SSN Practicum
Week 2

E.P. Schatborn
A. van Inge
N. Sijm

7 November 2011

1 Introduction

In this assignment you will use Cryptool. Download the current version (so not 2.0 beta) from `http://www.cryptool.com`. Install Cryptool in your Windows environment. After installation you should find, among other entries, a menu entry named "Script". The document contains very useful background information for the lectures.

2 Assignment DES/AES

Watch the DES animation and the AES animation, and read the following publications:

- `http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf`
- `http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf`

1. What is known about cryptoanalytic attacks on AES?

3 Assignment RSA

Download and study the RSA FAQ at `http://www.rsasecurity.com/rsalabs/node.asp?id=2152`.

2. How objective is this RSA FAQ? Explain your thoughts.