PWr, Inf. algo. CRYPTOGRAPHY, 2022 assignments list # 5, 31.3.2022 (updated)

1. Differential cryptanalysis requires to examine plaintexts with a given differences on a given positions. So if you perform a CPA attack, you can prepare the pairs in this way.

   What to do if the attack is a known plaintext attack (KPA): you get a large number of pairs (plaintext,ciphertext), but you cannot choose them. Is differential cryptanalysis still applicable?

2. Explain in detail how to use differential cryptanalysis together with faults to break AES. By generating fault we mean flipping a bit on a chosen position of a chosen intermediate value of the computation.

   Can linear cryptanalysis be directly applied together with faults of the same kind? Could linear cryptanalysis be simplified in case that you may set certain bits of intermediate values to 1?

3. For each of the block encryption modes discussed during the lecture:

   (a) check what happens with the plaintext, if just one bit is flipped in the ciphertext,

   (b) check what happens with the ciphertext, if just one bit is flipped in the plaintext,

   (c) what would be the consequences of repeating the same initial vector IV (provided that IV is used)?

4. During the lecture we have shortly discussed why ECB encryption mode is a wrong choice for encrypting data concerning bank operations to be executed by the recipient server.

   So is CBC a good choice in this case? You do not know the exact format of the transmission, size of the records, etc. So is CBC a good choice regardless what data format we use?

5. [homework] Encrypt (symetrically) this list with GnuPG software. Use the key starting with your student number (pad with bits zero if necessary). Which encryption mode has been used?

6. For disk encryption none of the encryption modes discussed during the lecture is used in a pure form. Find in the literature how disk encryption is organized. Deduce why it has been designed in this way.

/-/ Mirosław Kutyłowski