Criptografía

Profesor: Melvin Fernández Ch.

Video 8

fidélitas

Virtual

fidélitas Virtual

Criptografía simétrica y asimétrica

Módulo: 3

Cifrado simétrico de bloque

- El cifrado de bloque procesa la entrada de texto claro en bloques de tamaño fijo y produce un bloque de texto cifrado de igual tamaño para cada bloque de entrada.

- Los algoritmos de cifrado simétrico de bloque más importantes son:
  - Data Encryption Standard (DES).
  - Triple DES (3DES).
  - Advanced Encryption Standard (AES).

Data Encryption Estándar (DES)

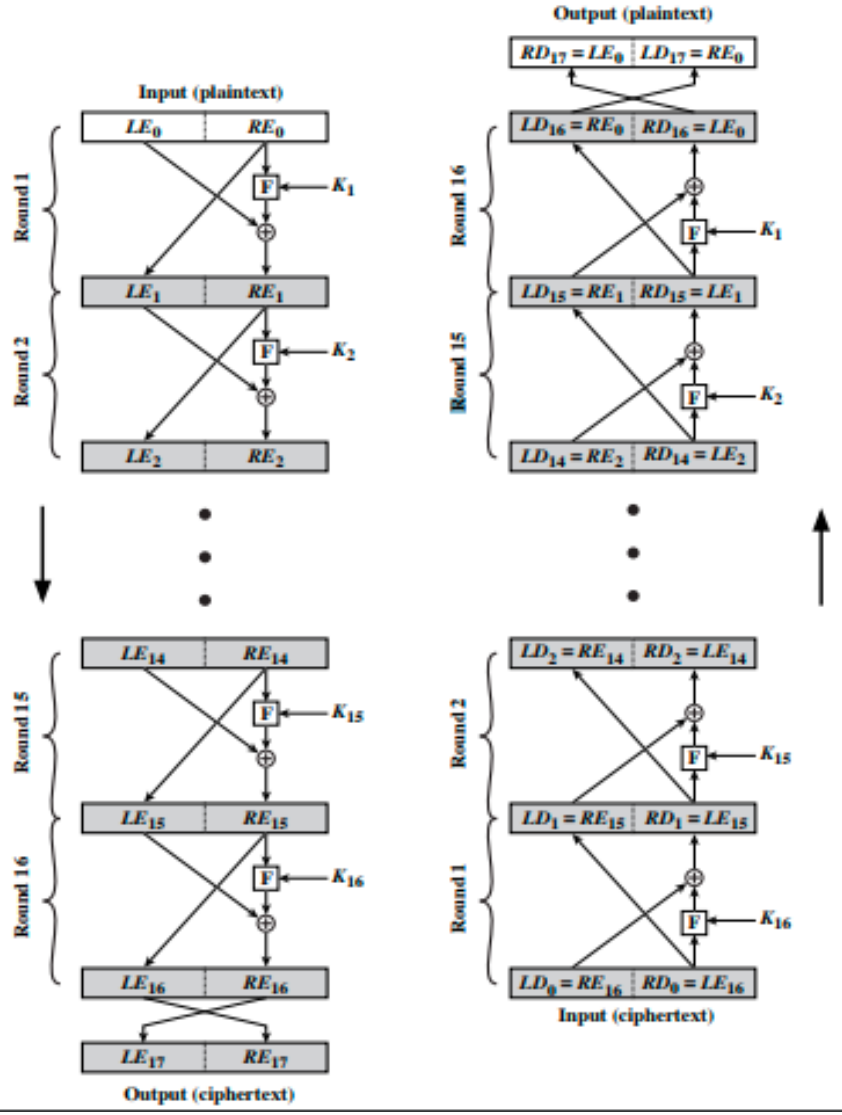
- Propuesto en 1977 por el NIST .
- Fue el esquema de cifrado más ampliamente usado en esa época.
- El algoritmo en sí se denomina Data Encryption Algorithm (DEA).
- Fue retirado en mayo de 2005.

- Descripción del algoritmo:
  - Tamaño de bloque de 64 bits.
  - Clave de 56 bits.
  - Red de Feistel con pequeñas variaciones.
  - 16 rondas de procesamiento.
  - El proceso de descifrado es esencialmente el mismo que el de cifrado.

Data Encryption Estándar (DES)

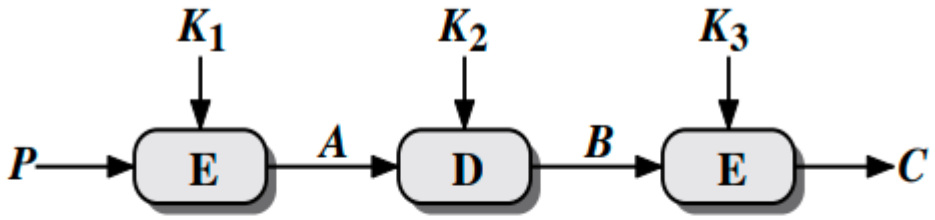
fidélitas Virtual

Red de Feistel (16 rondas)

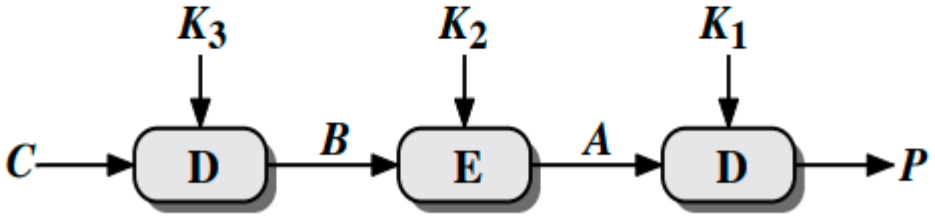


Triple DES (3DES)

- Propuesto por primera vez en 1985.
- El tamaño efectivo de la clave es de 168 bits.
- Si las llaves son todas iguales, el algoritmo sería igual al DES.



(a) Encryption



(b) Decryption

Advanced Encryption Estándar (AES)

fidélitas Virtual

- En 1997, el NIST lanzó una convocatoria para AES:
  - Debía tener una seguridad igual o mayor que 3DES y mejorar significativamente la eficiencia.
  - Debía usar cifrado simétrico de bloque, con un tamaño de bloque de 128 bits, y soportar claves de 128, 192 y 256 bits.
  - Los criterios de evaluación incluían seguridad, eficiencia, requisitos de memoria, idoneidad hardware y software.

- Finalmente, NIST seleccionó el algoritmo Rijndael:
  - Se publicó en 2001.
  - Los autores son los criptógrafos belgas Dr. Daemen y Dr. Rijmen.

Gracias

fidélitas Virtual