Programming Project 3

Course 01435: Practical Cryptanalysis
June 2016

Andrey Bogdanov
anbog@dtu.dk

1 Remarks

- hand in via campusnet before Wednesday, June 22, 11:59 pm (no print out necessary)
- work alone or in groups of up to 4 people
- free choice of programming language
- the code should be well-structured and contain a sufficient amount of comments such that it can be understand be an external programmer
- some written documentation of the code is necessary and you have to be able to explain every single detail when asked
- it is your responsiblity to be able to demonstrate your programme at the colloquium (make sure that a computer is available your programme runs on etc)

Programming Project (P)

Under file sharing on CampusNet, you can find the file `ciphertext_project3.bin`. This is a file which has been encrypted using AES-128, the U.S. encryption standard. It is your task to decrypt this file, assuming that you know the following:

- The 128-bit key was generated in the period June 22-28, 2014, using the GCC generator described in the lecture (update lecture slides too?):
  1. The inner state s_0 of the generator is initialised to the current system time (seconds since 00:00:00 UTC on January 1, 1970).
  2. The update function has the form

$$s_i = (s_{i-1} \cdot 1103515245) + 12345) \bmod 2^{31}$$

3. Each key byte $k[0], \ldots, k[15]$ is generated by first running the update function and then taking the 8 least significant bits of the current inner state.

- The text was encrypted using AES-128 in ECB mode (meaning that the plaintext was split into blocks of 16 bytes and processed blockwise during encryption). The plaintext length is a multiple of the block size and no padding was applied.
- The text is rather recent, from a newspaper and in (British) English, using normal text format (small/capital letters, whitespaces, punctuation etc.). It has something to do with the NSA, so you might want to use certain names.

Use your knowledge from the lecture to break this cipher using a clever key search given the low entropy of the key material.

Important: Hand in the plaintext in a seperate `.txt` or `.pdf` file next to your program.

Note: The ciphertext file is a collection of pretty random-looking bytes. In particular, it contains the byte that is interpreted as 'EOF' (end of file) by many file handlers. So check whether your program stops parsing the file too early; if it does, it has probably encountered the wrong 'EOF' symbol. In this case, you'll have to find a workaround (e.g. you can read in the file in binary format in C) - all tricks are allowed as long as they work.