D1

Cifra

Carlos Morales Socorro
cmorsoc@gmail.com
Twitter.com/cmorsoc
Cmorsoc.blogspot.com

D1

Cifra

Parte I: Un poco de Criptografía

Parte II: Diseño de tarea o proyecto

Carlos Morales Socorro

cmorsoc@gmail.com

Twitter.com/cmorsoc

Cmorsoc.blogspot.com

Parte I: Un poco de Criptografía

Algunos elementos a explorar:

- a) Asociación de un número a cada letra

Ejemplo:

Texto a cifrar:
Camina

Código cifrado:
402818310228

Letra	Equivalencia numérica
a	28
b	5
c	40
d	29
e	4
f	30
g	19
h	6
i	31
j	20
k	7
l	21
m	18
n	2
ñ	41

Parte I: Un poco de Criptografía

Algunos elementos a explorar:

- a) Asociación de un número a cada letra

Ejemplo:

Texto a cifrar:
Camina

Código cifrado:
402818310228

Letra	Equivalencia numérica
a	28
b	5
c	40
d	29
e	4
f	30
g	19
h	6
i	31
j	20
k	7
l	21
m	18
n	2
ñ	41

Acciones:

- Cifrar
- Descifrar
- Atacar cifrado - **¡Estadística!**

Parte I: Un poco de Criptografía

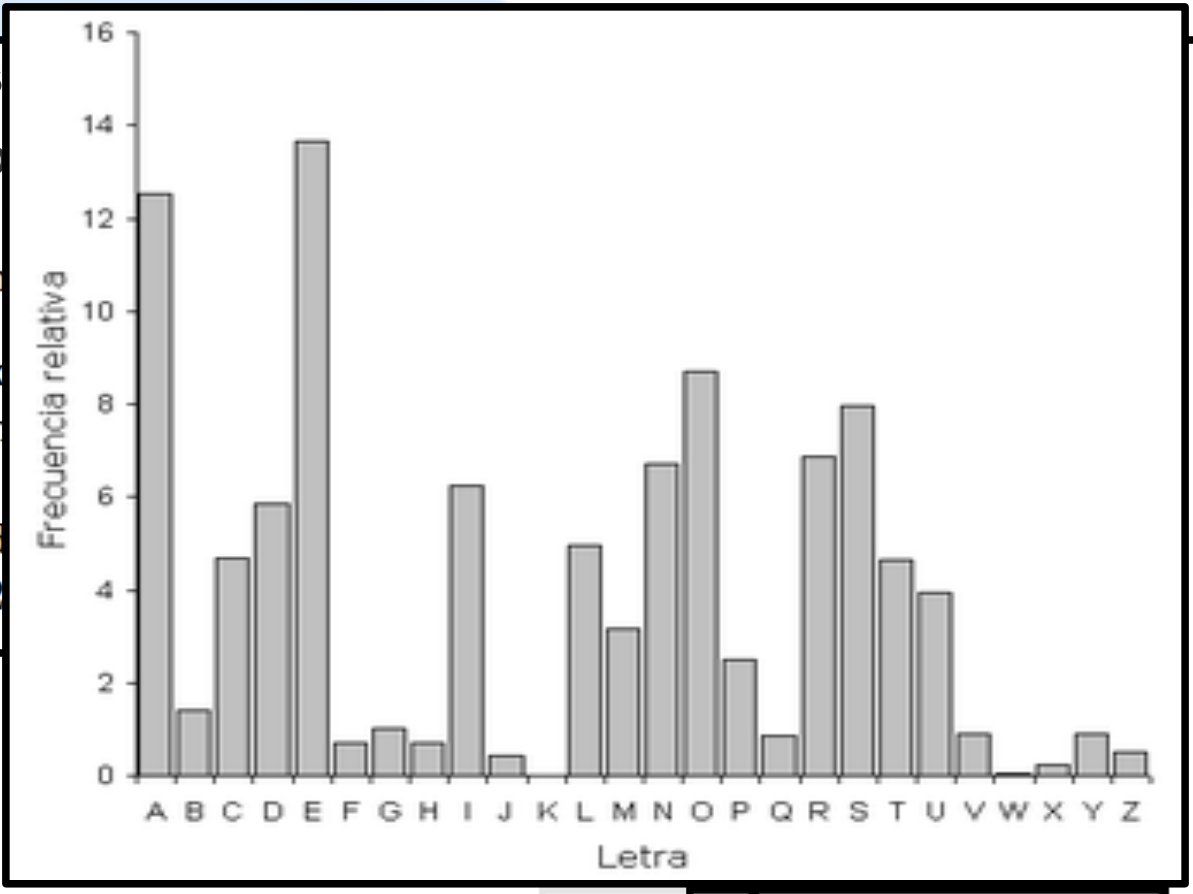
Algunos

- a) Aso

Ejer

Tex
Car

Cód
402



Acciones:

- Cifrar
- Descifrar
- Atacar cifrado

- **¡Estadística!**

41

Flickr CC: http://es.wikipedia.org/wiki/Frecuencia_de_aparici%C3%B3n_de_letras

Parte I: Un poco de Criptografía

Algunos elementos a explorar:

- b) Transformaciones polinómicas:

Ejemplo:

Texto a cifrar:
Camina

Equivalente numérico:
402818310228

$P(x) = 2x+1$

$P(40)=2\cdot40+1=81$

Código cifrado:
815737630557

Letra	Equivalencia numérica
a	28
b	5
c	40
d	29
e	4
f	30
g	19
h	6
i	31
j	20
k	7
l	21
m	18
n	2
ñ	41

Parte I: Un poco de Criptografía

Acciones:

- Cifrar
- Descifrar

Algunos elementos a explorar:

- b) Transformaciones polinómicas:

Ejemplo:

Texto a cifrar:
Camina

Equivalente numérico:
402818310228

P(x) = 2x+1

P(40)=2·40+1=81

Código cifrado:
815737630557

$P(x)=2x+1$

$x=\frac{P-1}{2}$

Letra	
a	
b	
c	
d	
e	
f	
g	19
h	6
i	31
j	20
k	7
l	21
m	18
n	2
ñ	41

Parte I: Un poco de Criptografía

Algunos elementos a explorar:

- b) Transformaci

Acciones:

- Ataque (no solo Estadística):
- Texto de 6 letras x 2 dígitos por letra
- Texto de 4 letras x 3 dígitos por letra
- Texto de … ¡A pensar!

Ejemplo:

Texto a cifrar:
Camina

Equivalente num
402818310228

P(x) = 2x+1

P(40)=2·40+1=81

Código cifrado:
815737630557

j	20
k	7
l	21
m	18
n	2
ñ	41

Parte I: Un poco de Criptografía

Algunos elementos a explorar

- b) Transformaci

Ejemplo:

Texto a cifrar:
Camina

Equivalente num
402818310228

P(x) = 2x+1

P(40)=2·40+1=81

Código cifrado:
815737630557

¿Y si usamos transformaciones más complejas?

$P(x) = 3x^2+1$

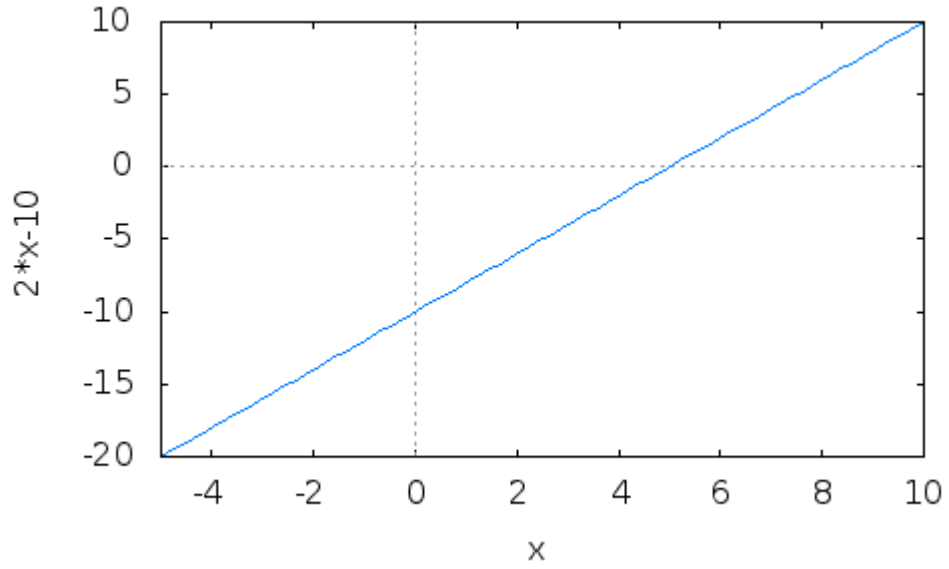
$P(x,i) = ix^2+i$ Yeah!

j	20
k	7
l	21
m	18
n	2
ñ	41

Parte I: Un poco de Criptografía

Algunos elementos a explorar:

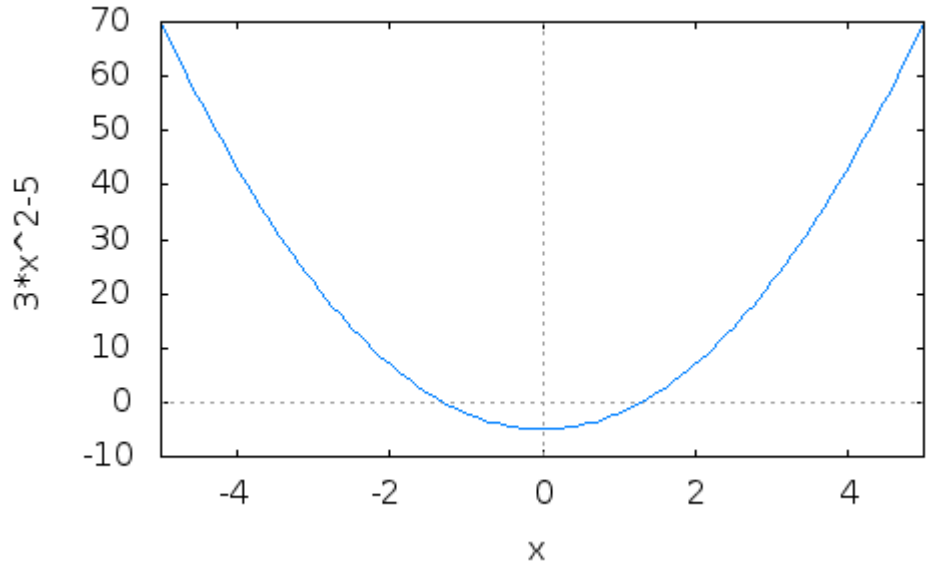
- c) Análisis teórico de las posibles funciones de transformación



Parte I: Un poco de Criptografía

Algunos elementos a explorar:

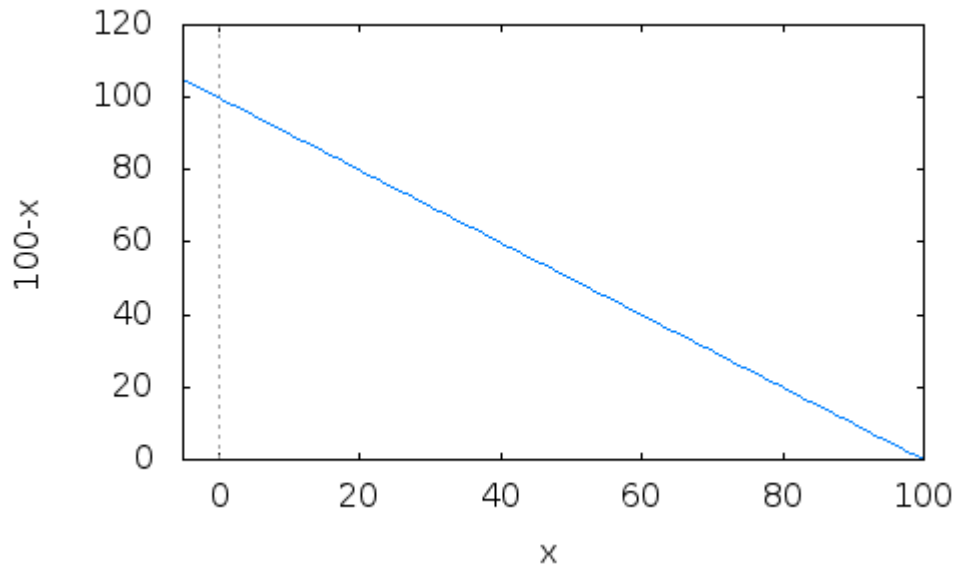
- c) Análisis teórico de las posibles funciones de transformación



Parte I: Un poco de Criptografía

Algunos elementos a explorar:

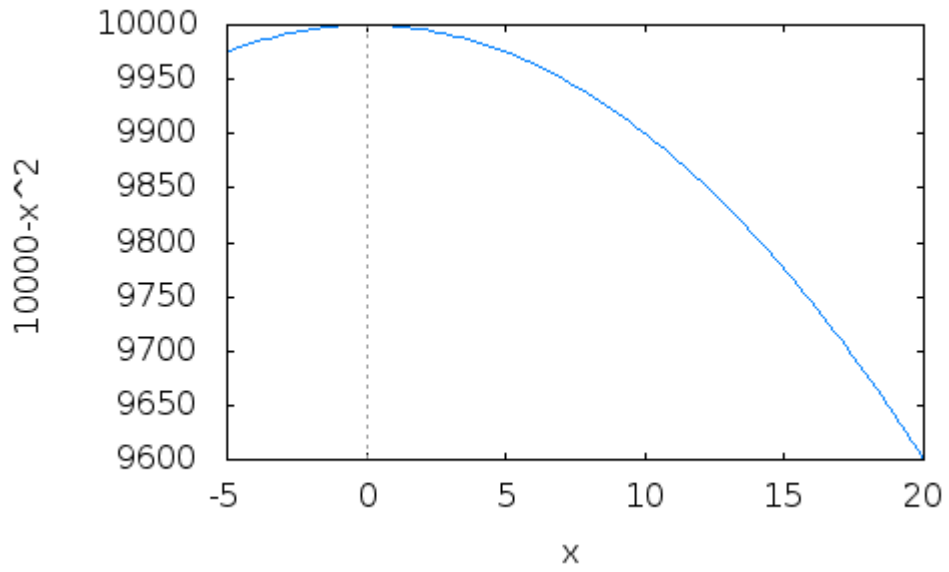
- c) Análisis teórico de las posibles funciones de transformación



Parte I: Un poco de Criptografía

Algunos elementos a explorar:

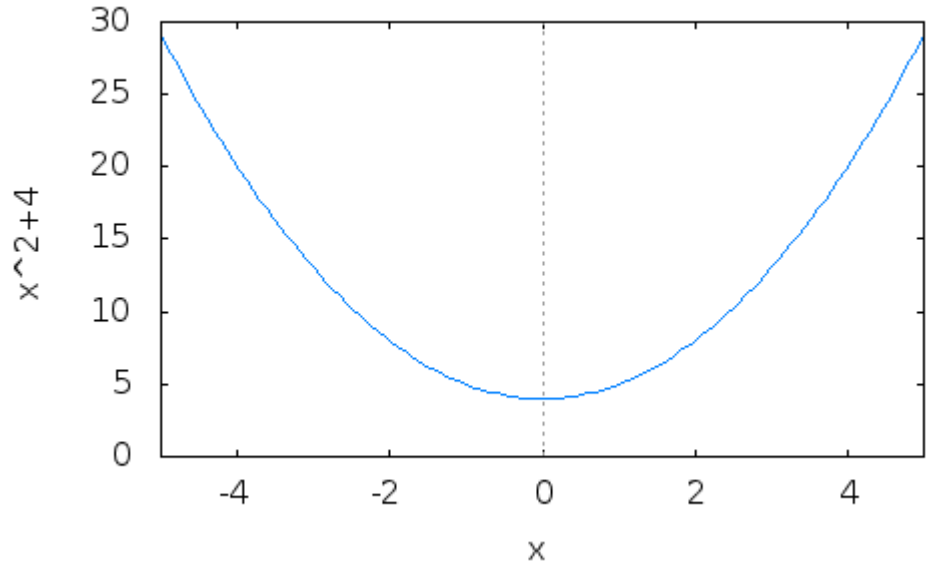
- c) Análisis teórico de las posibles funciones de transformación



Parte I: Un poco de Criptografía

Algunos elementos a explorar:

- c) Análisis teórico de las posibles funciones de transformación



Parte I: Un poco de Criptografía

Algunos elementos a explorar:

- d) Operaciones con polinomios: ¡Toma ya!

Llaves de nivel 1: $P_1(x)=10-4x^2$ y $P_2(x)=3x^2-3$

Llave de nivel 2: $P_3(x)=P_1(x)+2P_2(x)$

Para cifrar:

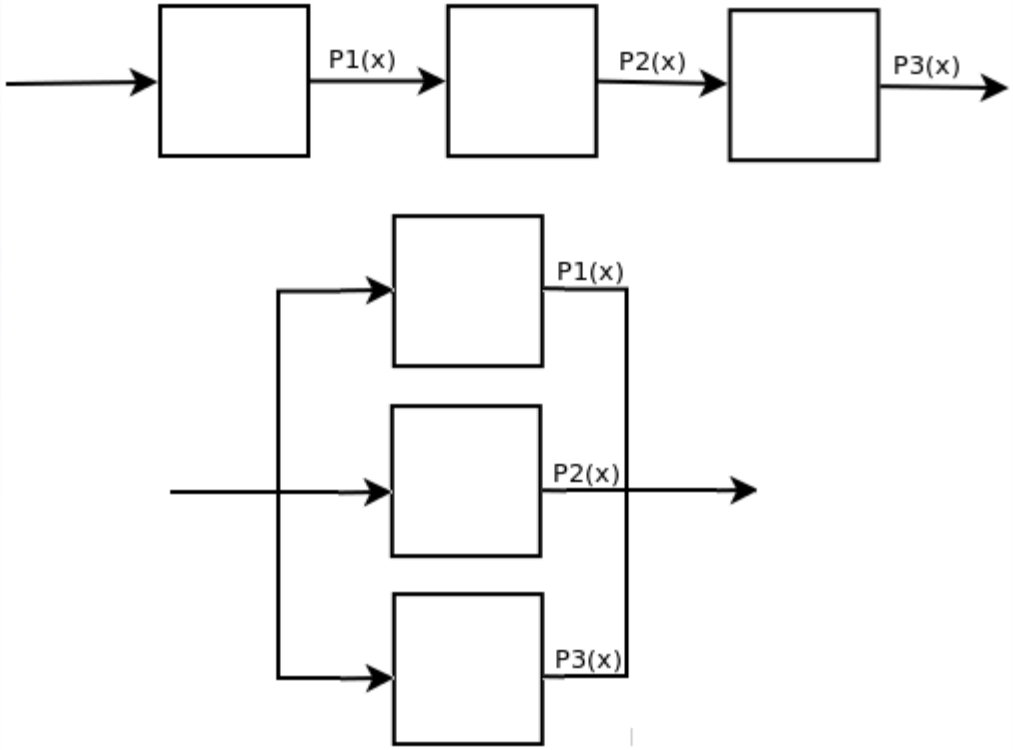
$$P_3(x)=P_1(x)+2P_2(x)=10-4x^2+2(3x^2-3)=10-4x^2+6x^2-6=4+2x^2$$

Para descifrar: $x=\sqrt{\frac{P_3-4}{2}}$

Parte I: Un poco de Criptografía

Algunos elementos a explorar:

- d) Operaciones con polinomios: ¡Toma ya!



Parte II: Diseño de tarea o proyecto

¡Cuando RoboTIX conoció a CIFRA!

D16

Parte II: Diseño de tarea o proyecto

Paso 1: Llegamos al aula y lanzamos la "bomba". El alumnado, organizado en equipos de 3 ó 4 personas, escuchará el mensaje modificado con Audacity:

"Hola, como ya te han comunicado, han robado la lista NOC de nuestra sede central. La identidad de todos nuestros agentes de campo está en peligro... Deberás contactar con nuestro enlace de emergencia. Al final de este mensaje te daré sus datos de contacto cifrados por el método cíclico i4. El tiempo es nuestro enemigo. El enlace te dará más instrucciones. Fin de transmisión."

¡Cuando RoboTIX conoció a CIFRA!

Parte II: Diseño de tarea o proyecto

Paso 1: Llegamos al aula y lanzamos la "bomba". El alumnado, organizado en equipos de 3 ó 4 personas, escuchará el mensaje modificado con Audacity:

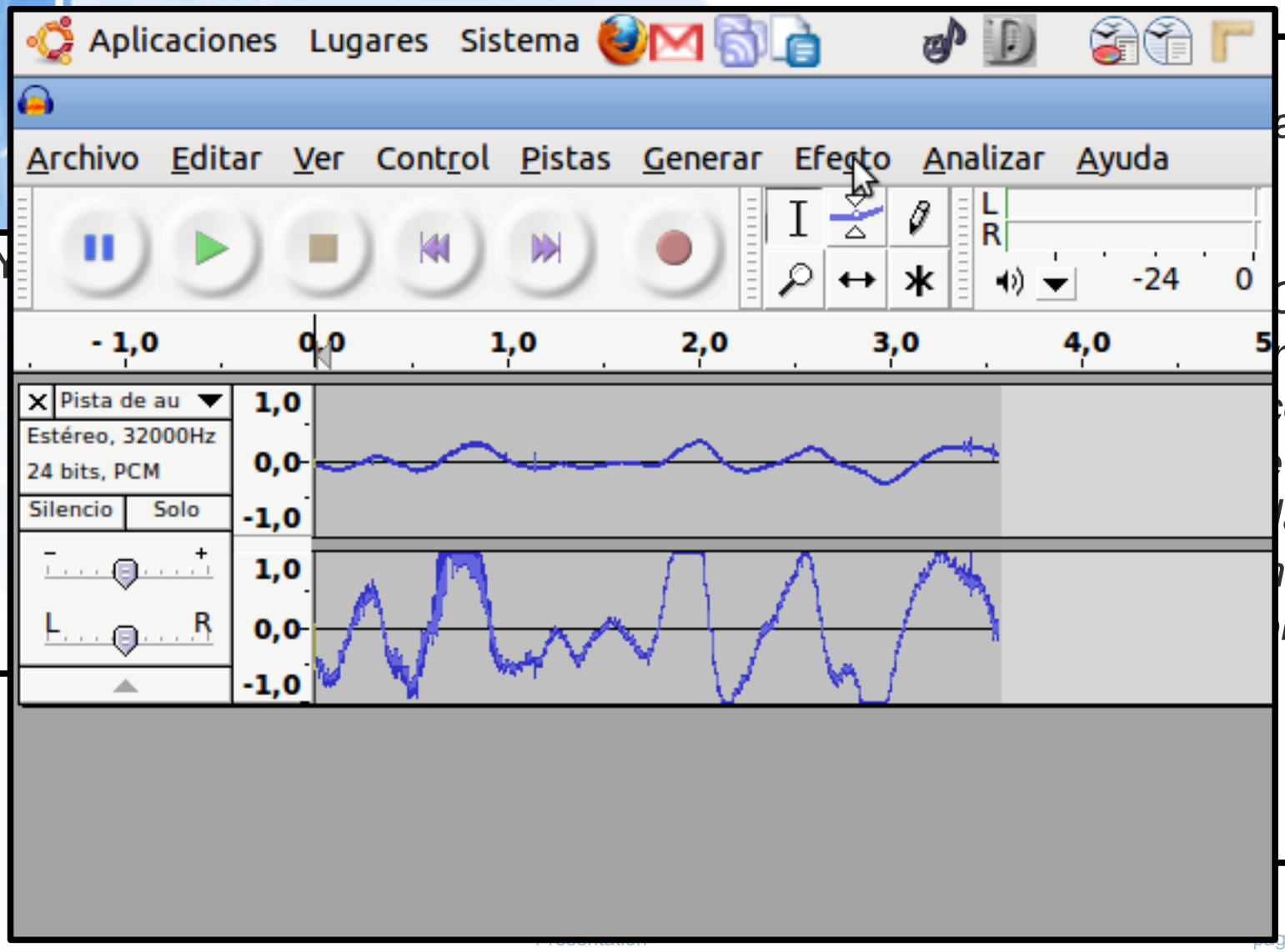
¿Y cómo modifico el audio?

http://audacity.sourceforge.net/?lang=es

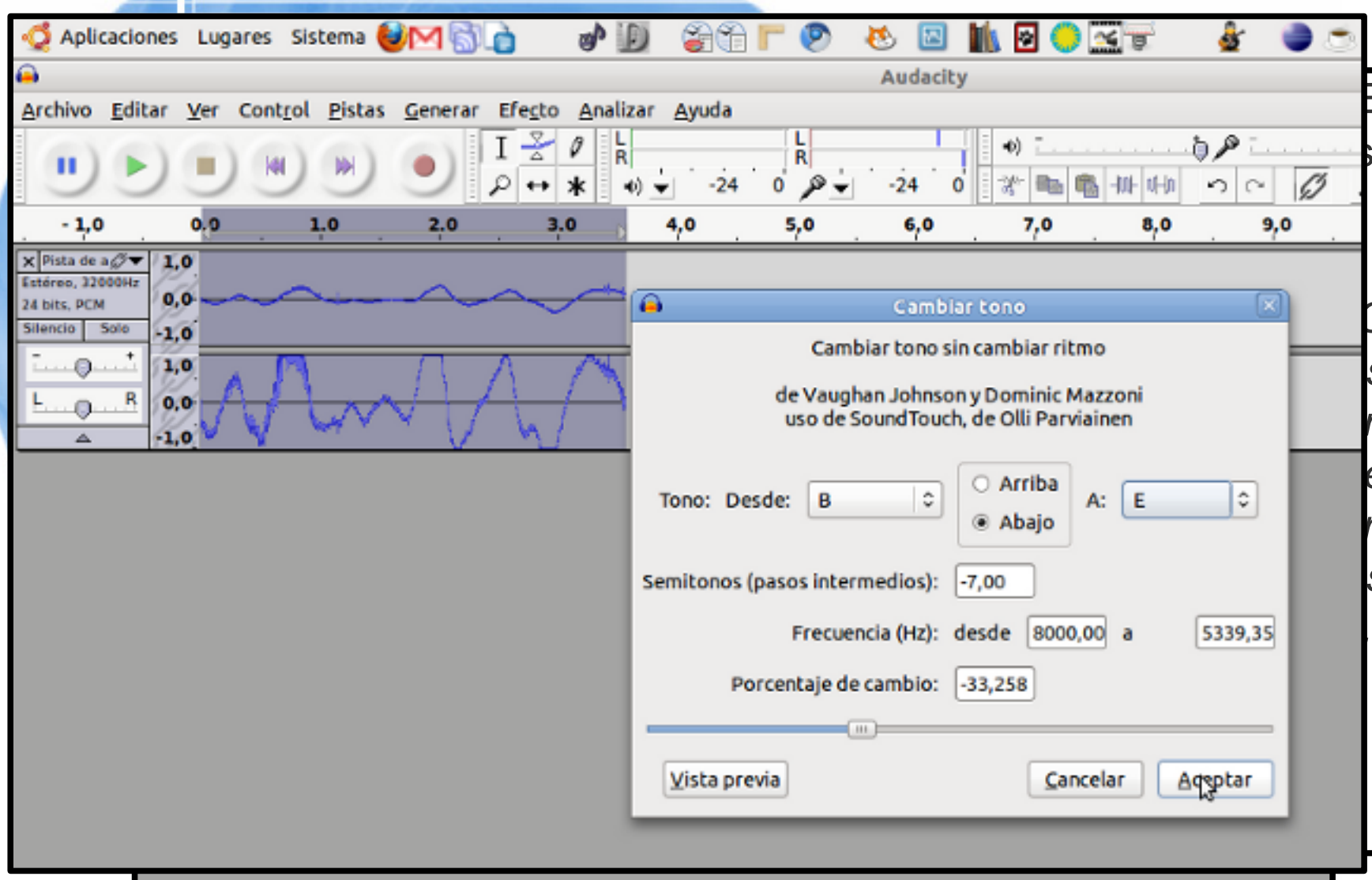
"Hola, como ya te han comunicado, han robado la lista NOC de nuestra sede central [illegible] nuestros agentes de campo está en [illegible] contactar con nuestro enlace de emerge[illegible] mensaje te daré sus datos de contacto cifrados por el método estándar. El tiempo es nuestro enemigo. El enlace te dará más instrucciones. Fin de transmisión."

¡Cuando RoboTIX conoció a CIFRA!

Parte II: Diseño de tarea o proyecto



Parte II: Diseño de tarea o proyecto



D20

Parte II: Diseño de tarea o proyecto

Paso 2: Tras descifrar los datos del enlace, deberán contactar con el mismo para obtener las siguientes instrucciones... ¡Hay muchas posibilidades!

¡Cuando RoboTIX conoció a CIFRA!

Parte II: Diseño de tarea o proyecto

Paso 3: El enlace... La misión está en su mensaje... ¡Vuelve a aparecer Audacity!

Flickr CC: http://www.flickr.com/photos/55046645@N00/314989744

Parte II: Diseño de tarea o proyecto

Hay que actuar rápido. Sabemos quién tiene la lista NOC, es más, sabemos dónde está, pero hay que intervenir con cautela. Te adjunto los planos de la casa del agente Cobf. Parece que la lista está en la zona marcada por los 4 puntos amarillos. Recuerda que tenemos orden de actuar de forma silenciosa... RoboTIX ya está en la zona y además está equipado con un brazo ultraligero inteligente. Los sistemas de transmisión de señales de vídeo están bloqueados dentro del edificio, por lo que, lamentablemente, deberás programar tú mismo el movimiento del robot desde la puerta hasta el lugar señalado. Crea al menos dos rutas de penetración para que el sistema de navegación del robot pueda conmutar de ruta si detecta obstáculos. No te preocupes por la entrada... La abriremos pirateando el sistema de control domótico. Déjalo de nuestra parte. En cuanto tengas el programa, envíalo por correo a la dirección de RoboTIX. No olvides cifrarlo por el método Crab12...

Parte II: Diseño de tarea o proyecto

Una vez recuperada la lista NOC, deberás descifrarla por el método cíclico i4 y contactar con cada uno de los agentes. Debes llevarles a un lugar seguro. Posteriormente, emite un mensaje de confirmación a la sede central con el sistema de llaves de nivel 2 estándar, y continúa el procedimiento normal de acciones de campo entregando a tu supervisor un informe detallado de la operación. Suerte. Fin de transmisión.

Flickr CC: http://www.flickr.com/photos/30397825@N00/2224172287

Parte II: Diseño de tarea o proyecto

Ejemplo:

Nombre del enlace: Pedro Marrero

Método de cifrado: cíclico i4

$$P(x,i) = ix^2+i$$

P: P(8,1)=1·8^2+1= 0065

E: P(4,2)=2·4^2+2= 0034

D: P(29,3)=3·29^2+3= 2526

R: P(27,4)=4·27^2+4= 2920

O: P(39,1)=1·39^2+1= 1522

: P(32,2)=2·32^2+2= 2050 ...

Mensaje: 00650034252629201522205009753140073014600051292015 22

Parte II: Diseño de tarea o proyecto

Ejemplo:

Nombre del enlace: Pedro Marrero

Método de cifrado: cíclico i4

P: P(80,1)=1·80^2+1= 6401

E: P(69,2)=2·69^2+2= 9524

D: P(29,3)=3·29^2+3= 2526

R: P(27,4)=4·27^2+4= 2920

O: P(39,1)=1·39^2+1= 1522

: P(32,2)=2·32^2+2= 2050 ...

Mensaje: 006500342526292015222050097531400730146000 5129201522

Método de cifrado: cíclico doble inverso ij5

$P(x,i,j) = ix^2+j$

Parte II: Diseño de tarea o proyecto

Ejemplo: Plano

Imagen cedida para fines educativos por :http://floorplanner.com/

Parte II: Diseño de tarea o proyecto

Ejemplo: Mensaje a RoboTIX **¡Mejor con una macro!**

Programa: Move(10,-10)

Método de cifrado: Crab12, $P(x) = x^2+12$

M: P(18)=18^2+12= 0336

O: P(39)=39^2+12= 1533

V: P(37)=37^2+12= 1381

E: P(4)=4^2+12= 0028

(: P(11)=11^2+12= 0133

1: P(16)=16^2+12= 0268 ...

Mensaje: 033615331381002801330268063717760496026806370208

Parte II: Diseño de tarea o proyecto

Ejemplo: Descifrando la lista NOC

¡El alumnado debe atacar en paralelo!

Lista cifrada con método cíclico i4:

078508840078006807302594456641000325304421903140102528903075000807851460235541000730016428860040

(Lista original: Alberto Mora y Sara Ruiz)

Descifrando:

$$P(x,i)=ix^2+i \rightarrow x(p,i)=\sqrt{\frac{p-i}{i}}$$

$$x(0785,1)=\sqrt{\frac{785-1}{1}}=28$$ ¡Ya tenemos la "A"!

$$x(0884,2)=\sqrt{\frac{884-2}{2}}=21$$ ¡Ya tenemos la "L"!

Parte II: Diseño de tarea o proyecto

Ejemplo: Confirmando el éxito de la misión

Método de cifrado: Llave de nivel 2 estándar

Llaves de nivel 1: $P_1(x)=10-4x^2$ y $P_2(x)=3x^2-3$

Llave de nivel 2: $P_3(x)=P_1(x)+2P_2(x)$

Para cifrar:

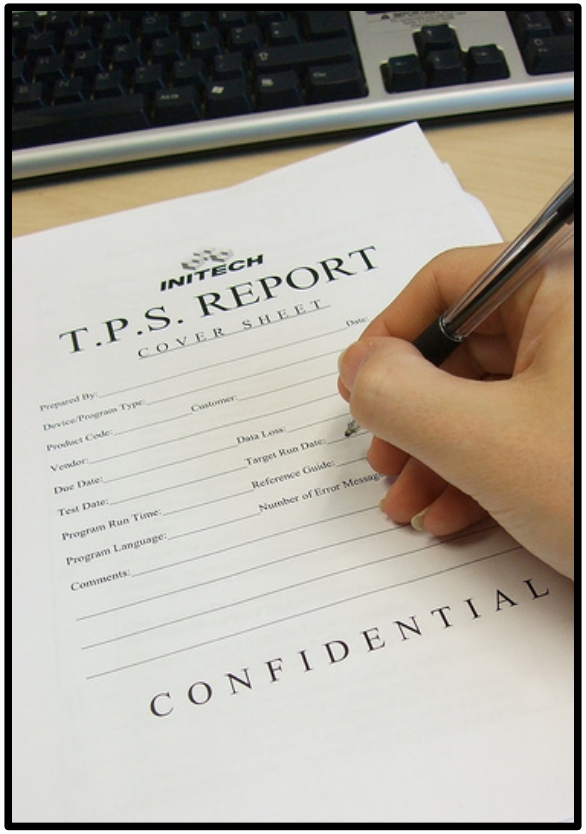
$$P_3(x)=P_1(x)+2P_2(x)=10-4x^2+2(3x^2-3)=10-4x^2+6x^2-6=4+2x^2$$

Para descifrar: $x=\sqrt{\frac{P_3-4}{2}}$

Mensaje: Exito total

Parte II: Diseño de tarea o proyecto

Paso 4: El informe detallado de la operación



Parte II: Diseño de tarea o proyecto

Y no nos olvidemos de la Ficha de Seguimiento Curricular de la Unidad/Tarea/Proyecto...

I.E.S. ---------- Departamento de Matemáticas

Ficha de Seguimiento Curricular de la Unidad

Matemáticas E.S.O. Prof.: ------ ------- -------

Proyecto ----------

¿Qué estoy aplicando? ¿Qué estoy aprendiendo?

	Aspectos trabajados
Aritmética	
Álgebra	
Análisis (Funciones)	

Parte II: Diseño de tarea o proyecto

Y no nos olvidemos de la Ficha de Seguimiento Curricular de la Unidad/Tarea/Proyecto...

¿Cómo lo llevo al aula?

- Planificar
- Identificar
- Aprender
- Aplicar
- Reflexionar

I.E.S. ----------

Departamento de Matemáticas

Ficha de Seguimiento Curricular de la Unidad

Matemáticas E.S.O. Prof.: ------ ------- ----

Proyecto ----

¿Qué estoy aplicando? ¿Qué estoy aprendiendo?

Aritmética	
Álgebra	
Análisis (Funciones)	

CIFRA+RoboTIX

¿Y ahora?

¡Ahora te toca a ti!

cmorsoc.blogspot.com