Advanced Encryption Standard (AES)

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:
http://www.cse.wustl.edu/~jain/cse571-17/

Overview

1. AES Structure
2. AES Round Function
3. AES Key Expansion
4. AES Decryption


Advanced Encryption Standard (AES)

- Published by NIST in Nov 2001: FIPS PUB 197
- Based on a competition won by Rijmen and Daemen (Rijndael) from Belgium
- 22 submissions, 7 did not satisfy all requirements
- Rijndael allows many block sizes and key sizes
- AES restricts it to:
  - Block Size: 128 bits
  - Key sizes: 128, 192, 256 (AES-128, AES-192, AES-256)
- An iterative rather than Feistel cipher
  - operates on entire data block in every round
- Byte operations: Easy to implement in software

Basic Structure of AES

- # Rounds \( N_l = 6 + \max\{N_b, N_k\} \)
- \( N_b = 32\)-bit words in the block
- \( N_k = 32\)-bit words in key
- AES-128: 10
- AES-192: 12
- AES-256: 14

Block Structure
1. Substitute Bytes

- Each byte is replaced by byte indexed by row (left 4-bits) & column (right 4-bits) of a 16x16 table.

```
\begin{array}{cccc}
5 & 6 & 7 & 8 \\
9 & A & B & C \\
D & E & F & 0 \\
\end{array}
```

2. Shift Rows

- 1st row is unchanged.
- 2nd row does 1 byte circular shift to left.
- 3rd row does 2 byte circular shift to left.
- 4th row does 3 byte circular shift to left.

3. Mix Columns

- Effectively a matrix multiplication in GF(2^8) using prime polynomial \( m(x) = x^8 + x^4 + x^3 + x + 1 \)

```
\begin{array}{cccc}
0 & 1 & 0 & 1 \\
1 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 \\
1 & 1 & 0 & 1 \\
\end{array}
```

```
\begin{array}{cccc}
87 & F2 & 4D & 97 \\
EC & 6E & 4C & 90 \\
4A & C3 & 46 & E7 \\
8C & D8 & 95 & A6 \\
\end{array}
```

AES Arithmetic

- Uses arithmetic in the finite field GF(2^8) with irreducible polynomial
- \( m(x) = x^8 + x^4 + x^3 + x + 1 \)
- which is \( \{1 0001 1011\} \) or \( \{11B\} \)

Example:

- \( \{02\} \cdot \{87\} \mod \{11B\} = (0000 \ 0010)(0000 \ 0111) \)
- \( x (x^4 + x^3 + x + 1) = (x^4 + x^3 + x^2 + x) \mod (x^8 + x^4 + x^3 + x + 1) \)
- \( = x^4 + x^2 + 1 \mod (0001 \ 0101) \)
- \( \{03\} \cdot \{6E\} = \{11\} \{110 \ 1110\} = (x + 1) (x^6 + x^4 + x^3 + x^2 + x) \mod (x^8 + x^4 + x^3 + x + 1) \)
- \( = x^4 + x^3 + x^2 + x \mod (x^8 + x^4 + x^3 + x + 1) \)
- \( \{06\} \cdot \{A6\} = \{1011 \ 0010\} \)
- \( 0001 \ 0101 \mod \{1011 \ 0010\} = 0010 \ 0110 \mod \{1010 \ 0110\} = 0100 \ 0111 \)
- \( \{47\} \)}
4. Add Round Key

- XOR state with 128-bits of the round key
  - Key = 0f 15 71 c9
  - Text = 01 23 45 67 89 abc de fe db a9 87 65 43 21 0

\[\begin{align*}
(01\ 89\ fe\ 76) & \oplus (0f\ 47\ 0c\ af) = (0e\ ce\ 72\ d9) \\
23\ ab\ dc\ 54 & \oplus (15\ d9\ b7\ 7f) = (36\ 72\ 6b\ 2b) \\
45\ cd\ ba\ 32 & \oplus (71\ e8\ ad\ 67) = (34\ 25\ 17\ 55) \\
67\ ef\ 98\ 10 & \oplus (c9\ 59\ d6\ 98) = (ae\ b6\ 4e\ 88)
\end{align*}\]

128-bit Text 128-bit Key 128-bit Sum

- \(W0\ W1\ W2\ W3\)

AES Key Expansion

- Use 4-byte subkeys \(w_i\). Subkey = 4 words.
- For AES-128:
  - First subkey \((w_0, w_1, w_2, w_3)\) = cipher key
  - Other words are calculated as follows:
    \[w_i = w_{i-1} \oplus w_{i-4}\]
    for all values of \(i\) that are not multiples of 4.
- For the words with indices that are a multiple of 4 \((w_{4k})\):
  1. RotWord: Bytes of \(w_{4k-1}\) are rotated left shift (nonlinearity)
  2. SubWord: SubBytes \(f\) is applied to all four bytes. (Diffusion)
  3. The result \(r_{sk}\) is XOR'ed with \(w_{4k-4}\) and a round constant \(r_{conk}\) (breaks Symmetry):
    \[w_{4k} = r_{sk} \oplus w_{4k-4} \oplus r_{conk}\]
- For AES-192 and AES-256, the key expansion is more complex.

AES Example Key Expansion

<table>
<thead>
<tr>
<th>Key Words</th>
<th>Auxiliary Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>w0 = 0f 15 71 c9</td>
<td>RotWord(w_0) = 7f 67 7a af = x1</td>
</tr>
<tr>
<td>w1 = 47 d9 e8 59</td>
<td>SubWord(w_1) = d2 85 46 79 = y1</td>
</tr>
<tr>
<td>w2 = 0e b7 ad 6f</td>
<td>Reun(1)(w_2) = 00 00 00 00</td>
</tr>
<tr>
<td>w3 = af 7f 67 98</td>
<td>y1 &amp; Reun(1) = d3 85 46 7a</td>
</tr>
</tbody>
</table>

AES Example Encryption

- \(01 + 0f = 0e\)
- \(89 + 47 = ce\)

\[\begin{pmatrix}
\begin{array}{c}
01 \\
89 \\
37 \\
9b \\
90 \\
37 \\
67
\end{array}
\end{pmatrix}
\begin{pmatrix}
\begin{array}{c}
0f \\
15 \\
71 \\
c9 \\
76 \\
fe \\
76
\end{array}
\end{pmatrix}
= \begin{pmatrix}
\begin{array}{c}
47 \\
9d \\
0a \\
6f \\
9b \\
08 \\
67
\end{array}
\end{pmatrix}
\]

\[\begin{pmatrix}
\begin{array}{c}
dc \\
90 \\
37 \\
9b \\
90 \\
37 \\
67
\end{array}
\end{pmatrix}
\begin{pmatrix}
\begin{array}{c}
0f \\
15 \\
71 \\
c9 \\
76 \\
fe \\
76
\end{array}
\end{pmatrix}
= \begin{pmatrix}
\begin{array}{c}
dc \\
90 \\
37 \\
9b \\
90 \\
37 \\
67
\end{array}
\end{pmatrix}
\]

\[\begin{pmatrix}
\begin{array}{c}
0f \\
15 \\
71 \\
c9 \\
76 \\
fe \\
76
\end{array}
\end{pmatrix}
\begin{pmatrix}
\begin{array}{c}
0f \\
15 \\
71 \\
c9 \\
76 \\
fe \\
76
\end{array}
\end{pmatrix}
= \begin{pmatrix}
\begin{array}{c}
47 \\
9d \\
0a \\
6f \\
9b \\
08 \\
67
\end{array}
\end{pmatrix}
\]

\[\begin{pmatrix}
\begin{array}{c}
dc \\
90 \\
37 \\
9b \\
90 \\
37 \\
67
\end{array}
\end{pmatrix}
\begin{pmatrix}
\begin{array}{c}
0f \\
15 \\
71 \\
c9 \\
76 \\
fe \\
76
\end{array}
\end{pmatrix}
= \begin{pmatrix}
\begin{array}{c}
dc \\
90 \\
37 \\
9b \\
90 \\
37 \\
67
\end{array}
\end{pmatrix}
\]

\[\begin{pmatrix}
\begin{array}{c}
0f \\
15 \\
71 \\
c9 \\
76 \\
fe \\
76
\end{array}
\end{pmatrix}
\begin{pmatrix}
\begin{array}{c}
0f \\
15 \\
71 \\
c9 \\
76 \\
fe \\
76
\end{array}
\end{pmatrix}
= \begin{pmatrix}
\begin{array}{c}
47 \\
9d \\
0a \\
6f \\
9b \\
08 \\
67
\end{array}
\end{pmatrix}
\]

\[\begin{pmatrix}
\begin{array}{c}
0f \\
15 \\
71 \\
c9 \\
76 \\
fe \\
76
\end{array}
\end{pmatrix}
\begin{pmatrix}
\begin{array}{c}
0f \\
15 \\
71 \\
c9 \\
76 \\
fe \\
76
\end{array}
\end{pmatrix}
= \begin{pmatrix}
\begin{array}{c}
47 \\
9d \\
0a \\
6f \\
9b \\
08 \\
67
\end{array}
\end{pmatrix}
\]

\[\begin{pmatrix}
\begin{array}{c}
0f \\
15 \\
71 \\
c9 \\
76 \\
fe \\
76
\end{array}
\end{pmatrix}
\begin{pmatrix}
\begin{array}{c}
0f \\
15 \\
71 \\
c9 \\
76 \\
fe \\
76
\end{array}
\end{pmatrix}
= \begin{pmatrix}
\begin{array}{c}
47 \\
9d \\
0a \\
6f \\
9b \\
08 \\
67
\end{array}
\end{pmatrix}
\]
Summary

1. AES encrypts 128 bit blocks with 128-bit, 192-bit or 256-bit keys using 10, 12, or 14 rounds, respectively.
2. Is not a Feistel cipher ⇒ All 128 bits are encrypted
3. Each round = 4 steps of SubBytes, ShiftRows, MixColumns, and AddRoundKey.
4. Last round has only 3 steps. No MixColumns.
5. Decryption is not the same as encryption (as in DES). Decryption consists of inverse steps.

Homework 5

Given the plaintext \([0001 0203 0405 0607 0809 0A0B 0C0D 0E0F]\) and the key \([0101 0101 0101 0101 0101 0101 0101 0101]\)

a. Show the original contents of state, displayed as a 4x4 matrix. Hint: First Row: 00 04 08 0C
b. Show the value of state after initial AddRoundKey. Hint: First Row: 01 05 09 0D
c. Show the value of State after SubBytes. Hint: First Row: 0F 7C 97 05
d. Show the value of State after ShiftRows. Hint: First Row: 7C 97 05 0F
e. Compute the value of State after MixColumns. Show detailed computations for all elements of the first row. To practice, you may compute 2nd, 3rd, 4th rows for step e but there is no need to submit. Submit only the first row for step e.

For all other steps, show all 4 rows. Hint: First Row: 75 87 0F B2
Acronyms

- AES  Advance Encryption Standard
- DES  Data Encryption Standard
- FIPS  Federal Information Processing Standard
- GF   Galois Field
- NIST  National Institute of Science and Technology
- RC   Ron's Code
- XOR  Exclusive OR

Related Modules

CSE571S: Network Security (Spring 2017),
http://www.cse.wustl.edu/~jain/cse571-17/index.html

CSE473S: Introduction to Computer Networks (Fall 2016),
http://www.cse.wustl.edu/~jain/cse473-16/index.html

Wireless and Mobile Networking (Spring 2016),
http://www.cse.wustl.edu/~jain/cse574-16/index.html

CSE571S: Network Security (Fall 2014),
http://www.cse.wustl.edu/~jain/cse571-14/index.html

Audio/Video Recordings and Podcasts of Professor Raj Jain's Lectures,
https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw