1 Horst Feistel

Horst Feistel es un famoso criptográfo alemán. Él trabajó en el diseño de encriptadores en IBM, iniciando la investigación que culminó en el desarrollo del *Data Encryption Standard (DES)* en 1970. Nacido en Berlin, Alemania, él emigró a Estados Unidos en 1934 obteniendo su licenciatura en el *Massachusetts Institute of Technology* y su maestría en *Harvard*, ambas en física. Fue de los primeros investigadores no gubernamentales en estudiar el diseño de los cifrados por bloque.

Una de sus principales aportaciones fue la creación del método en el que basan la construcción de cifradores por bloque, este método lleva su nombre *Redes Feistel*. En 1960, el encargado de IBM asignó a Feistel a la creación de un método de encriptación llamado Lucifer, además de la creación de DES.

Lucifer fue desarrollado para proteger los datos de un sistema dispensador de dinero que IBM había desarrollado para *Lloyds Bank* en el Reino Unido. Este proyecto más adelante fue comercializado. Se podría decir que Lucifer fue el precursor de DES, puesto que al intentar establecer Lucifer como el estándar en criptografía y ser rechazado varias veces, este fue modificado de una llave de 112 bits a 56 bits, los detalles del algoritmo fueron publicados y tras dos años de evaluación este se convirtió en el *Data Encryption Standard (DES).*

Algoritmos de Cifrado basados en Red Feistel

- Blowfish
- Camellia
- RC5
- 3DES
- ICE
- KASUMI
- MARS
- MAGENTA

2 Victor Saul Miller

Victor S. Miller es un matemático americano, estudió su licenciatura en la Universidad de Columbia en 1968 y su doctorado en mmatemáticas en Harvard en 1975. Suus principales áreas de interés son Teoría Númerica Computacional, Combinatronics, Compresión de Datos y Criptografía. Él es uno de los creadores de la criptografía de curva elíptica. También es co-creador del algoritmo LZW para la compresión de datos. Recibió la medaalla IEEE Millenium por ese

algoritmo. Además, creo un algoritmo que lleva su nombre, este algoritmo es fundamental para la *pairing-based cryptography* y del algoritmo Lagarias-Miller-Odlyzko para contar primos debajo de un número x.

La criptografía elíptica es un enfoque a la criptografía de llave pública basada en la estructura algebráica de las curvas elípticas sobre campos finitos. Esta requiere de llaves más pequeñas en comparación de criptografía basada en campos de Galois para proveer una seguridad equivalente. Esta se basa en el problema de el logaritmo discreto de la curva elíptica, este depende de la habilidad de computar un producto punto y la incapacidad de computar los multiplicando del producto punto original. El tamaño de la curva elíptica define la dificultad del problema.

3 Alexandra Boldyreva

Es una profesora asociada en la Escuela de Ciencias Computacionales en el Colegio de Computo en el Instituto de Tecnología de Georgia. Recibió su doctorado en Ciencias Computacionales en la Universidad de California en San Diego y licenciatura en Matemáticas Aplicadas en St. Petersburg State Techhnical University, Russia. Alexandra tiene a cargo distintas investigacioones en el área de la criptografía y seguridad de la información. Participa activamente publicando árticulos de criptografía, entre sus principales artículos están: *On Symmetric Encryption with Distinguishable Decryption Failures, Security of Symmetric Encryption in the Presence of Ciphertext Fragmentation, How to Strengthen the Security of RSA-OAEP.*