Block Ciphers

Es un cifrado determinístico, utilizando un algoritmo de encriptado y otro de desencriptado. El algoritmo recibe una entrada que es una instancia de cierto número de bits y la salida tiene exactamente el mismo tamaño, pero cifrado, en resumidas cuentas: el input y el output del algoritmo deben ser del mismo tamaño.

El cifrado de bloques no tiene memoria. Un cifrado de bloque se puede tomar como una caja negra que toma un valor y lo encripta o lo desencripta. Este sistema es seguro si la función de encriptado es computacionalmente indistinguible de cualquier otra operación computacional.