SSN Lab Assignment: DES, AES and Entropy [Bonus]*

V. Breider R. Vermeulen†

Feedback deadline:
Monday September 25, 2023 10:00 CET

1 DES

In the "SSN Lab 3" directory on the Desktop of the Virtual Box image you will find the Cryptool 1. suite. This suite contains a simulator for the DES encryption algorithm in the menu "Individual Procedures / Visualization of Algorithms / DES". Watch this animation.

Questions

1. Next, use the DES simulator DEScalc.jar[1] also in the "SSN Lab 3" directory (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).

3 Entropy

Entropy is an important concept in cryptography. Actually it is two concepts. First, it can refer to the randomness of data used in cryptographic protocols, for example, key parameters or nonces. If these are not random enough, i.e., predictable, an attacker may be able to guess them and thus break your system.

It can also refer to the information density of the contents of e.g. a file. If you look at the 8-bit values that are used to store a text, the first 3 bits are hardly used because the values are all in the printable ASCII range. This is different for JPEG and other highly efficiently encoded files.

*Based on earlier work by J. van der Ham. U. Odyurt. P. Prjevara. Version September 16, 2024

†vincent@os3.nl,labteachers@os3.nl

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

6. Linux has two sources of random data: `/dev/random` and `/dev/urandom`. What is the difference between these two sources?

7. Install `ent` and read its manual page. Run the following command for each `/dev/[u]random` source:

   ```
   dd if=/dev/urandom bs=100k count=1 iflag=fullblock | ent
   ```

   You may need to install `haveged`, an extra source of entropy for the Linux kernel, if your kernel version is lower that 5.6. After that, this functionality is included in the kernel.

8. Explain any difference in Entropy or the Chi-square distribution percentage metric

9. Why would we need the `haveged` service or a HAVEGED-like algorithm in the kernel?

4 Information Density

10. Find some files with the following content, and run the `ent` command on them
    (a) (a long) Text file
    (b) PNG image
    (c) JPEG image
    (d) An AES-encoded version of the text file. *Hint:* `openssl aes-256-cbc`
    (e) An AES-encoded version of the JPEG image

11. Based on these measurements, briefly explain how you can use `ent` to find encrypted data, and what the risks are.