Cryptanalytic world records, summer 2014

DANIEL LOEBENBERGER, KONSTANTIN ZIEGLER

1. Exercise sheet
Hand in solutions until Saturday, 12 April 2014, 23:59:59

Reminder.

- For the course we remind you of the following dates:
  - Lectures: Monday and Thursday 13:00h-14:30h **sharp**, b-it bitmax.
  - Tutorial: Monday 14:45h-16:15h, b-it bitmax.
- A word on the exercises. They are important. Of course, you know that. In order to be admitted to the exam it is necessary that you earned at least 50% of the credits. You need 50% of the marks on the final exam to pass the course. If you do, then as an additional motivation, you will get a bonus for the final exam if you attended the tutorial regularly **and** earned more than 70% or even more than 90% of the credits.

Exercise 1.1 (Secure passwords). (15+5 points)

Consider password with ℓ letters, where each letter was uniformly selected from an alphabet A.

(i) Compute the the required length ℓ such that any password generated uniformly at random has at least 80 bits of security, where

(a) $A = \{0, \ldots, 9\}$ are the Arabic numerals. [1]

(b) $A = \{a, \ldots, z\}$ are lowercase roman letters. [1]

(c) $A = \{a, \ldots, z, A, \ldots, Z\}$ are case-sensitive roman letters. [1]

(d) A are all 94 ASCII printable characters (excluding space). [1]

(e) A is a Diceware word list as found on our course webpage. [1]

(ii) For each of the above alphabets generate such password. Describe detailed how you proceeded and argue why you think the result is indeed drawn uniformly at random from all admissible passwords. [10]

(iii) Generate a human selected password with 40 bits security. Follow here the estimates from NIST Special Publication 800-63, Appendix A, available on our course page. [+5]

Exercise 1.2 (The security of your own password). (5 points)

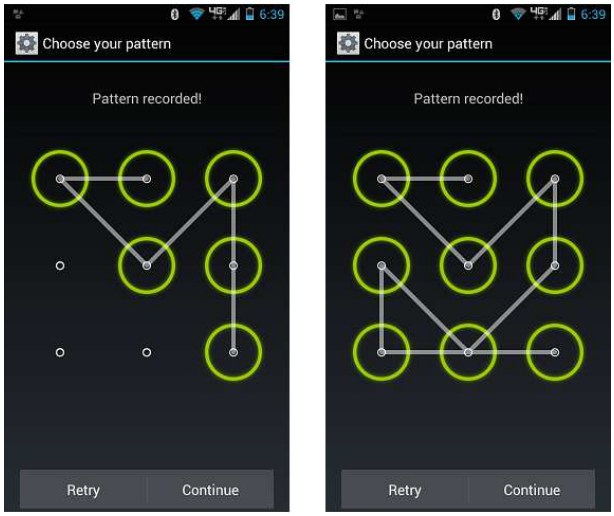
5

Find out how the operating system on *your own* computer stores passwords. Where do you find the corresponding files? Which encryption/hash algorithm is used? Judge about the security of this implementation. Hint: All current operating systems store their password in a similar fashion. However, the details of the encryption algorithms used differ considerably.

Exercise 1.3 (The entropy of Android swipe-patterns). (0+5 points)

+5

In order to access a modern Android device, the user has to paint with his fingers a pattern over a three times three grid. If the pattern matches the stored one, the device is unlocked.



Your task is to estimate the entropy of a randomly selected swipe-pattern with ℓ swipes for $\ell = 2, \ldots, 8$. Hint: The pattern starts at any of the nine positions. Assume then for simplicity that the pattern continues at any *adjacent* grid-point, where also diagonal movements are allowed. Compute the average number of possibilities for moving to another grid point and use it to estimate the entropy of each additional swipe.