NTNU Department of Information Security and Communication Technology

TTM4135 Applied Cryptography and Network Security
Semester Spring, 2023

Worksheet 3: Block ciphers and modes of operation

QUESTION 1

Review the definitions of the following concepts. They are things that you would be expected to know in a quiz or exam.

(a) confusion and diffusion;
(b) product cipher and iterated cipher;
(c) Feistel cipher;
(d) substitution-permutation network;
(e) ECB mode;
(f) CBC mode;
(g) CTR mode;
(h) true random number generator (TRNG) and pseudorandom number generator (PRNG).

QUESTION 2

Suppose a certain system can perform 2^{55} trial encryptions of a DES block in 1 second.

(a) Assuming that computational power remains the same, how may years should it take, on average, for this system to perform a brute force attack on two-key triple DES?

(b) Moore's law says that computers double their computational power every two years. Assuming this continues for ever, how long will it be before two-key triple DES can be broken within one day?

QUESTION 3

Consider a block cipher with encryption function E and decryption function D. Suppose that this cipher is *linear* with respect to messages:

$$E(M_1, K) \oplus E(M_2, K) = E(M_1 \oplus M_2, K)$$

for any messages M_1 and M_2 and any fixed key K. Suppose that the block size is 128 bits. Show that an attacker can use a chosen ciphertext attack, with just 128 chosen ciphertexts, to easily decrypt any message.

QUESTION 4

Consider the following two (toy) ciphers. Both ciphers are two-round iterated block ciphers with a block length of 8 bits and a key length of 8 bits. In each case work through the steps required to encrypt the plaintext block $P = 01010101$ using key $K = 11000011$.

(a) A substitution-permutation in which each S-box operates on sub-blocks of 2 bits. Thus $m = 4$ and $l = 2$.

cont/...

- The permutation π_S is defined by the following table:

Input block	00	01	10	11
Output block	10	00	01	11

- The permutation π_P is defined by the following table where the block bits are labelled from 0 to 7:

Input position	0	1	2	3	4	5	6	7
Output position	3	6	0	5	2	1	7	4

- The key schedule is defined by $K_1 = K$ and $K_2 = K_1 << 1$ where $<< 1$ denotes cyclic shift left by one position.

(b) A Feistel cipher with:

- f function defined by $f(X, K_i) = X \vee K_i$ for any half block X and subkey K_i. Here the $\vee$ operation is done on each bit separately so that if $K_i = (k_0, k_1, k_2, k_3)$ and $X = (x_0, x_1, x_2, x_3)$ then $f(X, K_i) = (k_0 \vee x_0), (k_1 \vee x_1), (k_2 \vee x_2), (k_3 \vee x_3)$.
- key schedule defined by K_1 is the 4 leftmost bits of K and K_2 is the 4 rightmost bits of K.

QUESTION 5

Consider the use of double encryption applied to the AES algorithm with two 128-bit keys. How much storage and computation would be required to execute a *meet-in-the-middle* attack (as described for DES in the lecture)?

QUESTION 6

Suppose we want to encrypt more than one block of random bits using ECB mode with a block cipher, but without padding. This can be achieved with a technique known as *ciphertext stealing*. For example, suppose we encrypt a 200-bit random key using AES in ECB mode with key K. The plaintext is two blocks M_1, M_2 where M_2 is a 72-bit 'short' block. Then we compute:

$$\begin{aligned} C_2 \parallel J &= E(M_1, K) \\ C_1 &= E(M_2 \parallel J, K) \end{aligned}$$

and send (C_1, C_2) to the receiver. Here J is a 56 bit random value which is never transmitted.

(a) What is the length of the ciphertext?
(b) Show how the message can be decrypted back to the original plaintext.

QUESTION 7

Suppose that the IV for CBC mode is chosen to be a counter instead of a random value (as it should be). Show that an attacker can gain information regarding the first block of a ciphertext by using a chosen plaintext attack. More specifically, show that the attacker can check whether C has first plaintext block equal to a particular block P_0 by asking for the ciphertext of a specific plaintext.

cont/...

QUESTION 8

Compare the following three modes of operation for block ciphers: ECB, CBC and CTR. Suppose that:

- AES is used as the block cipher;
- the padding method mentioned in the lectures slides (Lecture 6, Slide 7) is used (where needed);
- the nonce used in counter mode has 96 bits.

How many bits need to be transmitted in each of these three cases if the input plaintext has 104 bits?

QUESTION 9

The CTR-DRBG described in slides 28–30 of Lecture 6 keeps a counter state V and a key K in memory. The pair (K, V) is initialised, and occasionally updated, with a random seed using the Initialise and Reseed functions. In this question we assume that 128-bit keys and blocks are used (such as in AES) and also that each call to the Generate function outputs 10 blocks (1280 bits). Suppose that an attacker obtains the current (K, V) value after 5 blocks have been generated during a call to Generate.

(a) Explain why this attacker can obtain all of the 1280 bits generated from that call to Generate.

(b) Show further that the attacker can obtain the output from all future calls to generate until Reseed is called.

(c) Explain why this attacker cannot obtain the output from any previous calls to Generate, even if Reseed has never been called.