Wrocław University of Technology, WPPT 27.10.09

CRYPTOGRAPHY AND SECURITY, 2009 Assignments, list # 3

1. Derive the decryption algorithm of RC5. Show that RC5 is an algorithm that has the Feistel structure.

2. Assume that we change a single bit in the string $S[1]$ used by RC5. How does it change the intermediate data computed during a few first rounds. Discuss the rate in which the changes propagate.

3. Assume that through a bad hardware implementation it is possible to determine which circular shifts are performed at each round of RC5. Does it leak the secret key?

4. Generalize attack on double-encryption to triple-encryption scheme. Estimate complexity of this attack.

5. Generalize Feistel method to scheme using 4 blocks instead of 2. Which method seems to be most reasonable?

6. How to design permutations used in DES so that avalanche effect is strong? Estimate the number of rounds necessary for dissemination of changes.

7. Some DES keys are called weak. One of the reasons could be that the subkeys generated are the same, or there are just a few different subkeys. Does it potentially weaken the encryption? Find some keys of this type.

8. Prove that
$$\mathrm{DES}_{\overline{K}}(\overline{X}) = \overline{\mathrm{DES}_K(X)}$$
for each X and K, where $\overline{Y}$ denotes Y after flipping its each bit.

9. Consider the S-box S_5 of DES. (For the specification of Sboxes see the NIST publication: `http://www.itl.nist.gov/fipspubs/fip46-2.htm`.)
For each $x \in \{0,1\}^6$ and $y \in \{0,1\}^4$, for a random $z \in \{0,1\}^6$, compute the probability that
$$S_5(z) \text{ XOR } S_5(z \text{ XOR } x) = y$$

/-/ Mirosław Kutyłowski and Filip Zagórski