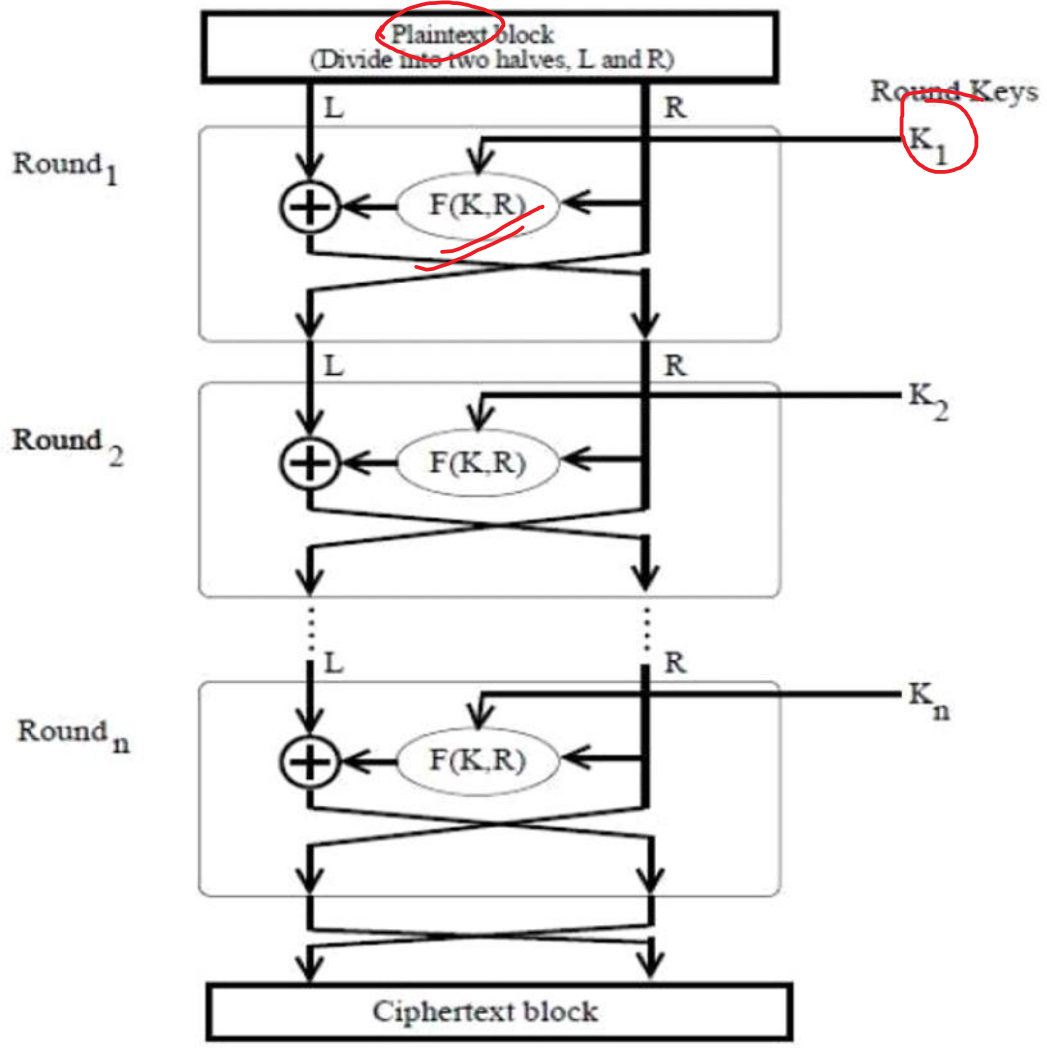
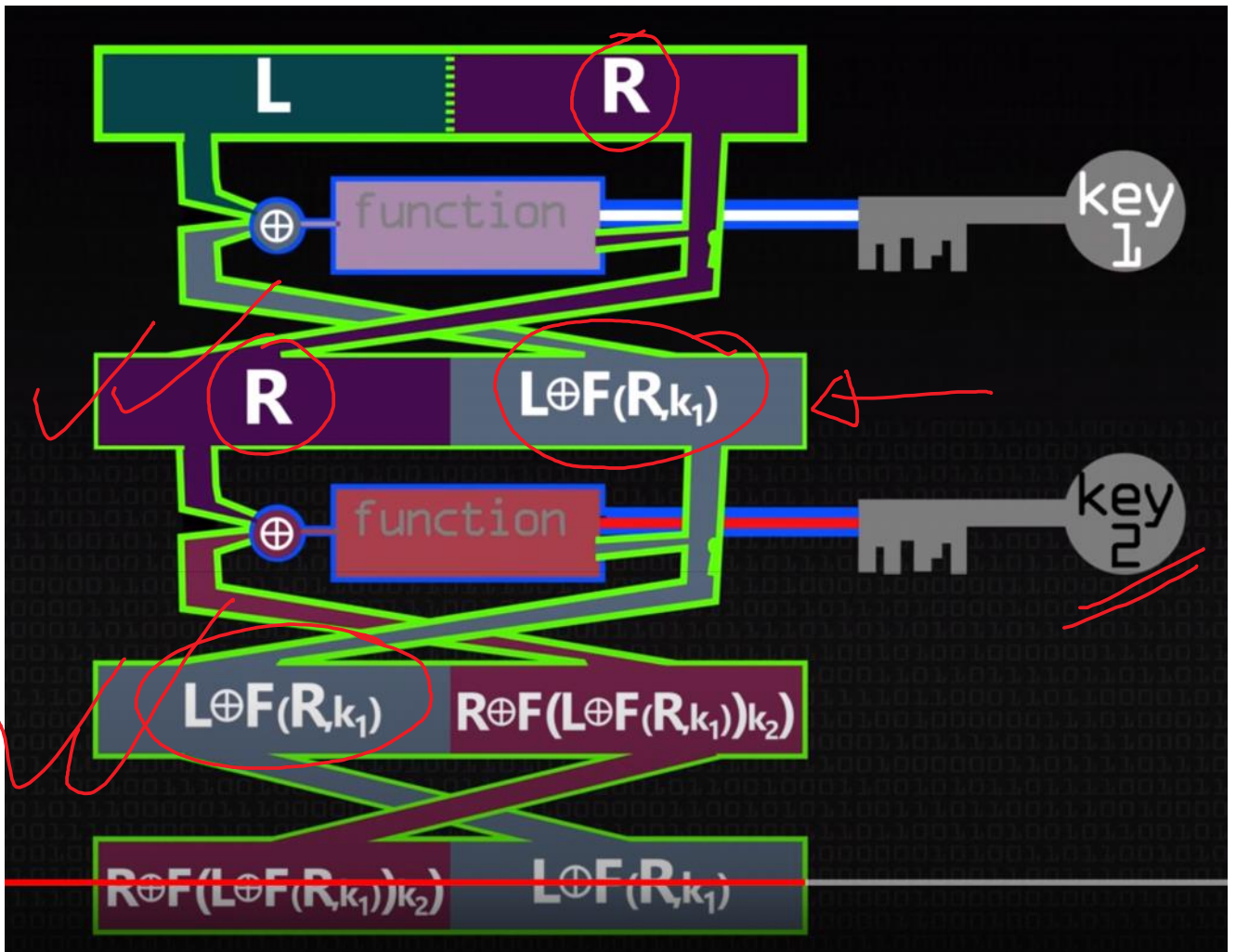


L I am a boy R



Screen clipping taken: 5/31/2020 10:13 AM



Round 1: Left half = L, Right Half = R
 $L \oplus F(R, k_1)$

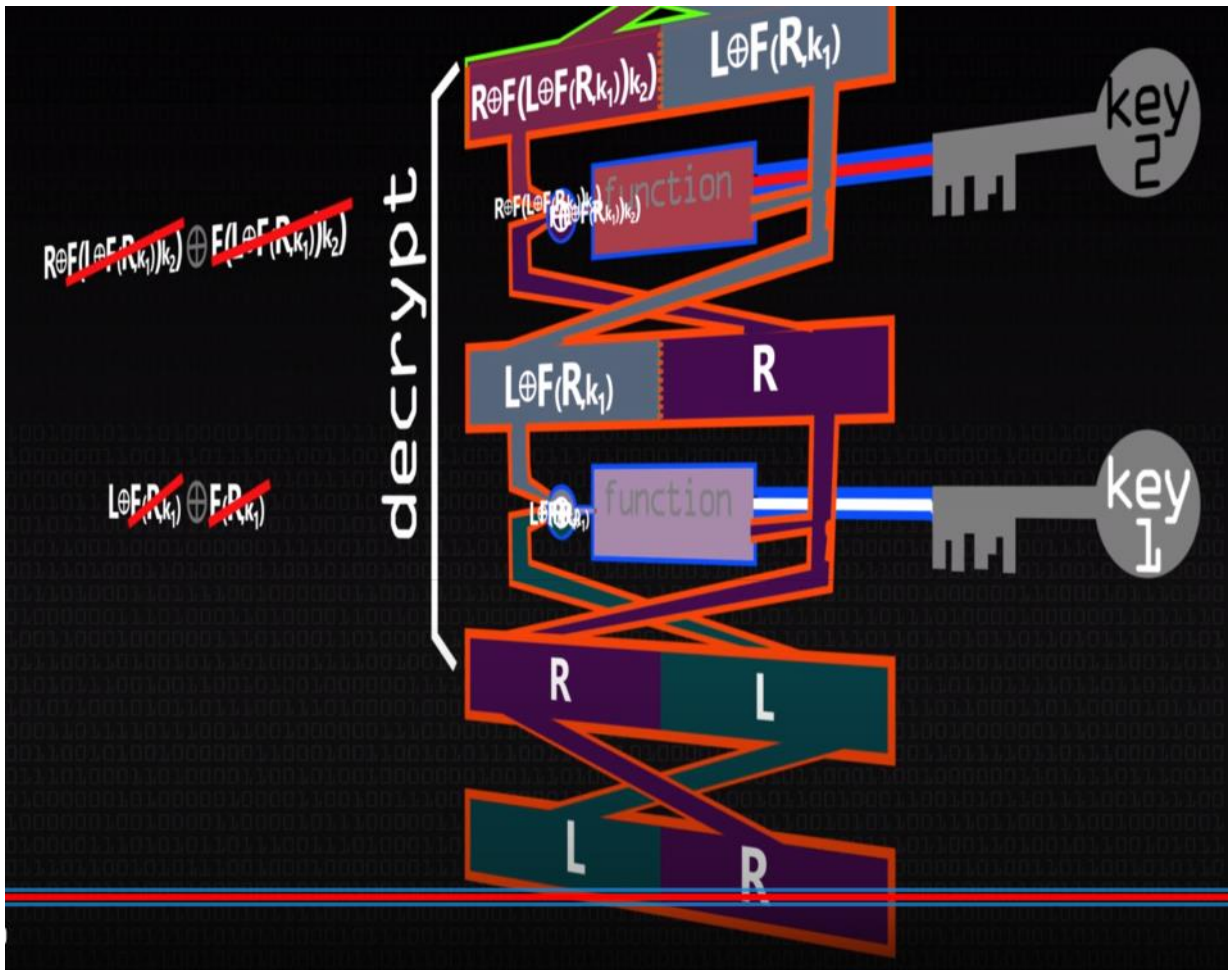
End of the round =>
 Left Half = R, Right Half = $L \oplus F(R, k_1)$

Round 2:
 Left Half = R, Right Half = $L \oplus F(R, k_1)$

End of the round =>
 Left Half = $L \oplus F(R, k_1)$,
 Right Half = $R \oplus F(L \oplus F(R, k_1), k_2)$

Let's assume there WAS NO Round 3. So, the ciphertext was
 $R \oplus F(L \oplus F(R, k_1), k_2) \parallel L \oplus F(R, k_1)$

DECRYPTION:



Round 1:

Left Hand = $R \oplus F(L \oplus F(R, k_1), k_2)$

Right Hand = $L \oplus F(R, k_1)$

At the end of Round 1:

Left Hand = $L \oplus F(R, k_1)$

Right Hand = $R \oplus F(L \oplus F(R, k_1), k_2)$

$XOR \ F(L \oplus F(R, k_1), k_2) = R$

Round 2:

Left Hand = $L \oplus F(R, k_1)$

Right Hand = R

At the end of Round 2:

Left Hand = R

Right Hand = $L \oplus F(R, k_1) \oplus F(R, k_1)$

$= L$

SWAP: Plaintext is L R