The Advanced Encryption Standard (AES) Wikipedia

If you remove redundancy and change key often, it is extremely secure. Even with infinite computing power, you wouldn’t be able to crack it.

Previously, the Data Encryption Standard (DES) was used before the AES. They are block ciphers; encryption occurs using a block size of 128 bits. It is called a symmetric-key algorithm because both encrypting and decrypting uses the same key.

Stream ciphers are too easy to crack. Say you have a AES block of 128 bit and encrypt it with 256 bit key, each bit in the encrypted message has a probability of 1/50 to change.

AES steps

1. Key Expansion (this is kind of like the pseudo random number generator)
2. Add Round Key

Number of rounds depends on the number of key bits.

* 10 cycles of repetition for 128-bit keys
* 12 cycles of repetition for 192-bit keys
* 14 cycles of repetition for 256-bit keys

You can break one cycle of AES, but we can add a cycle number to increase the security of the algorithm.

Each block has 8 bits, so we have a 4x4 blocks. S is a lookup table. S takes each block and converts it into another block B.

Everything except 0 will have a multiplicative inverse in .

To avoid algebraic attacks, the S is constructed by combining the inverse function with an invertible affine transformation (in other words, you mess it up).

One thing to note is that even a highly nonlinear function can be invertible.

1. Shift keys

Block are shifted right and down.

1. Mix columns

Diffusion means change spreads over the whole bits.

AES runs quickly because it uses the arithmetic available in the computer, but DES doesn’t.