Crypto

Lab nr 1
due date 13 III 2015

Assignment 1 (5 pts.) Write a program which takes as an input a message m (in fact: a path to a file containing a message m) and returns a cryptogram of the message. The program needs to support the following encryption schemes: AES-CTR, Salsa20, RC4.

A key needs to be stored in a keystore (*e.g.,* use Boucy Castle).

Assignment 2 (10 pts.) You have intercepted 17 cryptograms (the cryptograms are on the course webpage). You know that each of the messages was encrypted by a stream cipher and the same key was used every time *i.e.,* $c_i = \mathsf{Enc}(\mathsf{k}, \mathsf{m_i}) = m_i \oplus G(k)$ for $i = 1 \dots 17$, where G is a PRNG and k is the secret key. The length of each c_i equals to the length of the corresponding m_i – the output of $G(k)$ is trimmed to the appropriate length.

Write a program which on input gets l cryptogram encrypted by a stream cipher with the same key and outputs the corresponding plaintext.

You can use a program from the previous assignment to generate test data.

Check how your program behaves for:

- different lengths of cryptogram,
- different number of cryptogram, for $l = 1, 2, 3, 4, \dots$ (at what point it starts to work?)
- different stream ciphers,
- different character encoding ASCII/UTF-8/ISO-8859-2?