Cryptography, winter 2014/15

Passwords

Dr. Daniel Loebenberger

File `/etc/passwd`:

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
...
rpm:x:37:37::/var/lib/rpm:/sbin/nologin
...
daniel:x:500:500::/home/daniel:/bin/bash
```

File `/etc/shadow`:

```
root:$1$CQoPk7Zh$370xDLmeGD9m4aF/ciIlC.:14425:0:99999:7:::
bin:*:14425:0:99999:7:::
...
rpm:!!:14425:0:99999:7:::
...
daniel:$1$wKAP1RyH$JeCAcEGhSGVlD0J7.AMg.0:14396:2:5:7:30::
```

Details on the encrypted password:

`> man 3 crypt`.

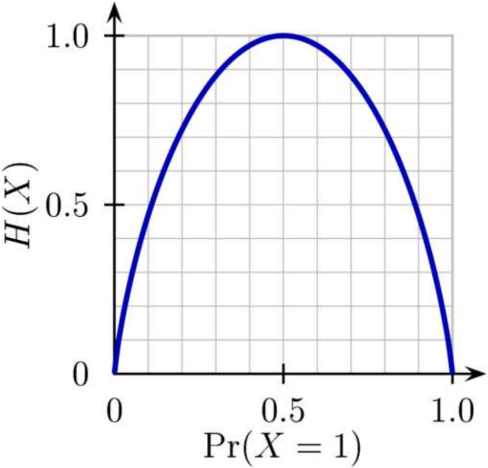
John the Ripper (http://www.openwall.com/john/) provides by default a list of 3546 most frequently used passwords:

```
123456
12345
password
password1
123456789
12345678
1234567890
abc123
computer
tigger
1234
qwerty
money
carmen
mickey
...
```

Claude Shannon (1951):

> *"The entropy is a statistical parameter which measures in a certain sense, how much information is produced on the average for each letter of a text in the language. If the language is translated into binary digits (0 or 1) in the most efficient way, the entropy H is the average number of binary digits required per letter of the original language."*

Binary entropy:



We have the following table of the entropy per symbol for uniformly selected passwords:

Alphabet	Cardinality	Entropy (in bits)
Arabic numbers (0-9)	10	3.322
Hexadecimal numbers(0-F)	16	4.000
Lower case latin alphabet (a-z)	26	4.700
Case-sensitive latin alphabet (a-z, A-Z)	52	5.700
Case-sensitive alphanumeric (a-z, A-Z, 0-9)	62	5.954
ASCII printable	95	6.570
Diceware word list	7776	12.925

Diceware english word list:

```
...
13314 bang
13315 banish
13316 banjo
13321 bank
13322 banks
13323 bantu
13324 bar
13325 barb
13326 bard
13331 bare
13332 barfly
13333 barge
...
```

What about user-generated passwords? Consult NIST Special Publication 800-63, Appendix A.

User-generated passwords according to NIST Special Publication 800-63:

- the entropy of the first character is taken to be 4 bits,
- the entropy of the next 7 characters are 2 bits per character,
- for the 9th through the 20th character the entropy is taken to be 1.5 bits per character,
- For characters 21 and above the entropy is taken to be 1 bit per character,
- A “bonus” of 6 bits of entropy is assigned for a composition rule that requires both upper case and non-alphabetic characters,
- A “bonus” of up to 6 bits of entropy is added for an extensive dictionary check.

Bruce Schneier (2005):

> *"Simply, people can no longer remember passwords good enough to reliably defend against dictionary attacks, and are much more secure if they choose a password too complicated to remember and then write it down. We're all good at securing small pieces of paper. I recommend that people write their passwords down on a small piece of paper, and keep it with their other valuable small pieces of paper: in their wallet."*

PGP key of Daniel Loebenberger, `daniel@bit.uni-bonn.de`

```
FC11 51FB 995E 58A0 186B B701 306A DAFE 965F 1E54
```