Wrocław University of Technology, WPPT 9.10.13

CRYPTOGRAPHY, 2013 Assignments, list # 2

1. One of the major properties of A5/1 is that it is hard to reconstruct its previous state. Estimate the number of possible previous states one step before the observed internal state of an LFSR. How does this influence a "brute force" attack on GSM use of A5/1? Recall that in GSM first the shared secret key is loaded into LFSR together with the frame number (parameter), then the generator is run for some time but the output is discarded, then a relatively small number of output bits are used, before the generator is restarted with a new frame number.
   Could you break a version A5/1 which uses LFSR registers of length 11, 12 and 13 with a standard computer? Estimate complexity of the attack.
   Why only a limited number of bits is used for each frame number? Does it improve security of the system?

2. Assume that you are holding an RC4 encryption device and you can influence it so that an arbitrary number of bytes is initially replaced as you want. Derive the secret key used by the device.

3. Long long time ago, the Romans used substitution ciphers. Simply, there was a secret permutation π (sometimes quite simple) and the ith character from the alphabet was replaced by the character at position $\pi(i)$ in the alphabet. As you have already noticed during the lecture, no π can help to resist such attacks.

   Discuss influence of the alphabet size. Would Chinese alphabet be secure against such an attack (more than thousands characters in standard texts)? For those (few) who do not read Chinese: a word in the language typically consists of 2 characters, each denoting a single syllable. The syllables typically bring some meaning. Some characters are used more frequently.

4. Assume that an adversary can determine the IV used in CBC encryption. What are potential dangers of this situation?

5. Discuss what happens if a certain part of CBC ciphertext becomes destroyed or lost. Can we decrypt the rest? Consider all error scenarios.

6. CFB encryption mode is given by the equation: $C_i = E(C_{i-1}, K)$ xor M_i. What is the behavior of CFB in case of transmission errors? What are the advantages and disadvantages of CFB in comparison with ECB and CBC?

7. Design an encryption method for file systems such that

   - without an encryption key one cannot determine if two blocks of plaintext are identical,
   - it is possible to replace each single block of plaintext by replacing a single block of the ciphertext.

   Note that neither ECB nor CBC fulfils these requirements.

/-/ Mirosław Kutyłowski and Maciej Gebala