

CMSC 414: HW 1

-
1. (text 3.3) In DES, how many keys, on the average, encrypt a particular plaintext block to a particular ciphertext block.
-
2. (text 3.5) Suppose the DES mangler function maps every 32-bit value to zero, regardless of the value of its input. What function would DES then compute?
-
3. (text 3.8) Why is a DES weak key its own inverse? (Hint: DES encryption and decryption are similar once the per-round keys are generated.)
-
4. (text 4.1) What pseudo-random block stream is generated by 64-bit OFB with a weak DES key.
-
5. (text 4.2) The pseudo-random stream of blocks generated by 64-bit OFB (i.e., $K\{IV\}$, $K\{K\{IV\}\}$, ...) must eventually repeat. Will $K\{IV\}$ necessarily be the first block to be repeated. Explain.
-