemático.

L	A	R	G	A	T	E		S	I	G	U	E	N		T	U	S		P	A	S	O	S

Instancia #2

a ¿Qué pasos siguió la Agente 99 para ocultar el mensaje secreto? *Expresa en lenguaje natural.*

A) ESCRIBIO EL MENSAJE Y LUEGO LO CIFRO

Instancia #2

a ¿Qué pasos siguió la Agente 99 para ocultar el mensaje secreto? *Expresa en lenguaje natural.*

A) ESCRIBIO EL MENSAJE Y LUEGO LO CIFRO

A: Corro tres lugares hacia la derecha cada letra del abecedario.

Instancia #2

a ¿Qué pasos siguió la Agente 99 para ocultar el mensaje secreto? *Expresa en lenguaje natural.*

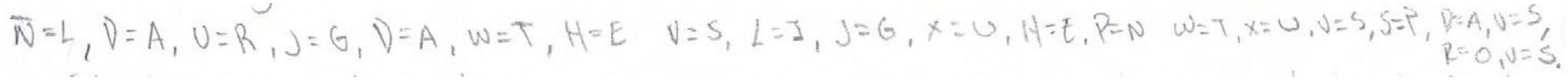
A) ESCRIBIO EL MENSAJE Y LUEGO LO CIFRO

A: Corro tres lugares hacia la derecha cada letra del abecedario.

A- los pasos que siguio la agente 99 para ocultar el mensaje fué usando el metodo de césar utilizando el abecedario normal y moviendo 3 lugares cada letra tenía una posición.

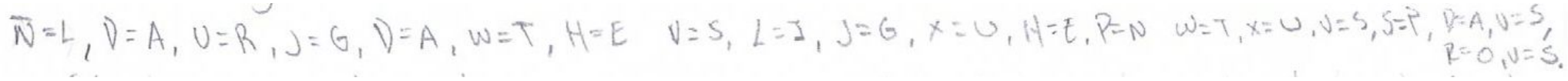
Instancia #2

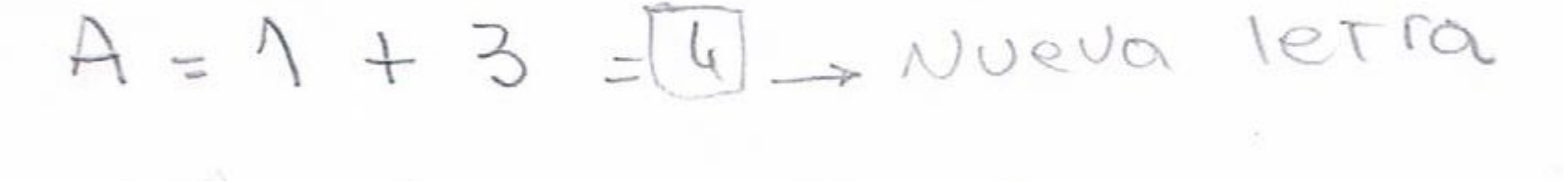
b ¿Puedes dar una expresión para la solución a la que llega?



Instancia #2

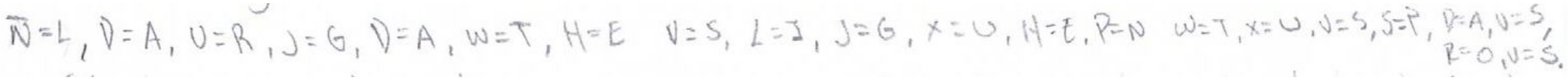
b ¿Puedes dar una expresión para la solución a la que llega?

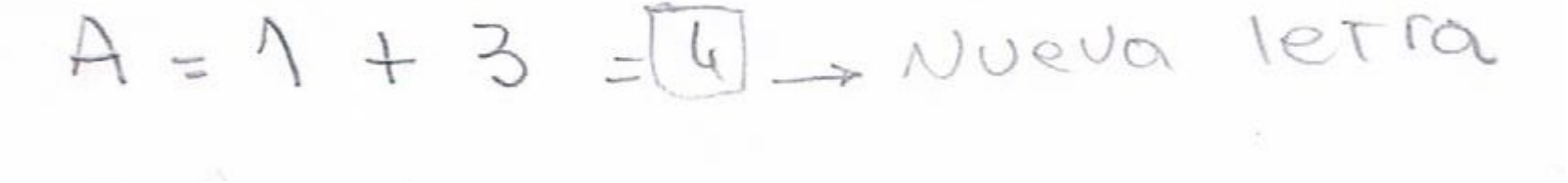


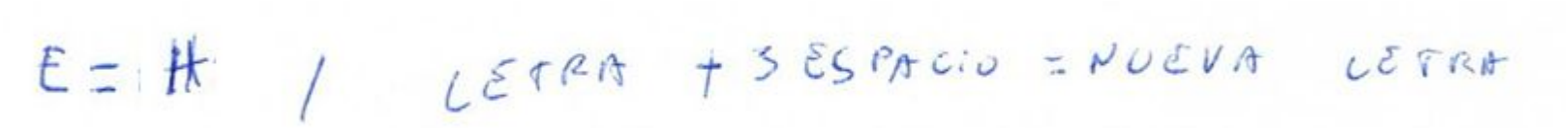


Instancia #2

b ¿Puedes dar una expresión para la solución a la que llega?



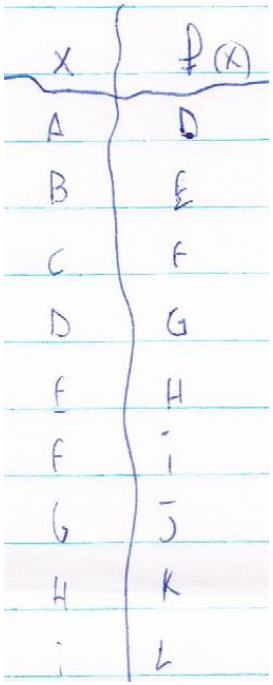


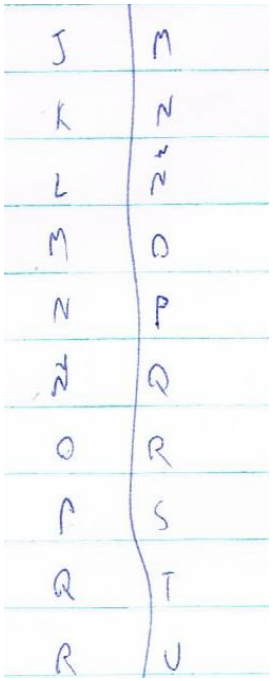


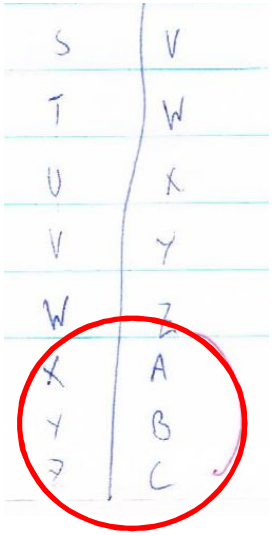
Instancia #2

C Un asunto de… ***informáticos!***

¿Puedes determinar una función que defina la expresión que has dado en la pregunta anterior?



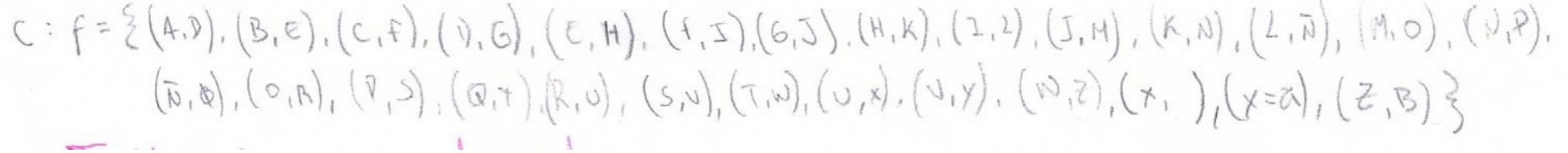




Instancia #2

C Un asunto de… ***informáticos!***

¿Puedes determinar una función que defina la expresión que has dado en la pregunta anterior?



Instancia #3

a BUSCANDO LA FUNCIÓN *v.1*

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	0	1	2
C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z		A	B

b BUSCANDO LA FUNCIÓN *v.2*

Si utilizamos la expresión de cifrado que ha sido determinada por algunos compañeros:

Nueva letra=*Letra escondida* + 3

c BUSCANDO LA FUNCIÓN *v.3*

Define la función asociada en lenguaje lógico-matemático.

Instancia #3

a BUSCANDO LA FUNCIÓN ***v.1***

ESTUDIANTE #1

$C \rightarrow f(3) = 3 + 3 = 6 \rightarrow F$

$L \rightarrow f(12) =$ 12+3=15 → Ñ

$A \rightarrow f(1) =$ 1+3=4 → D

$V \rightarrow f(23) =$ 23+3=26 → Y

$E \rightarrow f(5) =$ 5+3=8 → H

b BUSCANDO LA FUNCIÓN ***v.2***

$X \rightarrow f(25) =$ 25+3=28 →

$Y \rightarrow f(26) =$ 26+3=29 → A

$Z \rightarrow f(27) =$ 27+3=30 → B

¿Es correcta la solución inicial dada?

No es correcta porque el resultado no entra en la longitud 27

Instancia #3

a BUSCANDO LA FUNCIÓN *v.1*

ESTUDIANTE #2

$C \rightarrow f(3) = 3 + 3 = 6 \rightarrow F$

$L \rightarrow f(12) = 12+3 = 15 \rightarrow N$

$A \rightarrow f(1) = 1+3 = 4 \rightarrow D$

$V \rightarrow f(23) = 23+3 = 26 \rightarrow Y$

$E \rightarrow f(5) = 5+3 = 8 \rightarrow H$

b BUSCANDO LA FUNCIÓN *v.2*

$X \rightarrow f(25) = 25+3 = 28 \rightarrow$ No se ubica en el Abecedario

$Y \rightarrow f(26) = 26+3 = 29 \rightarrow$ No se ubica en el Abecedario

$Z \rightarrow f(27) = 27+3 = 30 \rightarrow$ No se ubica en el Abecedario

¿Es correcta la solución inicial dada?

No es correcto porque no se ubica en el Abecedario

Instancia #3

a BUSCANDO LA FUNCIÓN ***v.1***

ESTUDIANTE #3

$C \rightarrow f(3) = 3 + 3 = 6 \rightarrow F$

$L \rightarrow f(12) = 12 + 3 = 15 \rightarrow$ Ñ

$A \rightarrow f(1) = 1 + 3 = 4 - 0$ D

$V \rightarrow f(23) = 23 + 3 = 26 \rightarrow$ Y

$E \rightarrow f(5) = 5 + 3 = 8 \rightarrow$ H

b BUSCANDO LA FUNCIÓN ***v.2***

$X \rightarrow f(25) =$ [25 + 3 = 28 = 0]

$Y \rightarrow f(26) =$ A (1) [26 + 3 = 29 = 1]

$Z \rightarrow f(27) =$ B (2) [27 + 3 = 30 = 2]

= ESPACIO VACÍO (0)

¿Es correcta la solución inicial dada?

ES ~~PARCIALMENTE~~ INCORRECTA, SE APLICA A LA MAYORÍA DE LOS CASOS, PERO NO A ESTOS.

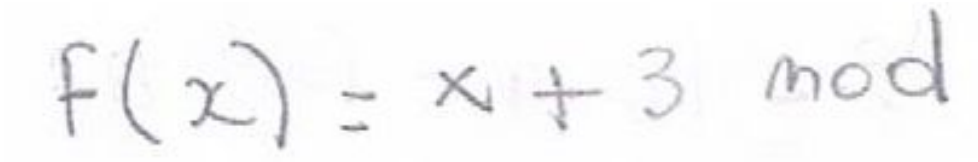
28 ($0 \leq X \leq 27$)

Instancia #3

C BUSCANDO LA FUNCIÓN *v.3*

ESTUDIANTE #1

Define la función asociada en lenguaje lógico-matemático.



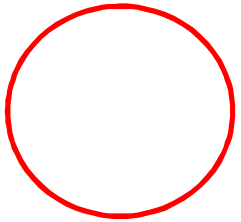
Instancia #3

C BUSCANDO LA FUNCIÓN *v.3*

ESTUDIANTE #1

Define la función asociada en lenguaje lógico-matemático.

$f(x) = x + 3 \mod$

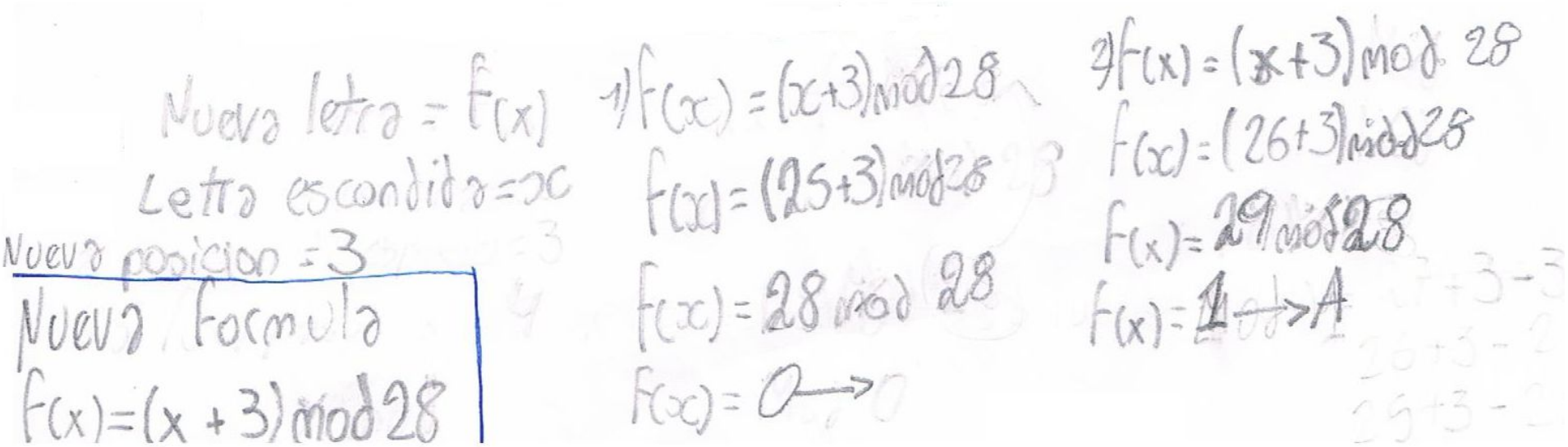


Instancia #3

c BUSCANDO LA FUNCIÓN *v.3*

ESTUDIANTE #2

Define la función asociada en lenguaje lógico-matemático.



Instancia #3

C BUSCANDO LA FUNCIÓN *v.3*

ESTUDIANTE #2

Define la función asociada en lenguaje lógico-matemático.

3 $f(x) = (x+3) \bmod 28$

$f(x) = (27+3) \bmod 28$

$f(x) = 30 \bmod 28$

$f(x) = 2 \rightarrow B$

30 | 28

2 | 1

Para mi la formula del cifrado de César

$f(x) = (x+3) \bmod 28$

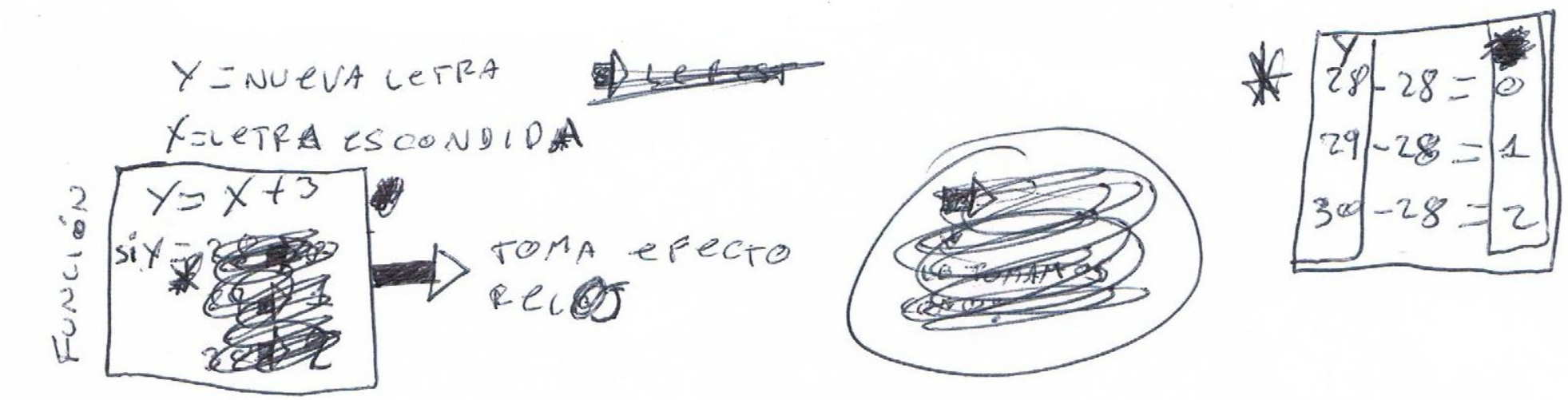
El 28 lo saque por el total de la longitud del Abecedario.

Instancia #3

C BUSCANDO LA FUNCIÓN *v.3*

ESTUDIANTE #3

Define la función asociada en lenguaje lógico-matemático.

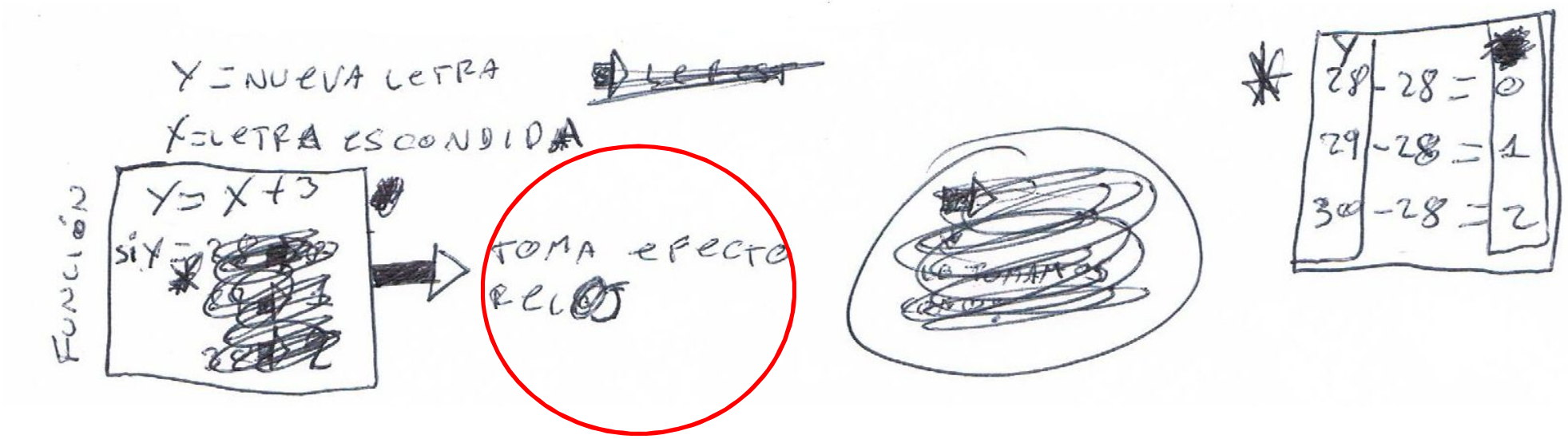


Instancia #3

c BUSCANDO LA FUNCIÓN *v.3*

ESTUDIANTE #3

Define la función asociada en lenguaje lógico-matemático.



Instancia #1

a PROPUESTA.

Es un paso más de lo trabajado en Introducción a la Computación.

Instancia #1

a PROPUESTA.

Es un paso más de lo trabajado en Introducción a la Computación.

Realizar un programa en Java que codifique y decodifique mensajes aplicando diversas técnicas de cifrado (por ejemplo la técnica del cifrado de César).

Instancia #2

a PRIMERAS VERSIONES.

Guiar a los estudiantes a codificar en lenguaje Java la función obtenida en Introducción a la Computación.

Instancia #2

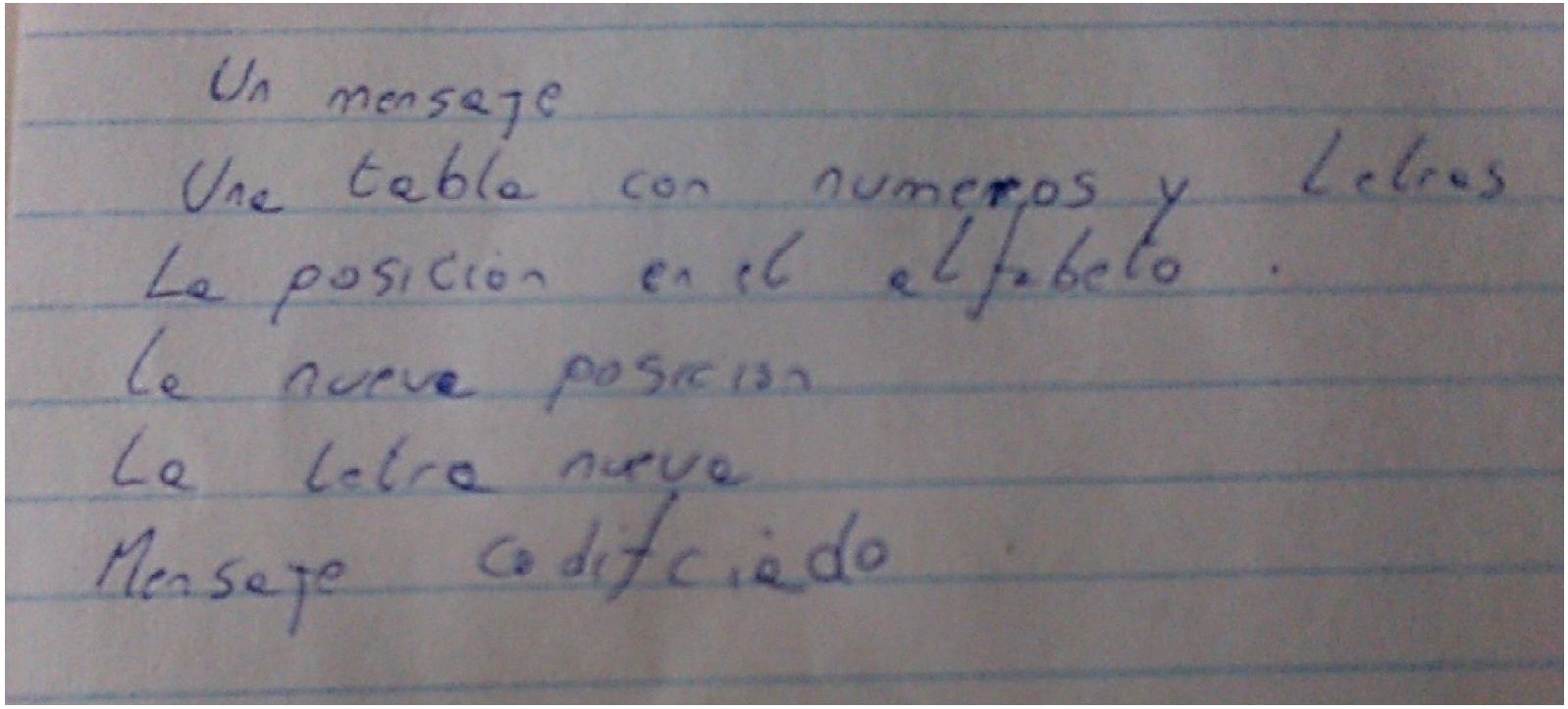
a PRIMERAS VERSIONES.

¿Qué datos necesita la función codificar?

Instancia #2

a PRIMERAS VERSIONES.

¿Qué datos necesita la función a codificar?



Instancia #2

a PRIMERAS VERSIONES.

Según la respuesta anterior, ¿Qué variables deben declarar en Java?

Instancia #2 (Prog.)

a PRIMERAS VERSIONES.

Según la respuesta anterior, ¿Qué variables deben declarar en Java?

Un mensaje.

Una tabla con números y letras.

La posición en el alfabeto.

La nueva posición.

Mensaje codificado.

Instancia #2

a PRIMERAS VERSIONES.

Según la respuesta anterior, ¿Qué variables debe declarar en Java?

Un mensaje.

```
String mensaje;
```

Una tabla con números y letras.

```
char[]letter = {' ','a','b','c','d','e','f','g','h','i'
```

La posición en el alfabeto.

```
int j;
```

La nueva posición.

```
int nuevaPosicion;
```

Mensaje codificado.

```
char[]P;
```

Instancia #2

a PRIMERAS VERSIONES.

¿Cómo se realizan las tareas de la función codificar?

- Separar el mensaje en letras.

- Buscar el número de la letra en el alfabeto.

- Calcular(x+3)mod 28.

Instancia #2

a PRIMERAS VERSIONES.

¿Cómo se realizan las tareas de la función codificar?

- Separar el mensaje en letras.
- Buscar el número de letra en el alfabeto.
- Calcular(x+3)mod 28.

```
letras=mensaje.toCharArray();

P=new char[letras.length];

for(i=0; i<letras.length; i++){
    for(j=0; j<letter.length; j++){
        if(letras[i]==letter[j]){
            nuevaPosicion=(j+ajuste+Code)%28;
            P[i]=letter[nuevaPosicion];
        }
    }
}
```

Instancia #3

a En esta última instancia se realizaron algunas optimizaciones de código.

Conclusiones y Trabajo a futuro

- Se identificó un tipo de error “característico”, que permite comprender el tipo de dificultad que tiene la construcción de algoritmos de cifrado por desplazamiento:
  - El problema del “efecto reloj”.

Conclusiones y Trabajo a futuro

- Se identificó un tipo de error “característico”, que permite comprender el tipo de dificultad que tiene la construcción de algoritmos de cifrado por desplazamiento:
  - El problema del “efecto reloj”.

- Necesidad de profundizar en el análisis de los obstáculos encontrados.

Conclusiones y Trabajo a futuro

- Se identificó un tipo de error “característico”, que permite comprender el tipo de dificultad que tiene la construcción de algoritmos de cifrado por desplazamiento:
  - El problema del “efecto reloj”.

- Necesidad de profundizar en el análisis de los obstáculos encontrados.

- Inquietud por implementar trabajos futuros en relación a la conceptualización de temas vinculados a nuestra disciplina.

judfldvcsrucvxcdwhpflrp

```
1-Seleccionar Cifrado
2-Cifrar Mensaje
3-Descifrar Mensaje
4-Forzar Decodificacion
5-Ver ultimo mensaje...
6-Salir
                                        Codigo actual:Cifrado de Cesar 3 espacios
```

```
1-Seleccionar Cifrado
2-Cifrar Mensaje
3-Descifrar Mensaje
4-Forzar Decodificacion
5-Ver ultimo mensaje...
6-Salir
                                    Codigo actual:Cifrado de Cesar 3 espacios
3
```

```
1-Seleccionar Cifrado
2-Cifrar Mensaje
3-Descifrar Mensaje
4-Forzar Decodificacion
5-Ver ultimo mensaje...
6-Salir
                                        Codigo actual:Cifrado de Cesar 3 espacios
3
Ingrese su mensaje para descodificar

```

```
1-Seleccionar Cifrado
2-Cifrar Mensaje
3-Descifrar Mensaje
4-Forzar Decodificacion
5-Ver ultimo mensaje...
6-Salir
                                        Codigo actual:Cifrado de Cesar 3 espacios
3
Ingrese su mensaje para descodificar
judfldvcsrucvxcdwhpflrp
```

```
1-Seleccionar Cifrado
2-Cifrar Mensaje
3-Descifrar Mensaje
4-Forzar Decodificacion
5-Ver ultimo mensaje...
6-Salir
                                        Codigo actual:Cifrado de Cesar 3 espacios
3
Ingrese su mensaje para descodificar
judfldvcsrucvxcdwhpflrp
gracias por su atencion
```

```
1-Seleccionar Cifrado
2-Cifrar Mensaje
3-Descifrar Mensaje
4-Forzar Decodificacion
5-Ver ultimo mensaje...
6-Salir
                                        Codigo actual:Cifrado de Cesar 3 espacios
3
Ingrese su mensaje para descodificar
judfldvcsrucvxcdwhpflrp
```

gracias por su atencion