Worksheet 3 (due Wednesday June 22, 11:59 pm)

Course 01435: Practical Cryptanalysis
June 2016

Andrey Bogdanov
anbog@dtu.dk

Introductory Remarks

All comments from worksheet 0 apply.

Weakest Link Principle

Recommended Reading

The lecture briefly touches on areas that are very deep. For example, the whole book "Security Engineering" by Ross Anderson (1st edition available online at `http://www.cl.cam.ac.uk/~rja14/book.html`; you have to scroll down a bit) implicitly discusses the weakest link principle for a variety of applications.

The security model for the pseudo-random number generator is inspired by the paper "A model and Architecture for PseudoRandom Generation and Applications to /dev/random" by Barak and Halevi, which is available from CampusNet.

The concept of entropy is discussed in many books on cryptography and almost all books on coding theory. As usual, you can also find plenty of resources on the web, see e.g. `http://en.wikipedia.org/wiki/Information_entropy`. For the seriously interested, Shannon's original articles (available from CampusNet) are surprisingly readable.

Exercises

Exercise 16: A physical "random" bit generator is measured to output a 0 with probability 0.45 and a 1 with probability 0.55. A key is generated by concatenating 40 output bits from this generator. What is the entropy of the resulting 40-bit key?

Exercise 17 (P): We have learned that the entropy of a key can be interpreted as the average number of bits required to store it if perfect compression is used. Of course, the same holds for the entropy of plaintexts.

Using the plaintext characteristics (frequency of letters for the English language), derive the average number of bits required to store one letter of British English if perfect compression is used?