DTTF/NB479: Dszquphsbqiz Day 15

- Announcements:
  - Ch 3 quiz Friday of week 5. Will include fields (today)
  - Upload electronic homeworks in pdf, preferably
  - Direct HW questions directly to grader, then to me
- Today:
  - Prep. for Rijndael and Discrete Logs: $GF(2^8)$
- Questions, like on DES?
  - I pulled the key into the input file
  - A good time to aim for would be ~10 s for 1M iterations.

DES round keys involve two permutations and a left shift

K =

0	1	1	1	1	1	1	0	0	1	0	0	1	0	0	0
1	1	0	0	0	0	1	0	1	0	0	0	0	0	1	0
0	0	0	1	1	1	0	0	0	0	0	0	1	1	1	0
1	1	1	1	0	1	0	0	1	1	1	0	1	0	0	0

Grab 56 permuted bits:[**57**, **49**, **41**, **33** …]

Get **1100**…

In round 1, LS(1), so: **100** …**1** *Careful!

Then grab 48 permuted bits:

[14, 17, 11, 24, 1, 5, 3, …]

Get … **1** **0** …

T&W, p. 127

Rijndael is the 128-bit, Advanced Encryption Standard (AES)

- 128-bit blocks
- Encrypted using functions of the 128-bit key for 10 rounds
  - Versions exist for keys with 192 bits (12 rounds), 256 bits (14 rounds)
- The S-boxes, round keys, and MixColumn functions require the use of GF(2^8), so today we study fields…

A *field* is a set of numbers with special properties

- Addition, with identity: $a + 0 = a$ and inverse $a+(-a)=0$
- Multiplication with identity: $a*1=a$ and inverse
  ($a * a^{-1} = 1$ for all $a != 0$)
- Subtraction and division (using inverses)
- Commutative, associative, and distributive properties
- Closure over all four operations

Examples:

- Real numbers
- GF(4) = $\{0, 1, \omega, \omega^2\}$ with these additional laws: $x + x = 0$ for all x and $\omega + 1 = \omega^2$.
- GF(p^n) for prime p is called a Galois Field.

Trappe&Washington, 3.11

Are these fields?

- A *field* is a **set of numbers** with the following properties:
  - Addition, with identity: a + 0 = a and inverse a+(-a)=0
  - Multiplication with identity: a*1=a, and inverse
    ($a * a^{-1} = 1$ for all a != 0)
  - Subtraction and division (using inverses)
  - Commutative, associative, and distributive properties
  - Closure over all four operations

- Examples:
  - Real numbers
  - GF(4) = $\{0, 1, \omega, \omega^2\}$ with these additional laws: x + x = 0 for all x and $\omega + 1 = \omega^2$.
  - GF(p^n) for prime p is called a Galois Field.

1. Positive integers
2. Integers
3. Rational numbers
4. Complex numbers
5. The set of 2x2 matrices of real numbers
6. Integers mod n (be careful here)

A Galois field is a finite field with p^n elements for a prime p

- Example: $GF(4) = GF(2^2) = \{0, 1, \omega, \omega^2\}$
- There is **only one** finite field with p^n elements for every power of n and prime p.

- The integers (mod p^n) aren't a field.
  - Why not?

$Z_2[X]$ is the set of polynomials with coefficients that are integers (mod 2)

- Example elements: $X+1$, $X^4 + X^2 + X + 1$
- Is this a field?
  - Does it have closure over add, subt, mult?
  - What about division?

- Almost a field. What about a closely-related finite field?
  - Consider $Z_2[X]$ mod $(X^2 + X + 1)$

$Z_2[X]$ (mod ($X^2 + X + 1$) is a finite field with only four elements)

- What are they?
- $\{0, 1, x, x+1\}$

Galois fields

If $Z_p[X]$ is set of polynomials with coefficients (mod p)

…and P(X) is degree n and irreducible (mod p)

(Reminder: irreducible = can't be factored into lower order terms)

Then $GF(p^n) = Z_p[X] \pmod{P(X)}$ is a field with p^n elements.

Consider $GF(2^8)$ with $P(X) = X^8 + X^4 + X^3 + X + 1$

Rijndael uses this!