

```

Key  2b7e151628aed2a6abf7158809cf4f3c  (16 bytes)
L    7df76b0c1ab899b33e42f047b91b546f  (16 bytes)
      /* since  $L = \text{AES}(\text{Key}, 0000\dots0000)$  */
L · u fbeed618357133667c85e08f7236a8de  (16 bytes)
      /* since  $\text{msb}(L) = 0$  and thus,  $L \cdot u = L \ll 1$  */
L · u2 f7ddac306ae266ccf90bc11ee46d513b  (16 bytes)
      /* since  $\text{msb}(L \cdot u) = 1$  and thus,
       $L \cdot u^2 = ((L \cdot u) \ll 1) \oplus 0000\dots0087$  */

```

