SSN Lab Assignment: Modern Crypto

C.Dumitru J. van der Ham M. Pouw* U. Seddigh

Feedback deadline:
September 21, 2017 10:00 CET

1 DES

The Cryptool 1.x suite contains a simulator for the DES encryption algorithm in the menu "Individual Procedures / Visualization of Algorithms / DES". Watch this animation.

1. Next, use the DES simulator DEScalc.jar[1] in the "SSN Lab 3" directory on the Desktop of the Virtual Box image (taken from `http://lpb.canb.auug.org.au/adfa/src/DEScalc/`). Step through the process of encrypting your name with the key `0x0101010101010101` and write the internal state of the device at the 8th round.
2. Inspect the key schedule phase for the given key and explain how the sub keys are generated for each of the 16 steps.
3. Comment on the behavior of DES when using the given key.

2 AES

The Cryptool 1.x suite contains an animation for the AES encryption algorithm. Watch the whole animation of AES using the `Rijndael Animation.exe` utility.

4. Identify the Shannon diffusion element(s).
5. Also identify the Shannon confusion element(s).

*mick@os3.nl

[1] This Java applet can refuse to quit, you can close it using the task manager.