Lecture 34 (Secure Processors)

1 Confusion

1. If a single bit in the key is changed, then most or all of the ciphertext bits should be affected
2. This ensures that the key and ct are not related

2 Diffusion

1. If we change a single bit in the plaintext, then half the bits in ct should change
2. Prevents related message attacks

3 Rounds in AES

1. Write the 16 bytes as a 4×4 matrix
2. Replace each of them using a lookup table S-box
3. Left rotate the i^{th} row by i positions
4. Take the four bytes in each column and modular multiply it with a matrix
5. Compute a bitwise XOR with the round key

4 Generating Round Key

1. Rotate word
2. Substitute word
3. XORWord - $B_0B_1B_2B_3 \rightarrow$
    - $B_0 = RC[i]$
    - $RC[0] = 1$, $RC[i] = 2 \cdot RC[i-1]$

5 AES Algo

1. First round - only the XOR with round key is performed
2. Final round - mix columns is skipped