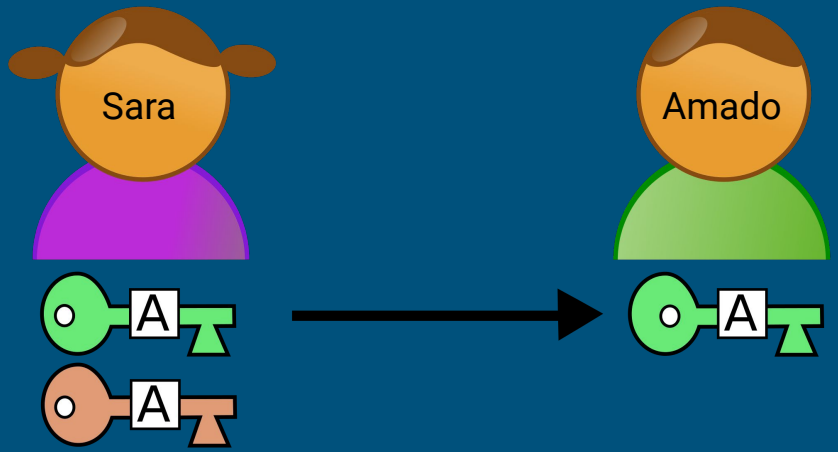
Laboratorio: Public Key Encryption Parte 2

ElGamal

Sara Nohemi Zavala (carné No. 18893)
Ricardo Antonio Valenzuela (carné No. 18762)
Jose Amado Garcia (carné No. 181469)
Juan Fernando De Leon Quezada (carné No. 17822)
Edgar Andreé Toledo Torres (carné No. 18439)

¿Qué es?

El procedimiento de cifrado/descifrado ElGamal se refiere a un esquema de cifrado basado en el problema matemático del logaritmo discreto. Fue descrito por Taher Elgamal en 19841 y se usa en software GNU Privacy Guard, versiones recientes de PGP, y otros sistemas criptográficos. Este algoritmo no está bajo ninguna patente lo que lo hace de uso libre. La seguridad del algoritmo se basa en la suposición que la función utilizada es de un solo sentido debido a la dificultad de calcular un logaritmo discreto. El procedimiento de cifrado y descifrado está basado en cálculos sobre un grupo cíclico cualquiera G, lo que lleva a que la seguridad del mismo dependa de la dificultad de calcular logaritmos discretos en G.



¿Cómo se relaciona con Diffie-Hellman?

Es un algoritmo de criptografía asimétrica basado en la idea de Diffie-Hellman y que funciona de una forma parecida a este algoritmo discreto. El algoritmo de ElGamal puede ser utilizado tanto para generar firmas digitales como para cifrar o descifrar.

¿Cuáles son los beneficios de su correcto uso?

Hasta el momento el algoritmo ElGamal de cifrado/descifrado puede ser considerado un algoritmo efectivo.

Un adversario con la habilidad de calcular logaritmos discretos podría ser capaz de romper un cifrado ElGamal. Sin embargo, en la actualidad, el algoritmo de computación de logaritmos discretos cuando trabajamos módulo un primo es subexponencial con una complejidad de $\lambda = 1/3$, la misma que la de factorizar dos números primos, y por tanto, no es accesible de realizar tal tarea en números grandes en un tiempo razonable. El logaritmo discreto es aún más difícil si trabajamos en otros grupos como por ejemplo, curvas elípticas.

¿Existen aplicaciones actualmente? ¿Cuáles?

Secure Shell: Es un protocolo de red con el que podemos acceder a una computadora remota, e incluso ejecutar aplicaciones en ella. Permite una comunicación segura sobre un canal inseguro. (Willems, 2009).

Secure Socket Layer: Es un protocolo de cifrado utilizado en todas las conexiones https que hay en la Web. Fue desarrollado por Netscape para la transmisión de datos por Internet en 1994. La versión más utilizada de SSL es la 3.0.

Prety Goog Privacy: Es un software de uso privado para cifrar mensajes electrónicos. Fue desarrollado por Phil Zimmermann, Desde 2002 utiliza el procedimiento de ElGamal 1985.

Una de las aplicaciones más comunes que podemos encontrar en el día a día es el uso de Firma Electrónica.

Referencias:

AES99] J. Deamen and V. Rijmen, AES Proposal: Rijndael, version 2, AES submission, 1999.

[BERN05] D. Bernstein, Cache-timing attacks on AES, 2005.

[BJN] D. Boneh, A. Joux and P.Q. Nguyen, Why textbook ElGamal and RSA encryption are insecure, Proceedings of Asiacrypt'00, Lecture Notes in Computer Science, no. 1976 (2000), Springer, pp. 30-43.

[BM04] S. Blanch and R. Moreno, Implementaci´on GnuPG con curvas el´ıpticas, Avances en Criptolog´ıa y Seguridad de la Informaci´on. Proceedings RECSI VIII, 2004, pp. 515–526.

[BMTFC] S. Blanch and R. Moreno, GnuPG Implementation with Elliptic Curves, Trabajo final de carrera, Marzo 2004.

[BRUM03] D. Brumley and D. Boneh, Remote timing attacks are practical, 2003.

[DHAES] M. Abdalla, M. Bellare and P. Rogeway, DHAES: An encryption scheme, based on the Diffie-Hellman Problem, 1999.