AES

Motivation. In his paper titled Communication Theory of Secrecy Systems in 1949, Claude Shannon suggested two principles that would make statistical attacks on cryptosystems hard:

- Confusion

- Diffusion

Substitution-permutation networks (SPN). An SPN is a procedure for transforming a plaintext $x$ and a key $K$ into a ciphertext. It consists of $N + 1$ rounds, and each round $i$ has a round key $K_i$ associated with it that is derived from $K$. At the beginning of round $i$, $1 \leq N$. the “current state” of the ciphertext is $w_{i-1}$. It then gets processed through an S-box and/or a permutation $\pi$. Finally, in the $N + 1$st round, $w_N$ is xor-ed with the round key $K_{N+1}$ one more time and returned as the ciphertext. Here is an algorithmic description of SPN: 1

1From Cryptography: Theory and Practice, 3rd Edition by D. Stinson
Let us now describe a specific SPN. For this example, the plaintext $x$ and ciphertext $y$ will have 16 bits. It will have 5 rounds so $N = 4$. The key $K$ has 32 bits and the 5 round keys will be derived from $K$. The S-box, described below, takes a 4-bit string and substitutes it with another 4-bit string. The strings are written in hexadecimal notation. In each round of the SPN, $u_r$ will be partitioned into blocks for 4-bits each and sent through the same S-box to produce $v_r$.

$$
\begin{array}{cccccccccccccccc}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & a & b & c & d & e & f \\
e & 4 & d & 1 & 2 & f & b & 8 & 3 & a & 6 & c & 5 & 9 & 0 & 7 \\
\end{array}
$$

The permutation $\pi$, described below, reorders the 16-bit string $v_r$ to produce $w_r$.

$$
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\
1 & 5 & 9 & 13 & 2 & 6 & 10 & 14 & 3 & 7 & 11 & 15 & 4 & 8 & 12 & 16
\end{pmatrix}
$$

Finally, suppose the 32-bit key is

$$K = 0011\ 1010\ 1001\ 0100\ 1101\ 0110\ 0011\ 1111$$

resulting in the following round keys:

$$
\begin{align*}
K_1 &= 0011\ 1010\ 1001\ 0100 \\
K_2 &= 1010\ 1001\ 0100\ 1101 \\
K_3 &= 1001\ 0100\ 1101\ 0110 \\
K_4 &= 0100\ 1101\ 0110\ 0011 \\
K_5 &= 1101\ 0110\ 0011\ 1111.
\end{align*}
$$

Then the encryption of $x = 0010\ 0110\ 1011\ 0111$ proceeds as follows:

$$
\begin{align*}
w_0 &= 0010\ 0110\ 1011\ 0111 \\
K_1 &= 0011\ 1010\ 1001\ 0100 \\
u_1 &= 0001\ 1100\ 0010\ 0011 \\
v_1 &= 0100\ 0101\ 1101\ 0001 \\
w_1 &= 0010\ 1110\ 0000\ 0111 \\
& \vdots \\
y &= 1011\ 1100\ 1101\ 0100
\end{align*}
$$
Confusion and Diffusion:

Advantages:

Security issues:

Variations:
On to AES. In 1997, NIST put out a public call to replace DES. This replacement would be called the *Advanced Encryption Standard* or *AES*. NIST required that AES has a block length of 128 bits, supports key lengths 128, 192 and 256 bits, and be available worldwide on a royalty-free basis. Initially, there were 21 submissions of which 15 met the above criteria. The candidate pool was then narrowed down to five: MARS, RC6, Rijndael, Serpent, Twofish. Finally, in October 2000, NIST chose Rijndael as the Advanced Encryption Standard.

*The openness of the section process.*

*Rijndael’s advantages.*

*Description of AES.*
Each round is *invertible* and consists of the following steps:

- **SubBytes step**
- **ShiftRows step**
- **MixColumns step**
- **AddRoundKey step**
Attacks on AES.

Modes of Operation for Block Ciphers

1. Electronic Codebook Mode (ECB)
2. Cipher-Block Chaining Mode (CBC)

3. Cipher Feedback Mode (CFB)

4. Output Feedback Mode (OFB)

5. Counter Mode (CTR)