Introduction to Cryptography: Assignment 4

Group number 57

Elwin Tamminga
s1013846

Lucas van der Laan
s1047485

1

(a) We make two online queries with a plaintext and the complement of the plaintext to the encryption device.

(b) If we make a query with the complement of a plaintext, then the complement of the resulting ciphertext should be the same as taking the ciphertext output of the complement of the key and the normal plaintext.

(c) We only need to test keys ending with 0, because using the complement of the plaintext we can also test the complement of the keys at the same time (which are the other keys ending with 1). So the set of keys K are all 56 bit keys ending with 0 (2^{55} keys in total).

(d) 1. Make two online queries to the encryption device with a plaintext P and it's complement $\overline{P}$ and remember both outputs C and $\overline{C}$.

2. Iterate through each key of the set of keys defined in (c), and for each key get the output of $\text{DES}_K(P)$.

3. If the output of $\text{DES}_K(P)$ matches the output of the encryption device C, then we found that our guessed key is the key K.

   If the complement of the output matches the output of the encryption device $\overline{C}$ (when we used $\overline{P}$ as input), then we found the complement of the real key $\overline{K}$, so then we can get the real key by getting the complement of the key we guessed.

(e) There are 2^{55} possible keys using the adapted key search, so the security strength is 55 bits.

2

(a)

- For ECB and CBC, they use blocks of 16 bytes. If the message does not fit in the last block, then padding is added at the end of the message. 900 bits fits in 8 blocks of 16 bytes, so the length of the ciphertext is $8 * 16 = 128$ bytes.
- For OFB and CTR, padding is not required, because the last part of the plaintext (P_l) is XORed with the first $|P_l|$ bits of the last keystream block and thus the ciphertext length is always the same as the plaintext length, in this case 900 bits.

(b)

- In the third block of the ciphertext one bit is flipped. In ECB this means that for m' half of the bits are flipped from 257 until 384 for a total of 64 bits.
- In CBC, m' also has bits flipped in the third block like ECB, but there is also a flipped bit in the fourth block at the position that the bit was flipped in C_3, which is m'_{428}.
- OFB and CTR are tolerant to bit flips, which means that only one bit is flipped in m' when one bit is flipped in the ciphertext, because the ciphertext is XORed with the output of the block cipher and the ciphertext of the previous block is not used in the next block. So m' only has a bit flipped at m'_{300}.