Key Avalanche Effect (Each Cycle)

Setup

1,000 PRNG plaintexts were generated. Then, for each of 500 keys, 128 almost exactly identical keys were produced, their difference being just one bit flipped from the original, 1 ‘flipped key’ for each bit position among 16 bytes (128 bits). Then, each copy of the plaintext was encrypted with the setup produced from each original key and all of the bit flipped keys. At the end of each encryption cycle, the intermediate ciphertext produced from the bit flipped key setup was compared to the intermediate ciphertext from the original key setup (Specific to the current cycle) to determine their difference in bits. A distribution of these differences for each cycle was produced. After outputting each of these 16 distributions (1 for each cycle), the descriptive statistics were calculated for each of these samples to examine their properties as they change from cycle to cycle.

Hypothesis

The mean of the differences between the original intermediate ciphertext and the intermediate ciphertext encrypted by the bit flipped keys will become within ± 1 of the median of 64 bits after the 1st cycle of encryption.

Reasoning

The reasoning for the hypothesis is that every part of the encryption function, minus the Diffusion Slide 2, is dependent on the key schedule. The key schedule has already been shown to vary greatly with a change of only 1 bit in the key (Specifically the mean being half of the key schedule changing), so this change should quickly produce changes in the intermediate ciphertext. What is not clear, however, is that from the previous “PAE Each Cycle” test, the Diffusion Slide 2 function was shown to make very large changes to the mean and range of the difference distribution, though it essentially “evened out” by the last cycle. While the hypothesis would still be true if the mean became close to the median after the 1st cycle, this mean might become warped every time the Diffusion Slide 2 is applied. It is known, however, that the KAE mean does become almost exactly the median by the end of all 16 encryption cycles, it is just untested as to how these changes develop as it goes through each cycle, but that is exactly what this test will show. Just like the previous PAE test for each cycle, on the next page is a large table tracking the changes throughout the encryption cycles.

Cycles	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Max	95	95	95	94	95	95	95	94	94	95	97	96	95	96	95	96
Min	29	32	31	34	34	29	31	32	30	29	33	33	33	35	34	32
Range	66	63	64	60	61	66	64	62	64	66	64	63	62	61	61	64
Mean	64	64	64	64	64	64	64	64	64	64	64	64	64	64	64	64
Mode (s)	64	64	64	64	64	64	64	64	64	64	64	64	64	64	64	64
Variance	32	32	32	32	32.01	32.01	32	32	32	32	32	32	31.99	32	31.99	32
Std. Dev.	5.66	5.66	5.66	5.66	5.66	5.66	5.66	5.66	5.66	5.66	5.66	5.66	5.66	5.66	5.66	5.66
Kurtosis	2.98	2.98	2.98	2.98	2.98	2.98	2.99	2.98	2.98	2.99	2.98	2.99	2.98	2.98	2.98	2.98
Kurt (Excess)	-0.02	-0.02	-0.02	-0.02	-0.02	-0.02	-0.01	-0.02	-0.02	-0.01	-0.02	-0.01	-0.02	-0.02	-0.02	-0.02
Mid Range	62	63.5	63	64	64.5	62	63	63	62	62	65	64.5	64	65.5	64.5	64
MAD	4.5	4.5	4.51	4.5	4.51	4.51	4.5	4.5	4.5	4.5	4.5	4.5	4.5	4.5	4.5	4.51
RMS	64.25	64.25	64.25	64.25	64.25	64.25	64.25	64.25	64.25	64.25	64.25	64.25	64.25	64.25	64.25	64.25
Skewness	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CV	0.09	0.09	0.09	0.09	0.09	0.09	0.09	0.09	0.09	0.09	0.09	0.09	0.09	0.09	0.09	0.09

*Median is always 64, and all decimal values are rounded to 1 or 2 decimal digits, or the whole number if very close to the whole number (See the descriptive statistics files for exact decimals).

Results Interpretation

Restating the hypothesis for clarity: “The mean of the differences between the original intermediate ciphertext and the intermediate ciphertext encrypted by the bit flipped keys will become within ± 1 of the median of 64 bits after the 1st cycle of encryption.”

The hypothesis was correct, the mean of the differences did enter that specified range after the 1st cycle. While the hypothesis made no mention of its potential behavior after the 1st cycle, it did actually stay within that range during the entire rest of the cycles. Given the results of the “PAE Each Cycle” test, I would have assumed that the mean and range would warp quite a bit after each cycle where the Diffusion Slide 2 was applied, however, looking at the resulting statistics after each 4th cycle, this doesn’t appear to be the case in these tests. In fact, the descriptive statistics for the difference distributions remained very consistent from cycle to cycle, differing only by a very small decimal amount. While the results of this test and the previous test look promising for the Key Avalanche Effect and the Plaintext Avalanche Effect, respectively, at this time it hasn’t been verified if this encryption system satisfies the SKAC and SPAC (Strict Key/Plaintext Avalanche Criterion).

--stringzzz, Ghostwarez Co.
03-10-2025