PWr, Inf. algo. CRYPTOGRAPHY, 2022 assignments list # 4, 24.3.2022

1. Assume that you have a block encryption scheme with block length 128. However, what you need to encrypt, are the messages of the length m which may be anything between 129 up to 256 bits.

   How to do it? Is it possible without extending the ciphertext length beyond the length m? (The answer to this question is not obvious, but the solution is beautiful.)

2. Read the key schedule of AES (see e.g. the white paper by Daemen and Rijmen). Answer the following questions:

   - is it true that each subkey bit equals some bit of the encryption key?
   - for a few key bits, trace which subkey bits are influenced by a given bit of the encryption key

   Consider these problems for the DES key schedule (again, find the key schedule algorithm in the internet).

3. Assume that Alice and Bob share a key K and exchange messages encrypted with K. An adversary Mallet starts an attack and for a given pair (plaintext,ciphertext) can find the encryption key by a brute force attack that costs 10.000.000 USD.

   Propose a method that protects against such attacks having in mind that Mallet's total budget is 100.000.000 USD. The solution must be as simple as possible and attractive from the practical point of view. We assume that there is no second channel between Alice and Bob, they cannot use asymmetric cryptography, ... We have to use the tools already discussed during the lecture.

4. Given the basic description of AES from the lecture (the algebraic one, not via lookup tables), describe how to construct the AES decryption process.

5. Again, find a description of the DES algorithm. Assume by now that it consists of 2 rounds (you may try also 3 rounds – it is then more interesting). Describe a full scenario of the differential cryptanalysis in this case. Do not go into details of the S-boxes. It is enough to specify which properties of the S-boxes will be used by your attack.

/-/ Mirosław Kutyłowski