



Last Updated: Sep 7, 2017

Programming Lab #1

- Implement AES
- Use the FIPS 197 spec as your guide
 - Avoid looking at code on the Internet
 - Challenge yourself to implement the algorithm based on sources mentioned in the lab specification
 - The standard provides programming language independent pseudo-code
 - 20 pages at the end of the spec has complete, step-by-step debugging information to check your solution

AES Parameters

- Nb Number of columns in the State
 o For AES, Nb = 4
- Nk Number of 32-bit words in the Key
 o For AES, Nk = 4, 6, or 8
- Nr Number of rounds (function of Nb and Nk)
 o For AES, Nr = 10, 12, or 14

AES methods

- Convert to state array
- Transformations (and their inverses)
 - AddRoundKey
 - SubBytes
 - ShiftRows
 - MixColumns
- Key Expansion

Inner Workings

• See Flash demo URL on course Lectures page

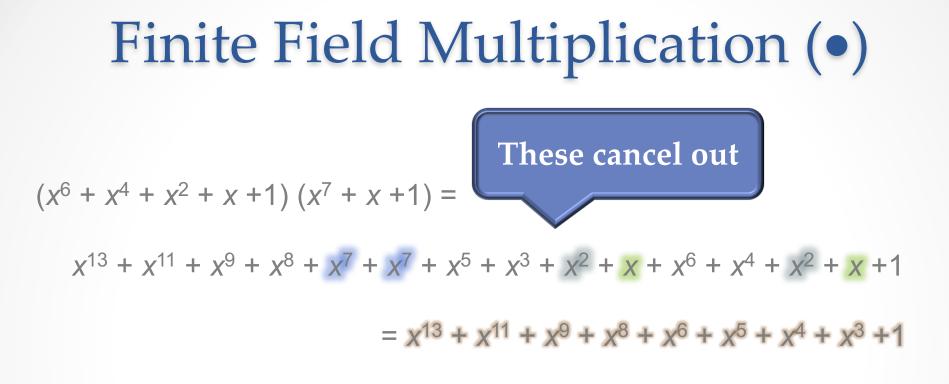
Finite Fields

- AES uses the finite field GF(2⁸)

 Polynomials of degree 8
 b₇x⁷ + b₆x⁶ + b₅x⁵ + b₄x⁴ + b₃x³ + b₂x² + b₁x + b₀
 {b₇, b₆, b₅, b₄, b₃, b₂, b₁, b₀}
- Byte notation for the element: $x^6 + x^5 + x + 1$
 - $\circ \quad 0x^7 + 1x^6 + 1x^5 + 0x^4 + 0x^3 + 0x^2 + 1x + 1$
 - o {01100011} binary
 - {63} hex
- Has its own arithmetic operations
 - Addition
 - Multiplication

Finite Field Arithmetic

- Addition (XOR)
 - $\circ (x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) = x^7 + x^6 + x^4 + x^2$
 - {01010111} ⊕ {10000011} = {11010100}
 - {57} ⊕ {83} = {d4}
- Multiplication is tricky
 - Study section 4.2 in the spec
 - In 4.2.1, a paragraph describes what your implementation will do. Study it. Difficult to interpret.



and

 $x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \text{ modulo} (x^8 + x^4 + x^3 + x + 1)$ = $x^7 + x^6 + 1$.

Irreducible Polynomial

Efficient Finite Field Multiply

- There's a better way
 - Patterned after the divide and conquer modular exponentiation algorithm (CS 312)
 - xtime() very efficiently multiplies its input by {02}
 - This is the same as multiplying a polynomial by x
 - \circ think about what is the binary representation of the polynomial x?
 - Figure out when the mod operation should occur.
- Multiplication by higher powers can be accomplished through repeated applications of xtime()

Efficient Finite Field Multiply

Example: {57} • {13} {57} • {02} = xtime({57}) = {ae} {57} • {04} = xtime({ae}) = {47} {57} • {08} = xtime({47}) = {8e} {57} • {10} = xtime({8e}) = {07}

 $= \{fe\}$

 $\{57\} \bullet \{13\} = \{57\} \bullet (\{01\} \oplus \{02\} \oplus \{10\}) \\ = \{57\} \bullet (\{01\} \oplus \{02\} \oplus \{10\}) \\ = (\{57\} \bullet \{01\}) \oplus (\{57\} \bullet \{02\}) \oplus (\{57\} \bullet \{10\}) \\ = \{57\} \oplus \{ae\} \oplus \{07\}$

Efficient Finite Field Multiply

Example: {57} • {13} $\{57\} \bullet \{02\} = xtime(\{57\}) = \{ae\}$ $\{57\} \bullet \{04\} = xtime(\{ae\}) = \{47\}$ $\{57\} \bullet \{08\} = xtime(\{47\}) = \{8e\}$ $\{57\} \bullet \{10\} = xtime(\{8e\}) = \{07\}$

These are hexadecimal numbers {xx}

decimal 10!

{57} = {5/} • ({**01**} \oplus {**02**} \oplus {**10**})

$$\{13\} = \{57\} \bullet (\{01\} \oplus \{02\} \oplus \{10\})$$

= {57} + {ae} + {07}

 $= \{fe\}$

$$= \{57\} \bullet (\{01\} \oplus \{02\} \oplus \{10\})$$

$$57\} \bullet (\{01\} \oplus \{02\} \oplus \{10\})$$

 $= (\{57\} \bullet \{01\}) \oplus (\{57\} \bullet \{02\}) \oplus (\{57\} \bullet \{10\})$

See detailed multiplication example on the Lectures web page