CMSC 414: HW 1 Solution and Grading

Solution

---

1. In DES, how many plaintext blocks, on the average, are encrypted to the same ciphertext block by a given key.

DES has 56-bit keys, 64-bit plaintext blocks, and 64-bit ciphertext blocks.
The number of ciphertext blocks equals the number of plaintext blocks.
DES is a 1-1 mapping between ciphertext blocks and plaintext blocks.
So 1 plaintext block is mapped to a given ciphertext block by any given key.

---

2. (text 3.3) In DES, how many keys, on the average, encrypt a particular plaintext block to a particular ciphertext block.

Each key maps 2^{64} plaintext blocks to 2^{64} ciphertext blocks.
So it has a $1/2^{64}$ chance of mapping a plaintext block b to a ciphertext block c.
There are 2^{56} keys, so the total probability of mapping p to c is $(1/2^{64}) \cdot 2^{56} = 1/256$.

---

3. (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?

DES does the following (see text figure 3-2):

- Initial permutation
- 16 DES rounds
- Swap left and right halves
- final permutation (inverse of initial permuation)

With a mangler function that outputs 0 always, each DES round just swaps L and R.
So after 16 (even number) DES rounds, the initial 64-bit word would be unchanged.
So DES would do the following:

- Initial permutation
- Swap left and right halves
- final permutation

Based on the initial permutation, the net result is a permutation that interchanges consecutive even and odd bits.
[If the swap were not there, DES would have no affect at all.]

---

4. (text 4.1) What pseudo-random block stream is generated by 64-bit OFB with a weak DES key.

The OFB pad sequence is $E_x(IV)$, $E_x(E_x(IV))$, $E_x(E_x(E_x(IV)))$, ...
A weak key is its own inverse, i.e., for any block b: $E_x(b) = D_x(b)$. So $E_x(E_x(b)) = b$.
So the resulting OFB pad sequence is $E_x(IV)$, IV, $E_x(IV)$, IV, ····

---

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.

K{IV} will be the first block to repeat.
Proof:
For brevity, let b_i denote the i-fold encryption of IV.
So the pad sequence is b_1, b_2, b_1, ..., where b_{i+1} is the encryption of b_i and b_i is the decryption of b_{i+1} (because decryption is the inverse of encryption).
Let b_k be the first repeat element and let $b_k=b_j$ where $j < k$.

- If j=1 we are done.
- If $j > 1$ then $b_{j-1} = b_{k-1}$ (since $b_j = b_k$). So b_k is not the first repeat element. Contradiction.

So $b_k = b_1$.

Note that we only needed the fact that encryption is reversable.

Grading

Problems graded:
Problems 3 and 5 were graded, each out of 5 points.

Grading key for problem 3:
1 point for just writing something.
2 points for saying that each DES round just exchanges L and R.
3 points for saying that each DES round just exchanges L and R,
so after 16 (even) rounds, there is no change.
4 points: if you miss the final L-R swap and just say that DES has no effect.
5 points: if you get the answer.

Grading key for problem 5:
1 point for just writing something.
2 points for saying K{IV} is the first block to be repeated.
3-5 points for the proof:

a) b_k is decryption of b_{k+1}, and b_{k+1} is encryption of b_k
b) if $b_k = b_j$, $k > j$, then $b_{k-1} = b_{j-1}$
c) b_1 is the first one to be repeated in the sequence $b_1, b_2, \cdots$

Missing any of (a), (b) or (c) will lose one point.
Correct proof but saying IV is first repeated block instead of K{IV} will lose one point.