Trabajo Terminal 2015-A010

Aplicación de cifrado contra adversarios clasificadores, para el correo electrónico

Presenta:

Jonathan Arcos Ayala

Allan Ulises Zepeda Ibarra

Dirige:

Sandra Díaz Santiago

Manuel Alejandro Soto Ramos

2 de junio de 2016

Contenido

1. Introducción
   - Información
   - Datos relevantes
   - Tipos de Adversarios
2. Problemática
   - Adversario Clasificador
   - Esquema de Díaz-Chakraborty (Envío)
   - Esquema de Díaz-Chakraborty (Recepción)
3. Propuesta de solución
   - Objetivos
   - Arquitectura propuesta
   - Tecnologías
4. Trabajo terminal I
   - Prototipos
5. Trabajo terminal II
   - Complemento para el cliente de correo Thunderbird
   - Complemento para el cliente de correo Nylas-N1

Introducción

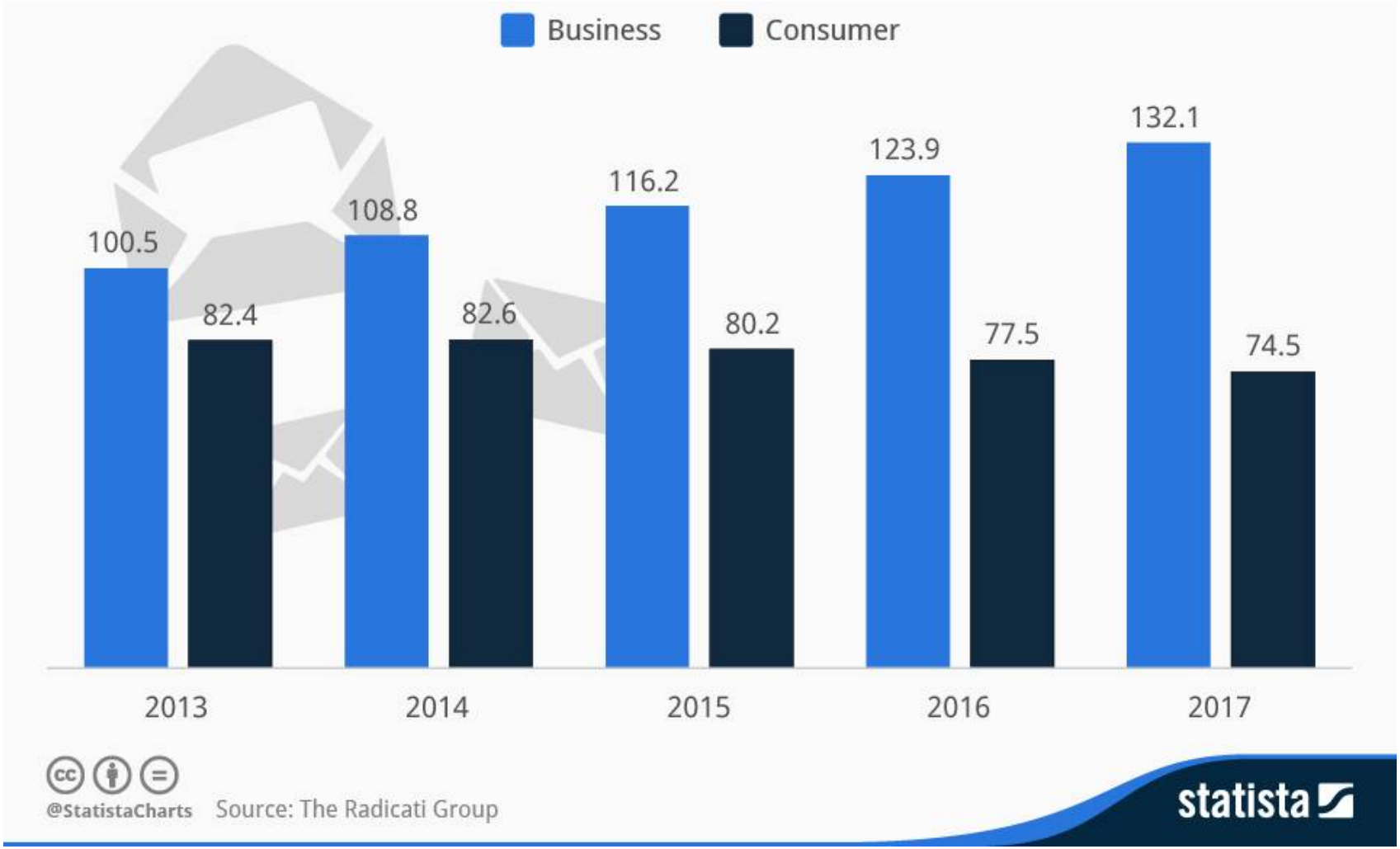


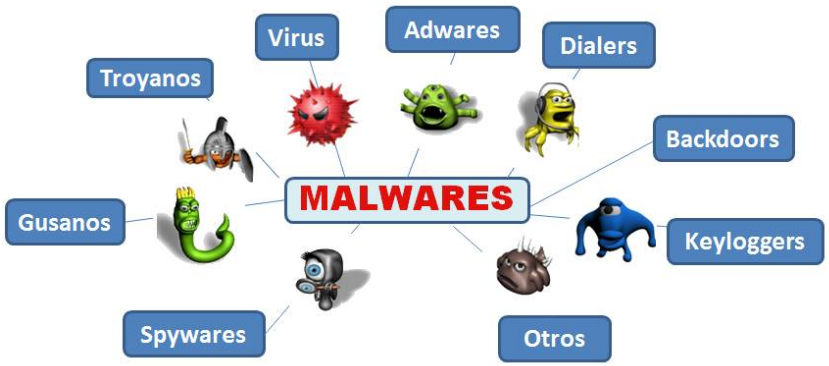
Figura: Estimación de mensajes enviados y recibidos en un día en todo el mundo (en billones)

Datos relevantes.

Datos relevantes

- 3.9 billones de cuentas de correo electrónico
- 3 mil millones de usuario en internet aproximadamente
- 1.55 mil millones de usuarios en facebook aproximadamente

Tipos de Adversarios.



Software

Personas o grupos de personas

Adversario Clasificador.

Adversarios

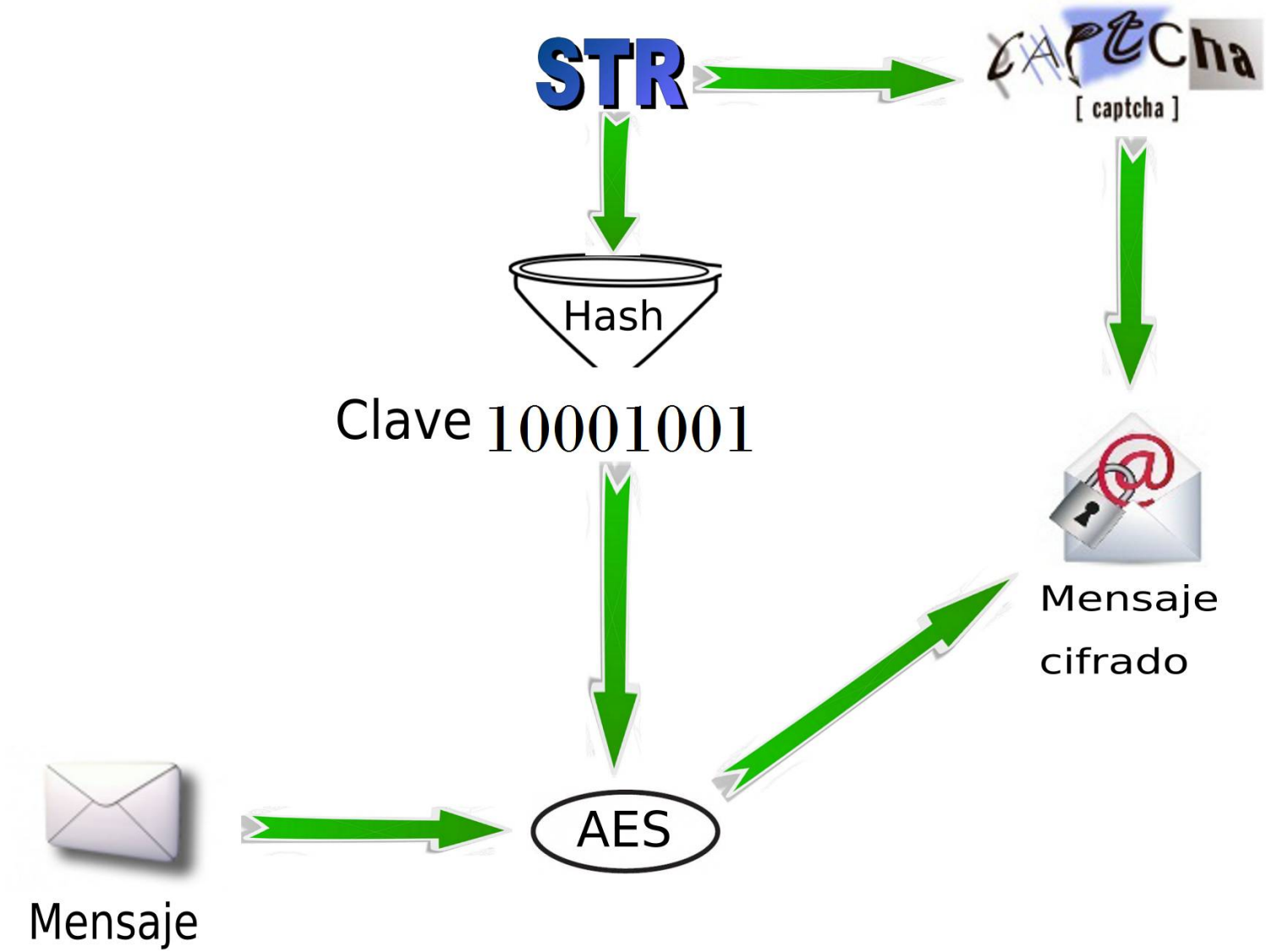
Clasificadores

On July 11,2014 Lang Lang performed together with Placido Domingo, Ana Maria Martinez, Maestro Eugene Kohn, the Orchestra Sinfonica Brasileira, Paula Fernandez and other musicians for World Cup Concert at HSBC Arena in Rio de

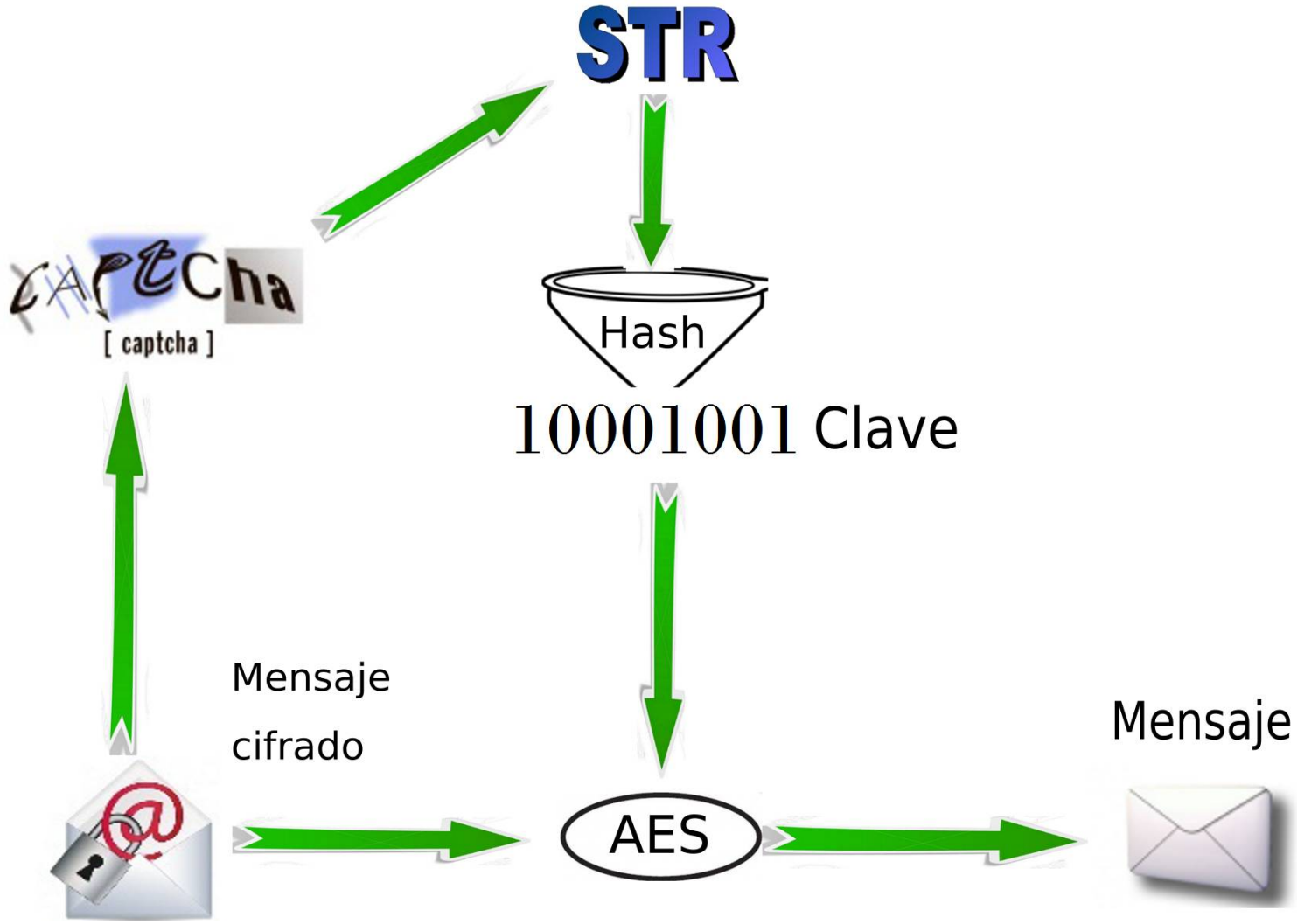
No

Si

Esquema de Díaz-Chakraborty



Esquema de Díaz-Chakraborty

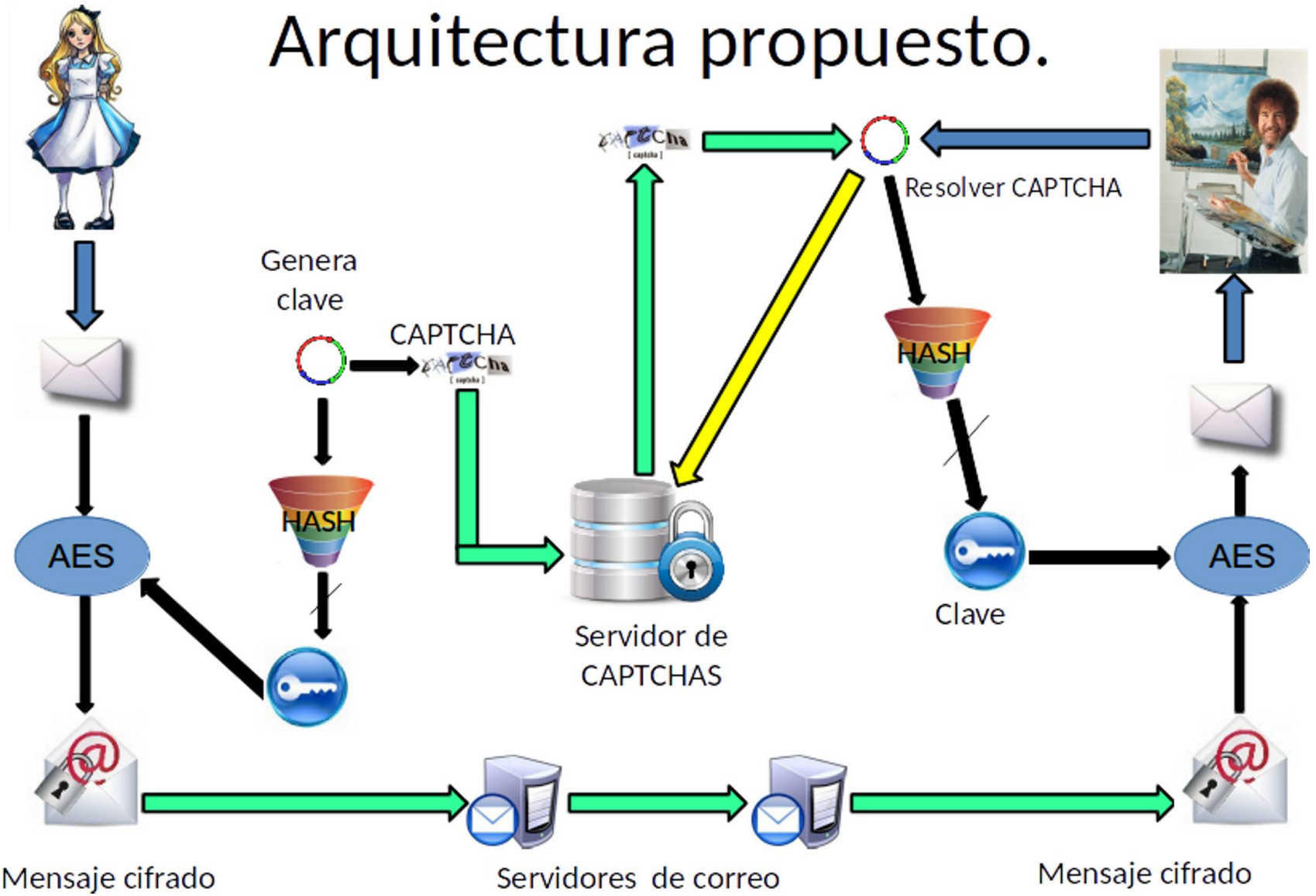


Objetivos

Objetivos

1. Desarrollar una herramienta en un cliente de correo electrónico para el envío y recepción de los correos cifrados y la generación, envío y recepción de CAPTCHAS.
2. Desarrollar un servidor de llaves que reciba, aloje y envíe los CAPTCHAS a los usuarios para descifrar los correos electrónicos.
3. Desarrollar un algoritmo de cifrado y descifrado basado en el envío y recepción de CAPTCHAS.

Arquitectura propuesto.



Tecnologías

Trabajo desarrollado en TT I

Prototipos

1. Prototipo de generación de CAPTCHAS en C++.
2. Prototipo de generación de CAPTCHAS en PYTHON.
3. Instalación de un cliente de correo electrónico web y un servidor DNS.
4. Prototipo de generación de CAPTCHAS a partir de un mensaje de correo electrónico recuperado del cliente de correo web.

Complemento para el cliente de correo Thunderbird

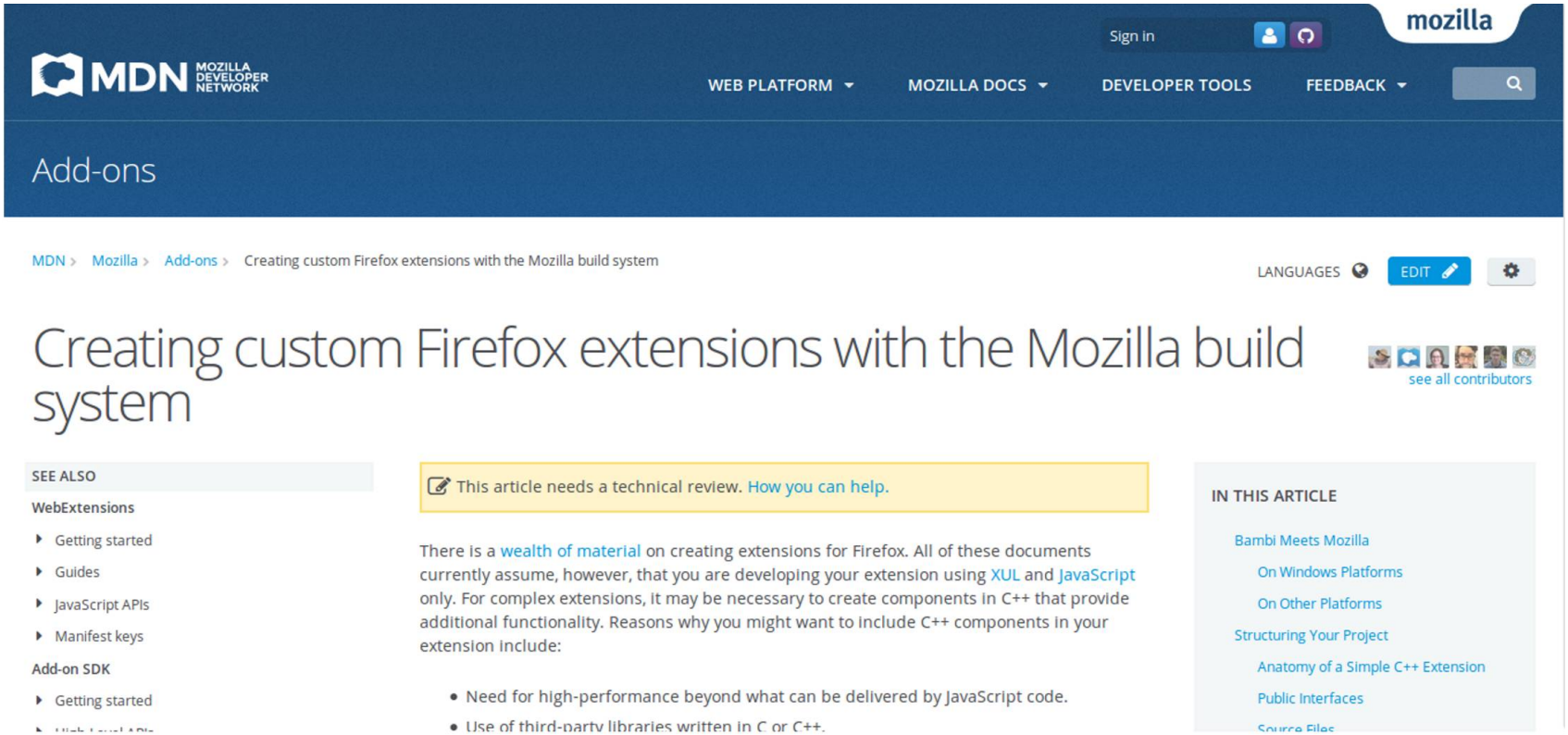


Figura: Página web de Mozilla Developer Network.

Complemento para el cliente de correo Nylas-N1

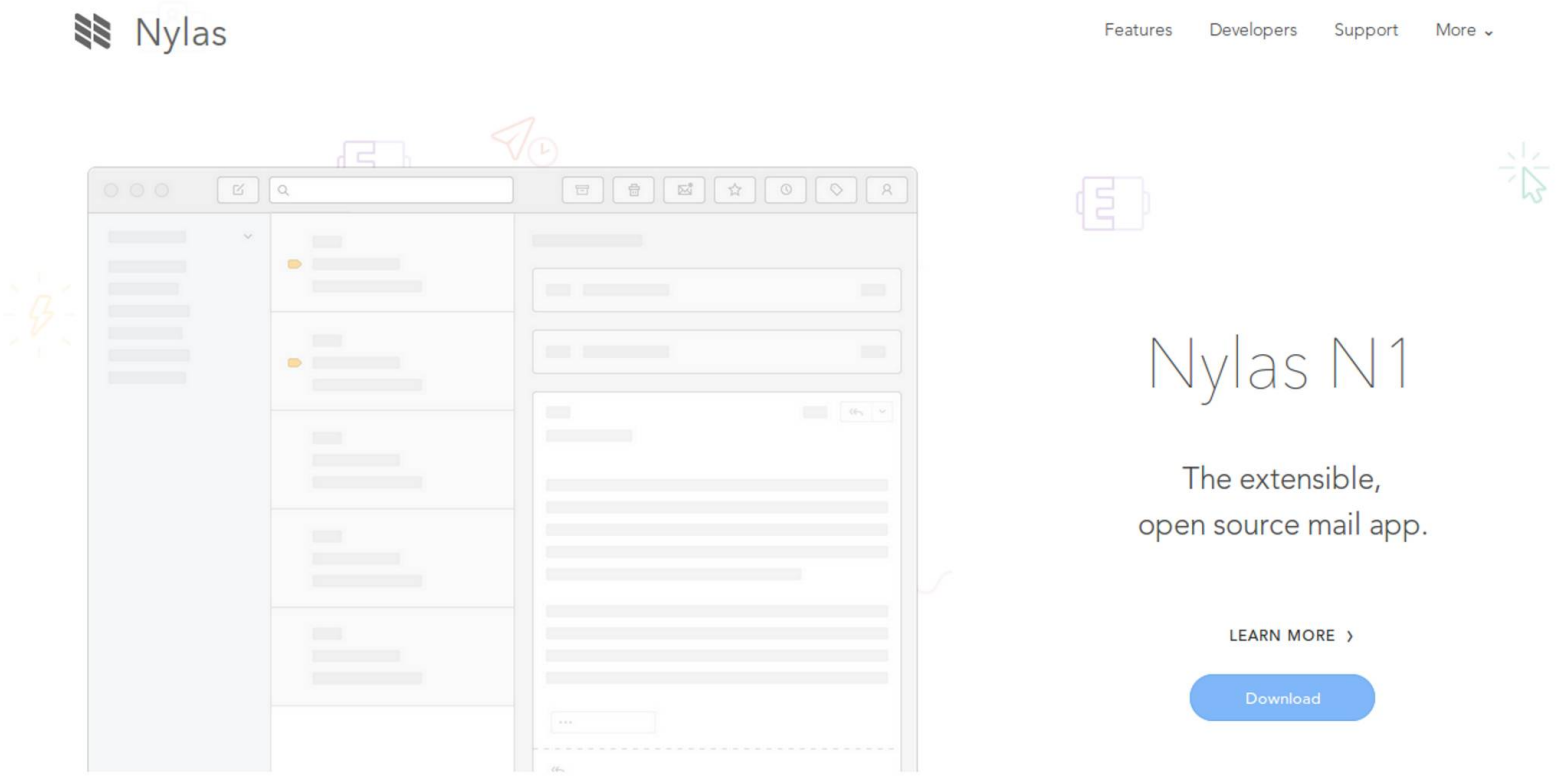


Figura: Página web de Nylas N1.

Implementación de un cliente propio

Conclusiones

Conclusiones

1. El esquema Díaz - Chakraborty es posible implementarse en los esquemas actuales de comunicación por correo electrónico.
2. El ataque de los agentes clasificadores es en los servidores de correo y no en las comunicaciones.

Trabajo Futuro

Conclusiones

1. Complemento para un otro tipo de clientes de correo electrónico.
2. Esquema de intercambio de claves.
3. Implementar un cifrado semántico.
4. Biblioteca de creación de CAPCHAS en el lenguaje PYTHON.

Sección de preguntas

División de la clave protocolo P'

Conjunto Z_p

$AL = \{A, B, ..., Z\} \cup \{a, b, ..., z\} \cup \{0, 1, ..., 9\} \cup \{+, /\}$

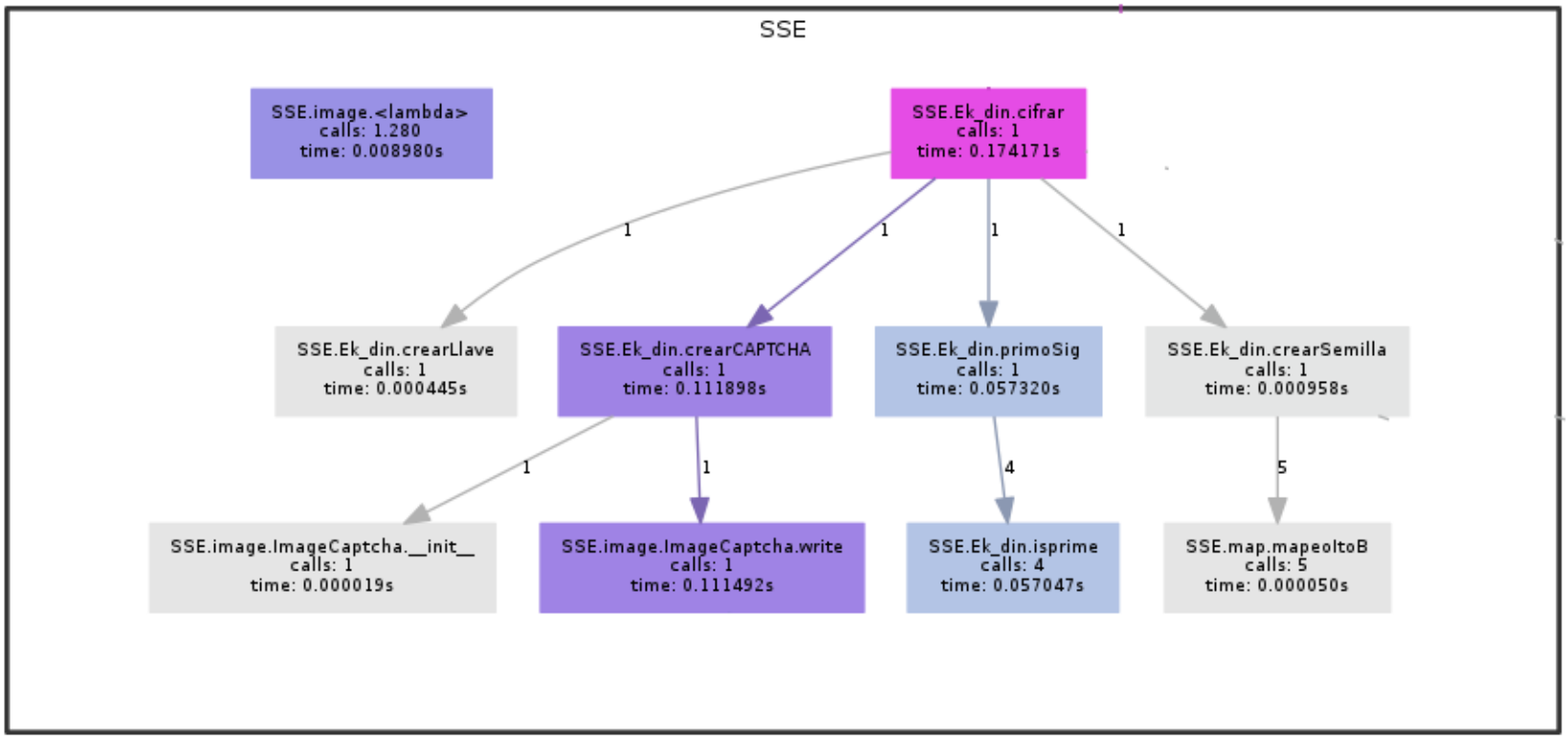
Codificación

- $STR = `ABC`$
- $\alpha = \{0, 1, 2\}$
- $bin_6(0) = 000000$
  $bin_6(1) = 000001$
  $bin_6(2) = 000010$
- $\Psi = 00000000000001000010$
- $v = toInt(\Psi) = 66$

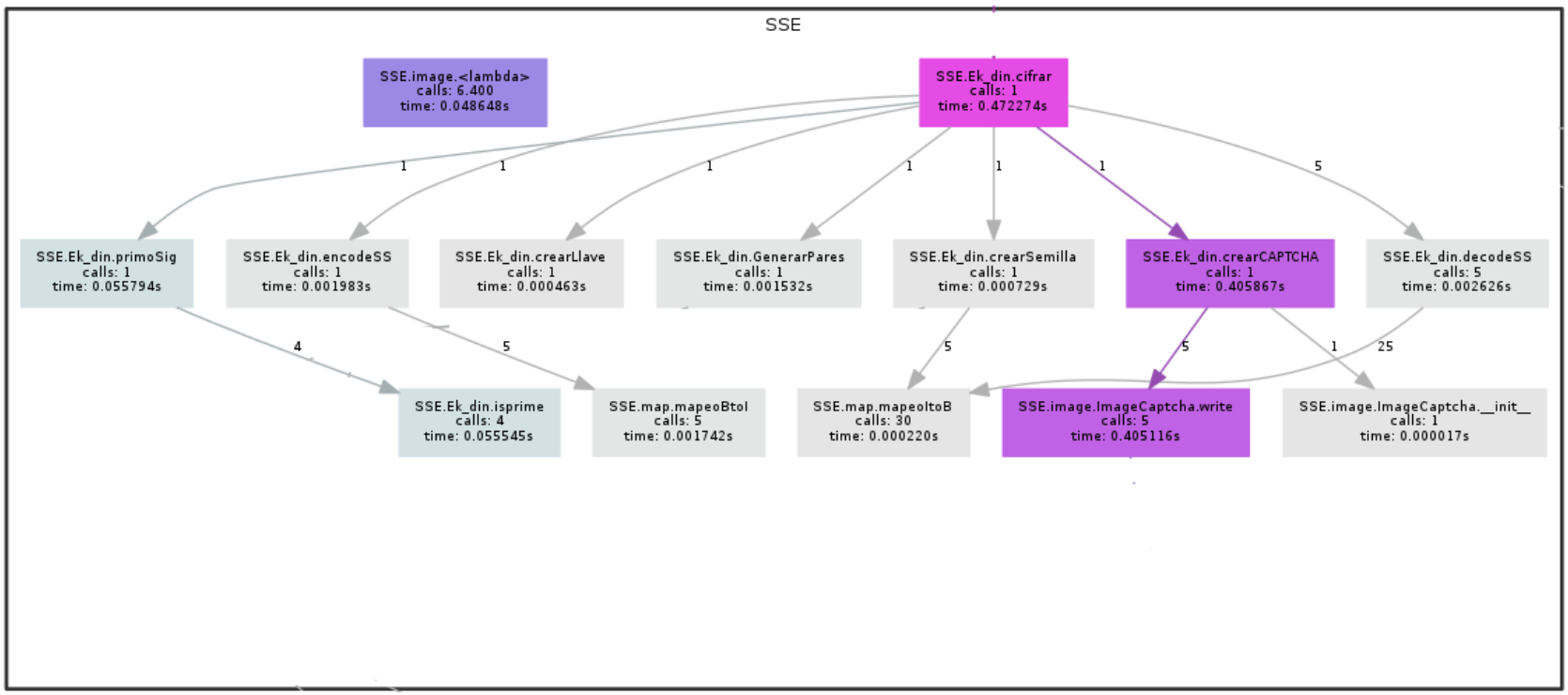
Decodificación

- $v = 66$
- $z = 00000000000001000010$
- $z_0 = 000000$
  $z_1 = 000001$
  $z_2 = 000010$
- $toInt(z_0) = 0, toInt(z_1) = 1, toInt(z_2) = 2$
- $s = `ABC`$

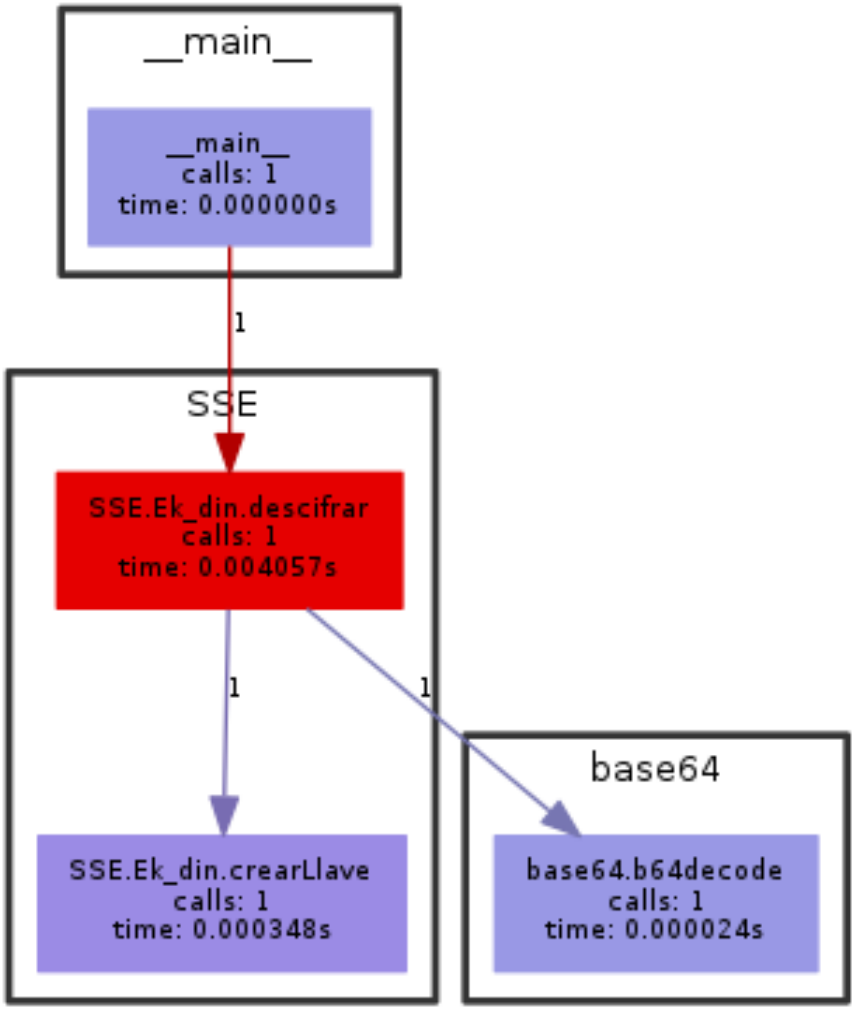
Prueba de cifrado unicaptchas



Prueba de cifrado multicaptchas



Prueba de descarga de CAPTCHAS



Generated by Python Call Graph v1.0.1
http://pycallgraph.slowchop.com

Prueba de descarga de multi-CAPTCHAS

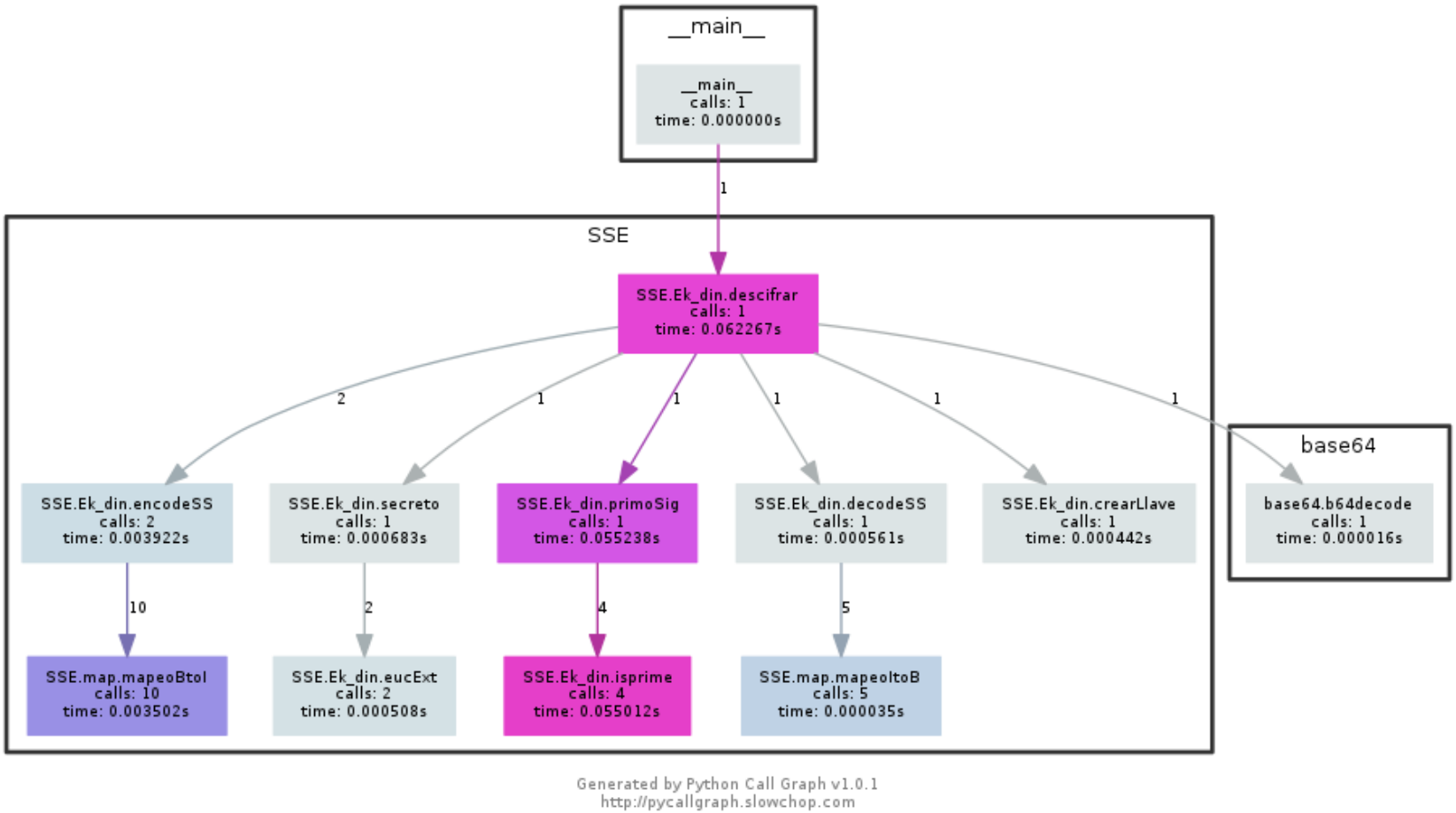


Tabla de resultados.

Tabla de Resultados	
PFSA:	126 Puntos función
PFA:	112.14 Puntos función
Lineas de Código:	2242.8 Lineas de código
Esfuerzo:	1121.4 horas/persona
Esfuerzo por Persona:	560.7 horas por persona
Duración del proyecto:	5.607 Meses
Costos de Operación:	$77,000.00
Costo total del proyecto:	$257,000.00

Tabla de costos de operación

	Mensual	Proyecto
Luz,Telefono, Internet	$2,500.00	$15,000.00
Renta de Oficinas	$5,000.00	$30,000.00
Renta de Servidores	$2,000.00	$12,000.00
	Subtotal:	$57,000.00
	Por equipo	Proyecto
Equipo de cómputo	$10,000.00	$20,000.00
Costos de Operación Total:		$77,000.00

Tabla de puntos función

		Atributos	Peso	Total
Entradas	Alta	1	6	6
	Media	3	4	12
	Baja	6	3	18
			Subtotal:	36
Salidas	Alta	2	7	14
	Media	2	5	10
	Baja	1	4	4
			Subtotal:	28
Consultas	Alta	0	6	0
	Media	0	4	0
	Baja	4	3	12
			Subtotal:	12
Ficheros Lógicos	Alta	2	15	30
	Media	2	10	20
	Baja	0	7	0
			Subtotal:	50
Ficheros Externos	Alta	0	10	0
	Media	0	7	0
	Baja	0	5	0
			Subtotal:	0
	Total de puntos función sin ajustar:			126

Tabla de 14 preguntas

Preguntas	Valor
1. Comunicación de Datos	3
2. Función Distribuida	4
3. Rendimiento	4
4. Configuración utilizada masivamente	2
5. Tasas de Transacción	1
6. Entrada On-Line de datos	1
7. Diseño para la eficiencia de usuario final	2
8. Actualización On-Line	0
9. Complejidad del procesamiento	3
10. Utilizable en otras aplicaciones	0
11. Facilidad de Instalación	1
12. Facilidad de Operación	0
13. Puestos Múltiples	0
14. Facilidad de Cambio	3
Total:	24