IDATT2503 - Cryptography - Autumn 2025

Cryptography Assignment 2

Task 1 - AES a little history

Since May 26, 2002, the AES (Advanced Encryption Standard) describes the official standard of the US government, replacing DES.
Search the net to find relevant information.

1. The evolutionary history of AES differs from that of DES. Describe how the processes of establishing the two standards differ.

2. What is the name of the *algorithm* that is known as AES and who developed this algorithm? Why was it by many a surprise that it was this that was chosen to be the new standard?

Task 2

In this exercise we shall look at *diffusion* and *confusion* of some ciphers. Use 128 bits for both messages and keys. Use the keys

$$K_1 = 0123456789ABCDEF0123456789ABCDEF$$
$$K_2 = 1123456789ABCDEF0123456789ABCDEF$$

written in hexadecimal (not very random!) and plaintexts also in hexadecimal:

$$x_1 = 01000000000000000000000000000000$$
$$x_2 = 02000000000000000000000000000000$$

The ciphers we are to consider are the following

A One-time pad (XOR) (see lecture notes)

B Affine cipher, use same key for both compoenents (see lecture notes)

C One round of AES

D Full AES.

For AES, you can use `https://www.cryptool.org/en/cto/aes-step-by-step`, use standard settings, 128-bits key, and no chaining.

a) For each cipher above, encrypt both x_1 and x_2, using the key K_1 and compare the results, with regards to *diffusion*.

b) For each cipher, encrypt x_1 using K_1 and K_2, and compare the results. How many bits change?

Task 3

Do the challenges on `https://www.cryptohack.org/challenges/aes/`, up to "Bringing it all together".
Write down the captured flags, and submit the code (its in Python).

Task 4

(exercise 4.2 in William Stalling) Consider a Feistel cipher composed of sixteen rounds with a block length of 128 bits and a key length of 128 bits. Suppose for a given key k, the key scheduling algorithm determines values for the first eight round keys $k_1, k_2, \ldots, k_8$ and then sets

$$k_9 = k_8, k_{10} = k_7, k_{11} = k_6, \ldots, k_{16} = k_1.$$

Suppose you have a cipher text c. Explain how, with access to an **encryption** oracle, you can decrypt c and determine m using a single oracle query. This shows that such a cipher is vulnerable to a chosen plaintext attack. (An encryption oracle can be thought of as a device that, when given a plaintext, returns the corresponding ciphertext. The internal details are not known to you and you cannot break open the device. You can only gain information from the oracle by making queries to it and observing its responses.)