ProtectStar™ Extended AES

Block-Size: 512-bit (64-byte)
Key Sizes: 128, 256 and 512-bit (16, 32 and 64 byte) (*default 256-bit*)
Modes of Operation: ECB, CBC, CFB, OFB and CTR (*default CTR*)
Total Round Number: 24

Abstract

This documentation explains the details of our extended version of AES encryption algorithm which uses fixed-length 512-bit block length and three possible key lengths respectively 128, 256 or 512 bits.

1. Motivation

The standard AES uses 128-bit message block length (i.e. 16 bytes) and 128-bit key length. 192 and 256-bit key lengths are also supported by AES. For the combination of 128/128 (Block/Key), the AES message block and key can be realized as a 4*4 matrix. Each matrix cell represents a single Byte and 16 (4*4) cells makes then 16 bytes which are equal to 128-bits.

Similarly, for the extended AES we use 4*16 matrix (4: row size, 16: column size) for representing the message blocks and the round keys. The extended AES uses some properties and functions of the original AES exactly (e.g. adding round key, column mixing, etc), whereas some properties and functions are specific to the extended AES (e.g. the total round number, row shifting, etc.).

In the following sections, the relevant properties and functions used in the original AES and the extended AES are explained in details.

2. Modes of Operations

All the supported modes of operation by the original AES *(i.e. Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB) and Counter (CTR)*) have been also implemented for the extended AES.

3. Total Round Numbers

For encrypting and decrypting a single block, the original AES algorithm applies its functions in total within 10 rounds. This number 10 is calculated with the following formula:

Round number = (key size or block size in words) + 6

The constant number 6 is specified and fixed by the AES designers according to the known crypto attacks. If the key size is 256-bit then 14 rounds (8+6) are required.

For the extended AES, the block length is fixed to 512-bit. That makes 16 words because each word is 4 bytes. The total round number is calculated as 22 based on the formula above. Actually we need 2 more rounds due to ShiftRow operation as explained in the next sections. As a conclusion, the extended AES applies 24 rounds for encrypting and decrypting a single block.

4. Padding

The padding operation is very common for padding message blocks and key blocks for the block ciphers. For the extended AES, we need both message and key padding.

Message Padding

The length of the input messages should be multiple of 512 in the extended AES. For the padding operation, we follow the padding mechanism described in RFC 1321. In this padding method, after the original last message bit, a bit “1” is inserted and then “0” bits are appended until the last message block has the length 512. If there is no space left for any extra padding “0”s, then a new 512-bit block is added at the end of the message.

Key Padding

The extended AES support the key sizes of 16, 32 and 64 bytes. For initializing the key block, a password given by the users is used. If the password does not contain enough characters to fill up the key block, then the remaining bytes in the key block are filled up by zeros. Actually this simple padding would be enough for the original AES, but not for the extended AES. Considering the key size 64 bytes, assume the password only composes of the first 10 bytes in the key block and the remaining 54 bytes are assigned to zero. On the other hand, this initial key block is used for generating the round keys. In this case, there would exist many round keys whose value is zero due to the fact that the key block contains many zero bytes. To prevent this problem and not generate many round keys with the value zero, we do apply the original AES encryption on the zero-padded key block with a fixed key in CBC mode. The encryption result becomes the padded key to generate the round keys and we prevent the many-zero problem.

5. Round Keys Generation

The round keys are generated from the padded key block which explained in the previous "Key Padding" section. The original round key generation process (see Rijndael Block Cipher Specification, pg. 15) is slightly modified for the extended AES and the following algorithm is used to generate the round keys:

```
KeyExpansion(byte Key[4*Nk] word W[Nb*(Nr+1)])
{
   for(i = 0; i < Nk; i++)
         W[i] = (key[4*i],key[4*i+1],key[4*i+2],key[4*i+3]);

   for(i = Nk; i < Nb * (Nr + 1); i++)
   {
         temp = W[i - 1];
         if (i % Nk == 0 || (I % Nk==4 && Nk>6))
               temp = SubByte(RotByte(temp)) ^ Rcon[i / Nk];
         else if ((i % Nk == 8 || i % Nk == 12) && Nk>6)
               temp = SubByte(temp);
         W[i] = W[i - Nk] ^ temp;
   }
}
```

6. Functions

The original AES uses basically 4 main functions. These are xor-add operation between the message block and the round key (AddRoundKey), Sbox lookups (SboxSubstitution), row shifting (ShiftRow) and mixing each column in the matrix (MixColumn).

AddRoundKey

For the round key adding process, there is no difference between the original and the extended AES.

SboxSubstitution

The Sbox lookup process is also identical in the original and the extended AES.

ShiftRow

The row shifting process is different in the original and the extended AES. The original AES applies {0,1,2,3} offsets for the row shifting. That means in the ShiftRow operation, the bytes in the first row are not shifted. The bytes in the second row are shifted 1-byte to the left (*for encryption*); the bytes in the third row are shifted 2-byte to the left and finally the bytes on the last row are shifted 3-byte to the left. The ShiftRow operation is applied in each round of the AES and after two rounds the combination of the ShiftRow and the MixColumn operations provide a total diffusion over the matrix; that means after two rounds, each matrix cell affects the value of all the other cells in the matrix.

But if we apply the {0,1,2,3} offsets for the row shifting in the extended AES, this total diffusion is achieved after 5 rounds, instead of 2 rounds. Hence, we should find better shifting offsets which provide the total diffusion in a few rounds. For this purpose, we did write a program (*see com.crypt.test.OptimumShiftRow.java the distributed source code*) which did compute the optimum shifting offsets. The result was that the total diffusion can only be achieved after 4 rounds for the extended AES. There were many candidates that provide the total diffusion in 4 rounds and we have chosen the {0,1,4,5} offsets for the extended AES.

MixColumn

The same MixColumn operation is applied for the original and the extended AES. In the original AES, there are only 4 columns, whereas the extended AES contains 16 columns.

References

- The Rijndael Block Cipher: http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf
- AES: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
- Modes of Operation: http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

Contact

ProtectStar Research
1901 60th Place
Suite L3604
Bradenton, FL
USA

Phone: +1 888 218 4123
Fax : +1 888 218 8505