

## CMSC 414: Hw 1 Solution and Grading Guidelines

- 
1. (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  $(1/2^{64}) \cdot 2^{56} = 1/256$ .

- 
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?

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

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

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.]

- 
3. (text 3.8) Why is a DES weak key its own inverse? (Hint: DES encryption and decryption are the same once the per-round keys are generated.)

For a DES weak key, each of  $C_0$  and  $D_0$  is equal to all ones or all zeros. Each  $C_i$  is a permutation of  $C_0$ , so each  $C_i$  equals  $C_0$ . Each  $D_i$  is a permutation of  $D_0$ , so each  $D_i$  equals  $D_0$ .  $K_i$  depends only on  $C_i$  and  $D_i$ , so all  $K_i$ 's are equal. So the sequence  $K_1, K_2, \dots, K_{16}$  is the same as the sequence  $K_{16}, K_{15}, \dots, K_1$ . So the encryption operation is the same as the decryption operation (because decryption is the same as encryption but with the keys in reverse order).

**Explanation of the hint:** In case the hint is not clear, here are more details.

```
DES_encryption {
  initial permutation to get  $L_0|R_0$  from data block
  for  $n=1, 2, \dots, 16$  do  $L_n|R_n := E_n(K_n, L_{n-1}|R_{n-1})$ ,
    where  $E_n$  denotes the computation of encryption round  $n$ .
  swap left and right halves, yielding  $R_{16}|L_{16}$ 
  inverse of initial permutation, yielding cipher block
}
```

```

DES_decryption {
  initial permutation of cipher block, yielding  $R_{16}|L_{16}$ 
  for  $n = 16, 15, \dots, 1$  do  $R_{n-1}|L_{n-1} := D_n(K_n, R_n|L_n)$ ,
    where  $D_n$  denotes the computation of decryption round  $n$ .
  swap left and right halves, yielding  $L_0|R_0$ 
  inverse of initial permutation, yielding data block.
}

```

Section 3.3.4 explains that decryption round  $n$  is identical to encryption round  $n$  with  $L_n$  and  $R_n$  swapped, i.e.,  $D_n(K_n, R_n|L_n)$  equals  $E_n(K_n, L_n|R_n)$ . Substituting this in DES\_decryption, we see that the only difference between encryption and decryption is that the  $K_n$ 's are used in the opposite order. So there is no difference if all the  $K_i$ 's are the same.

- 
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  $E_x(IV), E_x(E_x(IV)), E_x(E_x(E_x(IV))), \dots$

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  $E_x(IV), IV, E_x(IV), IV, \dots$

- 
5. (text 4.2) The pseudo-random stream of blocks generated by 64-bit OFB (i.e.,  $K\{IV\}, K\{K\{IV\}\}, \dots$ ) 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  $b_1, b_2, b_3, \dots$ , 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 reversible.

---

## Grading Guidelines

---

Problems graded:

Problems 2 and 5 were graded, each out of 5 points.

### **Grading key for problem 2:**

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  $b_1, b_2, \dots$

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.

---