Scribe: Cryptography and Network Security (Week 6 - Class 5)

Rashil Gandhi

10-Oct-2020

1 Introduction

This class goes into the details of the four steps - Byte Sub, Shift Row, Mix Column, and Add Key - of the AES 128-bit algorithm and provides insights on how decryption is implemented in a manner similar to encryption by introducing some workarounds.

2 The Steps

The plaintext is broken down into square blocks of 4x4x(8bit) = 128bit matrices before encryption. Padding is used to make up for insufficient plaintext data. The following steps are performed in all 10 rounds of 128-bit AES (except the last round, where Mix Column isn't performed).

2.1 Substitution Box

This is the most crucial part of AES algorithm, since it is the only step that involves non-linear transformations. First, the input (each byte) is mapped to it's multiplicative inverse in GF(2^8). The output undergoes an affine transformation which is basically a matrix multiplication with a predefined constant matrix and then addition with a constant matrix. The addition matrix is used to avoid fixed points and opposite fixed points in the output.

Since the transformation invloves constants, lookup tables are generally used to avoid recalculations. The column in the lookup table is identified by the least significant nibble of the input, and the row by the most significant nibble.

2.2 Shift Row

The block obtained from the previous step is then processed as follows: - the first row is left as is, the second row is circularly shifted left by one step, the third row is circularly shifted left by two steps and the last row is circularly shifted left by three steps. This transformation ensures diffusion of entropy obtained from the S-Box procedure into all the columns.

2.3 Mix Columns

Each column of the block obtained from the previous step undergoes matrix multiplication with a constant matrix. This ensures the diffusion of entropy spreads into all rows of all columns. The constant matrix is chosen such that maximum spread is achieved.

Mix column step is skipped in the last round as it can be proved that it is redundant in the last round.

2.4 Add Key

The round key is simply XORed with the output elements of the matrix obtained in previous step. Round keys are obtained from the AES key using Key Scheduling Algorithm.

3 Decryption

All the transformations invloved in the encryption process are intentionally made invertible to make the decryption process possible. Now, we can't just simply feed in the cipher text and key into the algorithm to obtain the plain text, because some of the steps in each round need to be performed in a specific order.

Decryption is usually costlier (in terms of performance) than encryption as some additional steps (like computing inverses of matrices) need to be performed such that the decryption flow can be made exaclty opposite to the encryption flow.

4 Conclusion

We saw in the class with detailed examples how each round of AES is performed and saw how decryption process can be made to run on the same hardware as the ecnryption hardware with some slight modifications.