AES (Advanced Encryption Standard)

DES - 56 bit key 2^{56} keyspace

late 1990s - DES Challenge - distributed effort

~50ish days + key was found.

Made a Competition for a new Standard

① secure

② fast

③ simple

Winner: Rijndahl

"rain doll"

* 3 Versions: 128 bit version
192 bit version
256 bit version *

Key drawn as a byte array of 16 bytes (8 bits)
2 HEX CHAR

State Matrix

b_1	b_5	b_9	b_{13}
b_2	b_6	b_{10}	b_{14}
b_3	b_7	b_{11}	b_{15}
b_4	b_8	b_{12}	b_{16}

① Add Round Key

② Sub Bytes

③ Shift Rows

④ Mix Columns

Encrypt (10 ROUNDS)

1. Plaintext
2. Add Round Key (round 0 key)
3. RUN 9 FULL ROUNDS
4. RUN LAST ROUND ADJUSTED

REG ROUND

a. Sub bytes
b. Shift rows
c. mix cols
d. Add Round Key

ROUND 10

a. Sub bytes
b. Shift Rows
c. Add Round Key

Sub bytes (S box)

Straight look up table -
for each byte w/ sub it with another byte

Shift Rows

b_{00}	b_{01}	b_{02}	b_{03}
b_{10}	b_{11}	b_{12}	b_{13}
b_{20}	b_{21}	b_{22}	b_{23}
b_{30}	b_{31}	b_{32}	b_{33}

→

b_{00}	b_{01}	b_{02}	b_{03}
b_{11}	b_{12}	b_{13}	b_{10}
b_{22}	b_{23}	b_{20}	b_{21}
b_{33}	b_{30}	b_{31}	b_{32}

Mix Cols

Fixed matrix encryption + decryption
↓
inverse of encryption

fixed!

State

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 47 & B1 & 76 & 98 \\ 3A & C3 & 59 & BB \\ B2 & 72 & EA & D2 \\ F0 & 19 & 03 & E3 \end{bmatrix}$$

Use the same "pattern" as matrix multiplication, but mult and add are done completely differently!

$$R1C1 = 2 \times 47 + 3 \times 3A + 1 \times B2 + 1 \times F0$$
$$\text{w i}$$

All AES computations occur in the field GF_{2^8} with the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$.

$$47 = 01000111 = x^6 + x^2 + x + 1$$
$$x^7\ x^6\ x^5\ x^4\ x^3\ x^2\ x^1\ x^0$$

$$3A = 00111010 = x^5 + x^4 + x^3 + x$$

GF_{2^8} means a poly w/ max degree 7
all coeff $\{0, 1\}$