AES – Galois Counter Mode
Crib Dragging Attack
(*Known Plaintext Attack*)