INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE CÓMPUTO

SUBDIRECCIÓN ACADÉMICA

No de TT: 2015 – A010 Junio 2016

Documento Técnico

"Aplicación de cifrado contra de adversarios clasificadores, para el correo electronico."

Presentan

Jonathan Arcos Ayala[1]

Allan Ulises Zepeda Ibarra[2]

Directores

Dr. Sandra Díaz Santiago **M. en C. Manuel Alejandro Soto Ramos**

RESUMEN

En este reporte técnico se explica el desarrollo de una herramienta de cifrado que protegerá al correo electrónico, contra un tipo especial de adversario, denominado adversario clasificador. El objetivo de este adversario es analizar una gran cantidad de información, para clasificar al usuario en categorías predeterminadas. La herramienta que se propone utiliza de manera novedosa los CAPTCHAs y una técnica criptográfica conocida como secreto compartido, para facilitar el acuerdo de las claves de cifrado. Adicionalmente, la aplicación utilizará un servidor de llaves para la autenticación de los usuarios para proveer una forma segura de enviar mensajes cifrados y recuperarlos.

Palabras clave: Criptografía, Correo electrónico, Secreto compartido, CAPTCHAs.

[1]jonas.arcos.99@gmail.com [2]balaju01@gmail.com