CIS3362 9/30/24

(1) DES Code
(2) Start AES - field GF_{2^8}. ← transition

In 1997-8, DES challenge. (Distributed)
it took ~ 2 months to brute force key.
New Competition → 15 candidates → 5 after initial review
WINNER: Rijndahl ("Raindoll" pronunciation)
Vincent Rijmen + John Daemen
3 versions: 128 bit
192 bit Version ← Block + keysize!
256 bit

AES is based in Group Theory, in particular
it uses a field within $GF(2^8)$, which I'll explain later. These are polynomials of 1 up to degree x^7 with coefficients either 0 or 1.

Selected because of its combination of
security
speed
ease of implementation

What is $GF(2^8)$?

The 2 means all coefficient are calculated mod 2.

8 means all polynomials are calculate mod an irreducible polynomial of degree 8.

→ AES a fixed polyomial is chosen: $x^8+x^4+x^3+x+1$ (memorize This)...

Irreducible means that the only way to express $x^8+x^4+x^3+x+1$ as a product of 2 polynomials with coefficient mod 2 is $1 \times (x^8+x^4+x^3+x+1)$

MOD w/polynomial? $a(x) \bmod b(x) = r(x)$

means $a(x) = q(x)b(x) + r(x)$, degree $r(x) <$ degree $b(x)$.

Good news

$$(a(x) + b(x)) \bmod c(x)$$
$$= a(x) \bmod c(x) + b(x) \bmod c(x)$$

$$x^8 \bmod (x^8+x^4+x^3+x+1) = x^4+x^3+x+1$$

$$x^8 + x^4+x^3+x+1 \;\Big|\; \overline{1}$$
$$x^8$$
$$-\,x^8+x^4+x^3+x+1$$
$$-x^4+x^3-x-1$$
$$+x^4+x^3+x+1$$

$x^9 \bmod (x^8 + x^4 + x^3 + x + 1)$

$= x - x^8$

$= x(x^4 + x^3 + x + 1)$

$= x^5 + x^4 + x^2 + x$

Multiplication in field

$(x^2 + x + 1)(x^3 + x + 1)$

$= x^5 + x^3 + x^2$

$x^4 + x^2 + x$

$x^3 + x + 1$

$x^5 + x^4 + 2x^3 + 2x^2 + 2x + 1 = \boxed{x^5 + x^4 + 1}$