**Praktikum 6**

1. Kasutades <http://www.testyourpassword.com/> või muud vahendit loo 10 parooli, mis vastaksid järgmistele tingimustele:

Parooli testimisel lehel <http://www.passwordmeter.com/> peaks tulema

1. kolme parooli tugevuse skooriks 25-50%.
2. järgmise kolme parooli tugevuse skooriks 51-70%
3. ülejäänud paroolide tugevus 71-100%

!! Paroolide seas peaksid olema ka sellised, mille tugevuse skoor on 100%

Paroolide seas peaks olema kolm parooli, mis on moodustatud ainult tähtedest koos numbritega (ehk mitte kasutada erisümboleid jne) ning mille pikkus on maksimaalselt 7.

|  |  |
| --- | --- |
| **Parool** | **Tugevuse skoor %** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. Millega peaks arvestama väga tugevate paroolide loomise juures?

|  |
| --- |
|  |

1. Kasutades <http://www.fileformat.info/tool/hash.htm> arvuta moodustatud paroolide jaoks MD5, SHA-1 ja SHA-256 hash-koode:

|  |  |
| --- | --- |
| Parool | hash |
| 1.Mat34Har15 | MD5 | 0a9c088c4171744a4d0c74ac87e84871 |
| SHA-1 |  |
| SHA-256 |  |
| 2.Mat34 | MD5 | a15d4db669b333a129b501a1f2adbaab |
| SHA-1 |  |
| SHA-256 |  |
| 3. | MD5 |  |
| SHA-1 |  |
| SHA-256 |  |
| 4. | MD5 |  |
| SHA-1 |  |
| SHA-256 |  |
| 5. | MD5 |  |
| SHA-1 |  |
| SHA-256 |  |
| 6. | MD5 |  |
| SHA-1 |  |
| SHA-256 |  |
| 7. | MD5 |  |
| SHA-1 |  |
| SHA-256 |  |
| 8. | MD5 |  |
| SHA-1 |  |
| SHA-256 |  |
| 9. | MD5 |  |
| SHA-1 |  |
| SHA-256 |  |
| 10. | MD5 |  |
| SHA-1 |  |
| SHA-256 |  |

1. Rainbow tabelite kasutamine. Lae alla programm, mis asub aadressil: <http://project-rainbowcrack.com/rainbowcrack-1.5-win32.zip>

Selle programmi kasutamiseks on vaja genereerida vastavad tabelid, tabelite genereerimine võtab palju aega. Uuri juhend <http://project-rainbowcrack.com/tutorial.htm>

1. Käivita CommandPromt ning mine kataloogi, kus asub lahtipakitud programm RainbowCrack 1.5. Selles kaustas proovi genereerida osa tabelist, mis kasutab paroolides ainult väikesi tähti. Paroolide pikkuseks olgu 1-5 tähte. Millise käsuga alustasid genereerimist?

|  |
| --- |
|  |

1. Katkesta tabeli genereerimine umbes 10 min pärast (CTRL+C cmd aknas). Uuri kuidas sorteerida saadud tabelit. Millise käsuga õnnestus sorteerimist teostada?

|  |
| --- |
|  |

1. Käivita programmi graafiline liides rcrack\_gui ning uuri selle tööd. Selleks vajad korraliku tabelit, mis on paigutatud Y kettale, või mille saad alla laadida aadressilt: [www.tlu.ee/~matsak/crypto/temp/tabel](http://www.tlu.ee/~matsak/crypto/temp/tabel)
Paki see tabel lahti (kui laed internetist).
NB! Selle tabeli abil sul ei õnnestu hash-koode murda, kuna see on üks mitmest vajalikest tabelitest.
2. File menüüst saad lisada hash-i. Seejärel menüüs Rainbow Table vali Search Rainbow Tables ning ava eelmises punktis mainitud tabel. Kopeeri siia saadud tulemused (aknas Messages ilmub mõne aja pärast tagasiside):

|  |
| --- |
|  |