Programming Lab #1

• Implement AES
  o Use FIPS 197 as guide
    • Everything in this tutorial but in more detail
    • Pseudocode
    • 20 pages of complete, step by step debugging information
Finite Fields

• AES uses the finite field GF($2^8$)
  - $b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$
    - \{b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0\}

• Byte notation for the element: $x^6 + x^5 + x + 1$
  - $0x^7 + 1x^6 + 1x^5 + 0x^4 + 0x^3 + 0x^2 + 1x + 1$
  - \{01100011\} – binary
  - \{63\} – hex

• Has its own arithmetic operations
  - Addition
  - Multiplication
Finite Field Arithmetic

- Addition (XOR)
  - \((x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) = x^7 + x^6 + x^4 + x^2\)
  - \(\{01010111\} \oplus \{10000011\} = \{11010100\}\)
  - \(\{57\} \oplus \{83\} = \{d4\}\)

- Multiplication is tricky
Finite Field Multiplication (\( \bullet \))

\[(x^6 + x^4 + x^2 + x + 1) (x^7 + x + 1) = \]

\[x^{13} + x^{11} + x^9 + x^8 + x^7 + x^7 + x^5 + x^3 + x^2 + x + x^6 + x^4 + x^2 + x + 1\]

These cancel out

\[= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1\]

and

\[x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \mod (x^8 + x^4 + x^3 + x + 1) = x^7 + x^6 + 1.\]
Efficient Finite Field Multiply

• There’s a better way
  o \texttt{xtime()} – very efficiently multiplies its input by \{02\}

• Multiplication by higher powers can be accomplished through repeat application of \texttt{xtime()}
Efficient Finite Field Multiply

Example: \{57\} \cdot \{13\}

\{57\} \cdot \{02\} = xtime(\{57\}) = \{ae\}
\{57\} \cdot \{04\} = xtime(\{ae\}) = \{47\}
\{57\} \cdot \{08\} = xtime(\{47\}) = \{8e\}
\{57\} \cdot \{10\} = xtime(\{8e\}) = \{07\}

\{57\} \cdot \{13\} = \{57\} \cdot (\{01\} \oplus \{02\} \oplus \{10\})
= \{57\} \cdot (\{01\} \oplus \{02\} \oplus \{10\})
= (\{57\} \cdot \{01\}) \oplus (\{57\} \cdot \{02\}) \oplus (\{57\} \cdot \{10\})
= \{57\} \oplus \{ae\} \oplus \{07\}
= \{fe\}
AES Parameters

- **Nb** – Number of columns in the State
  - For AES, Nb = 4

- **Nk** – Number of 32-bit words in the Key
  - For AES, Nk = 4, 6, or 8

- **Nr** – Number of rounds (function of Nb and Nk)
  - For AES, Nr = 10, 12, or 14
AES methods

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

Input block:
Inner Workings

• See Flash demo URL on course Lectures pages