AES Secrecy

Marco Christiani

December 2019

1 Confusion

We begin with a baseline example: a 32 byte key and 16 byte plaintext.

Key: a13112f2b1365c819203a34fe1ccd41cd1ff5db33a474eafe08beebd1b0111bf
Plaintext: f921ade849c8aac7b2036636443aed99
Ciphertext: 838958fb8c24640f8f23d161f9666329

To examine the confusion and diffusion properties of AES, we encrypt the plaintext again yet with 1 bit flipped:
Original Plaintext: f921ade849c8aac7b2036636443aed99
bin(0xad) = 10101101 → 10001101
hex(10001101) = 0x8d
New Plaintext: f9218de849c8aac7b2036636443aed99
Encrypting with the same key as before
Ciphertext: a816f87010d4ba67672325cfb5be20ec

To assess how different our two ciphertexts are, we XOR the bits and sum the 1's:

838958fb8c24640f8f23d161f9666329 XOR a816f87010d4ba67672325cfb5be20ec

10101110011111101000001000101110011100111100001101111011010001110100
00111101001010111010011001101100010000111100010 1
= 61 bits (51.7%) have been flipped after changing just one bit.

One key thing to note here is that although it was the 15th bit in the plaintext that was flipped, many of the first 15 bits in the new ciphertext were also altered.
Let's see AES could acheive a comparable amount of confusion if the last bit of the plaintext was altered instead:
Original Plaintext: f921ade849c8aac7b2036636443aed99
bin(0x99) = 10011001 → 10011000
hex(10011000) = 0x98
New Plaintext: 79218de849c8aac7b2036636443aed98

Encrypting with the same key as before:
Ciphertext: a1823eb7b6d0de74f5f943f0aee6d11e

Repeating the process as before, we XOR with the original ciphertext and count 63 changed bits which corresponds to 54.3%.

This illustrates how effectively AES creates confusion, since even a 1 bit change in the plaintext will propagate throughout the ciphertext irrespective of where that bit change occurs.

2 Diffusion

To assess AES's ability to create diffusion, we start with another example but the plaintext has an intentional pattern:

Key: a13112f2b1365c819203a34fe1ccd41cd1ff5db33a474eafe08beebd1b0111bf
Plaintext: a1b2c3d4e5f6778888776f5e4d3c2b1a
Notice that the plaintext string forms a palindrome.
Ciphertext: 4c77e6ea58d64755b8deb26c042c6e5f
In examining the ciphertext, we find no palindrome properties and 0x77 and 0xb2 to be the only shared bytes although in distance locations and out of order. Additionally we find no shared patterns, and no obvious patterns within the ciphertext.