

A Short Introduction to the AES Algorithm Rijndael

Christian Boesgaard

Department of Computer Science, University of Copenhagen, pink@diku.dk

October 3, 2001

This document is meant as a short overview of Rijndael. Please consult [1] for details.

Rijndael

Rijndael is a block cipher. Rijndael was chosen as the algorithm for the Advanced Encryption Standard (AES). Rijndael was designed by Joan Daemen and Vincent Rijmen.

Rijndael consists of a number of rounds, each round makes a number of transformations on a state, and uses a round key derived from the encryption key. The number of rounds depends on the block and key size. An odd number of regular rounds is followed by a special final round, this is done to make use of an encryption implementation for decryption easier and has nothing to do with security (This is described in 5.3 in [1]).

Rijndael is, unlike DES and a lot of other block ciphers, not based on a feistel network¹. All the transformations used are invertible, which makes decryption possible.

The state can be pictured as a rectangular array of bytes, consisting of four rows and a number of columns defined by the block size in bytes divided by four. A block size of 128 bit, would require a state of four rows and $(128/8)/4 = 4$ columns.

The state is initialized with a block of plaintext and after the rounds are completed it will hold the ciphertext.

The round transformations

There are four transformations:

AddRoundKey

AddRoundKey is an XOR between the state and the round key. This is of course invertible.

ByteSub

ByteSub is a substitution of each byte in the block independent of the position in the state. It is a bijection on all possible byte values and therefore invertible. This is the non-linear transformation. The S-box used is proved to be optimal with regards to non-linearity. The S-box is based on operations in $GF(2^8)$.

ShiftRow

ShiftRow is a cyclic shift of the bytes in the rows in the state and is clearly invertible.

¹A feistel network is a construction like DES where the block is split into halves and one half is used to encrypt the other by a function that is not necessarily invertible, see definition 7.81 in [2].

MixColumn

Each column in the state is considered a polynomial with the byte values as coefficients. The columns are transformed independently by multiplication with a special polynomial $c(x)$ (see 4.2.3 in [1]). $c(x)$ has an inverse $d(x)$, that is used to reverse the multiplication by $c(x)$.

The rounds

A round is composed of:

```
Round(State, RoundKey) {
    ByteSub(State);
    ShiftRow(State);
    MixColumn(State);
    AddRoundKey(State, RoundKey);
}
```

The final round is like a regular round, but without the MixColumn transformation:

```
FinalRound(State, RoundKey) {
    ByteSub(State);
    ShiftRow(State);
    AddRoundKey(State, RoundKey);
}
```

The RoundKey

The Roundkeys are made by expanding the encryption key into an array holding the RoundKeys one after another. The expansion works on words of four bytes. Nk is a constant defined as the number of four bytes words in the key.

The encryption key is filled into the first Nk words and the rest of the key material is defined recursively from preceding words. The word in position i , $W[i]$, except the first word of a RoundKey, is defined as the XOR between the preceding word, $W[i-1]$, and $W[i-Nk]$. The first word of each RoundKey, $W[i]$ (where $i \bmod Nk == 0$), is defined as the XOR of a transformation on the preceding word, $T(W[i-1])$ and $W[i-Nk]$. The transformation T on a word, w , is w rotated to the left by one byte, XOR'ed by a round constant and with each byte substituted by the S-box.

References

- [1] J. Daemen and V. Rijmen. Aes proposal: Rijndael, 1998.
- [2] A. J. (Alfred J.) Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. The CRC Press series on discrete mathematics and its applications. CRC Press, 2000 N.W. Corporate Blvd., Boca Raton, FL 33431-9868, USA, 1997.