Foundations of Computer Security

Lecture 46: Advanced Encryption Standard

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

Modern Symmetric Encryption

Most modern symmetric encryption algorithms are:

block ciphers: take input in fixed size blocks;

implemented in rounds: perform similar operations repeatedly to a "state";.

Such an algorithm is called an *iterated block cipher.*

Designed to process large volumes of text quickly, they use machine operations (arithmetic, bitwise, table lookup) that are cheap and easy to implement.

Advanced Encryption Standard

In 1995, NIST began a search for a new, fast, secure symmetric encryption algoithm that was:

- unclassified;
- publicly disclosed;
- available royalty-free for use worldwide;
- symmetric block cipher algorithm for blocks of 128 bits;
- usable with key sizes of 128, 192, and 256 bits.

From 15 contenders, the Rijndael algorithm of Dutch researchers Vincent Rijmen and Joan Daemen was chosen as the Advanced Encryption Standard (AES).

Overview of AES

A 128-bit block is arranged as a 4×4 array of bytes called the "state," which is modified in place in each round.

$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix}$$

The key is also arranged as a $4 \times n$ array of bytes, and is initially expanded in a recursive process into $r + 1$ 128-bit keys, where r is the number of rounds.

AES uses 10, 12, or 14 rounds for keys of 128, 192, and 256 bits, respectively.

Rounds in AES

Each round consists of four steps.

subBytes: for each byte in the array, use its value as an index into a 256-element lookup table, and replace byte by the value stored at that location in the table.

shiftRows: Let R_i denote the i^{th} row in state. Shift R_0 in the state left 0 bytes (i.e., no change); shift R_1 left 1 byte; shift R_2 left 2 bytes; shift R_3 left 3 bytes.

Rounds in AES

mixColumns: for each column of the state, replace the column by its value multiplied by a fixed 4 × 4 matrix of integers (as illustrated below).

$$\begin{bmatrix} a_0' \\ a_1' \\ a_2' \\ a_3' \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

addRoundKey: XOR the state with a 128-bit round key derived from the original key K by a recursive process.

Decryption in AES

The decryption algorithm is the inverse of encryption, with the following differences:

- The subkeys are used in reverse order.
- Each of the steps is inverted.
- The first and last rounds are slightly different.

Inverting the MixColumns step requires multiplying each column by the following fixed array:

$$\begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix}$$

For that reason, decryption typically takes longer than encryption.

Security of the AES

AES is incorporated in a large number of commercial encryption products. The algorithm is fairly new, but has been subjected to extensive analysis,

No flaws have been discovered, but that doesn't mean that none exist.

AES is modular and the key length can be extended if necessary. Similarly, the number of rounds can be increased.

Lessons

- AES is a widely-used modern symmetric encryption algorithm.
- AES uses a block of 128-bits.
- AES allows keys of size 128-bits, 192-bits, and 256-bits, with 10, 12, 14 rounds, respectively.

Next lecture: Modes of Usage