10

Cryptography I, Homework 3

Explain what the lookup-table structure of the 4 tables T_0, T_1, T_2, T_3 in AES looks like; recall that these are the tables that combine *SubBytes*, *ShiftRows*, and *Mixcolumns*.

5/5

In the lookup-table the different steps of the round transformation are combined, allowing a very fast implementation on processors with word length 32 or above.

One column of the round output can be expressed as a function of the round input A, where $a_{i,j}$ denotes the byte of A in row i and column j, a_j denotes the column j of State A.

For the SubBytes we have;

$$b_{i,j} = S[a_{i,j}]$$

After that we apply the ShiftRows on the SubBytes with a certain shift offset depending on the block lengths;

$$\begin{bmatrix} c_{0,j} \\ c_{1,j} \\ c_{2,j} \\ c_{3,j} \end{bmatrix} = \begin{bmatrix} b_{0,j} \\ b_{1,j-C1} \\ b_{2,j-C2} \\ b_{3,j-C3} \end{bmatrix}$$

In the case of a block length of 4, $C1 = 1, C2 = 2$ and $C3 = 3$.

After this the Mixcolumns is applied, this can be done by matrix multiplication.

$$\begin{bmatrix} d_{0,j} \\ d_{1,j} \\ d_{2,j} \\ d_{3,j} \end{bmatrix} = \begin{bmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{bmatrix} \begin{bmatrix} c_{0,j} \\ c_{1,j} \\ c_{2,j} \\ c_{3,j} \end{bmatrix}$$

Combine these 3 steps into 1 you get that the round transformation is as follows.

$$\begin{bmatrix} d_{0,j} \\ d_{1,j} \\ d_{2,j} \\ d_{3,j} \end{bmatrix} = \begin{bmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{bmatrix} \begin{bmatrix} S[a_{0,j}] \\ S[a_{1,j-C1}] \\ S[a_{2,j-C2}] \\ S[a_{3,j-C3}] \end{bmatrix}$$

The matrix multiplication can be expressed as a linear combination of vectors:

$$\begin{bmatrix} d_{0,j} \\ d_{1,j} \\ d_{2,j} \\ d_{3,j} \end{bmatrix} = S[a_{0,j}] \begin{bmatrix} 02 \\ 01 \\ 01 \\ 03 \end{bmatrix} \oplus S[a_{1,j-C1}] \begin{bmatrix} 03 \\ 02 \\ 01 \\ 01 \end{bmatrix} \oplus S[a_{2,j-C2}] \begin{bmatrix} 01 \\ 03 \\ 02 \\ 01 \end{bmatrix} \oplus S[a_{3,j-C3}] \begin{bmatrix} 01 \\ 01 \\ 03 \\ 02 \end{bmatrix}$$

The multiplication factors $S[a_{i,j}]$ of the four vectors are obtained by performing a lookup in the S-box table $S[256]$

With T_0 to T_3 the four tables that are defined by

$$T_0[a] = \begin{bmatrix} S[a] \cdot 02 \\ S[a] \\ S[a] \\ S[a] \cdot 03 \end{bmatrix}, T_1[a] = \begin{bmatrix} S[a] \cdot 03 \\ S[a] \cdot 02 \\ S[a] \\ S[a] \end{bmatrix}, T_2[a] = \begin{bmatrix} S[a] \\ S[a] \cdot 03 \\ S[a] \cdot 02 \\ S[a] \end{bmatrix}, T_3[a] = \begin{bmatrix} S[a] \\ S[a] \\ S[a] \cdot 03 \\ S[a] \cdot 02 \end{bmatrix}$$

These are 4 tables with 256 4-byte word entries. Using these tables, the round transformation can be expressed as:

$$d_j = T[a_{0,j}] \oplus T[a_{1,j-C1}] \oplus T[a_{2,j-C2}] \oplus T[a_{3,j-C3}]$$

A table-lookup takes only 4 table lookups and 4 XORs per column per round.

A message of length 64 bytes is encrypted with AES and sent via a network. During the transmission one bit in the second block is flipped.

- Explain for each of the 5 modes of operation how many bits are definitely and how many bits are potentially different in the deciphered text compared to the initial plaintext

5/5

AES has a fixed block size of 128 bits so a message of 64 bytes has 4 blocks. The key-size is variable and can be 128, 192 or 256 bits. AES uses at least 10 cycles of repetition.

Encrypting a 128bit-string with one bit flipped via AES will mess up the whole string. The particular byte with the flipped bit is first mapped to a whole different byte by the round key, then the inverse Mixcolumns is applied which will mess up all the bytes in the column with the messed up byte. Then by ShiftRows each of the messed up bytes will be put in a different column and by again applying the inverse Mixcolumns the whole block is messed up.

Because AES is inversible at least 1 bit of the encrypted 128bit-string should be flipped, potentially the whole block is flipped.

Electronic Codebook mode

Because the electronic codebook mode encrypts each block separately only the second block is messed up. This means 128 bits are potentially messed up with this mode. Because the inverse property of AES there is definitely 1 bit flipped.

Cipher-block chaining mode

Because the ciphertext of block 2 is used to decrypt block 3 by a simple XOR operation one of the bites in block 3 will be flipped. Furthermore the bytes of block 2 will all be mixed up because its ciphertext is encrypted with AES. In total, there will be 2 bits definitely flipped and 129 potentially.

Cipher feedback mode

The Ciphertext of block 2 is damaged. This chipher text is used to decrypt itself by a simple XOR operation with the plain text from the first block. So one bit in block 2 is flipped.

The ciphertext of block 2 after encryption via AES is used to decrypt block 3 by XOR operation. But since this encryption gives us a messed up 128bit-string there will definitely be 1 flipped and potentially 128 flipped bits in the plaintext of block 3.

In total there will be definitely 2 bits flipped and potentially 129.

Output feedback mode

With the output feedback mode only the initialization vector is put through the EAS encryption and after that it is multiplied by a XOR operator to the ciphertext to get the plaintext. Because the ciphertext has one flipped bit, the plaintext of block 2 will also have exactly one flipped bit.

Counter mode

With the counter mode only the counted nonce will be encrypted with EAS. Afterwards this encryption is multiplied by a XOR operator to the ciphertext to get the plaintext. Because the ciphertext has 1 flipped bit, the plaintext will also have exactly one flipped bit.