77900676

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Bc. Martin Strapko
Študijný program: informatika (Jednoodborové štúdium, magisterský II. st., denná forma)
Študijný odbor: informatika
Typ záverečnej práce: diplomová
Jazyk záverečnej práce: slovenský
Sekundárny jazyk: anglický

Názov: Metódy útoku hrubou silou na TrueCrypt
Methods of brute-force attack on TrueCrypt

Cieľ: Cieľom práce je napísať program, ktorý sa snaží hrubou silou, ale čo najefektívnejšie, nájsť heslo pre dešifrovanie disku zašifrovaného pomocou programu TrueCrypt.

Riešenie projektu je možné rozdeliť do viacerých podproblémov:
* Preštudovanie dokumentácie a implementácie šifrovania v programe TrueCrypt.
* Izolovanie minimálneho kódu potrebného pre overenie korektnosti hesla.
* Navrhnúť popis na generovanie hesiel spĺňajúcich určité pravidlá. Napríklad:
* Minimálna, maximálna dĺžka.
* Počet znakov, cifier, a nealfanumerických znakov.
* Tvar hesla, napríklad pomocou regulárnych výrazov (napr. /(\d){2,3}\[a-z\]+(\[A-Z\]){4,7}/).
* Heslo sa má nachádzať v definovanom slovníku.
* Vytvoriť takýto slovník pre SK.
* Generovanie potenciálnych hesiel na základe navrhnutého popisu.
* Zohľadniť pravdepodobnosť výskytu slov alebo písmen (napr. podľa použitého jazyka).
* Overovanie hesiel (paralelne na viacerých jadrách CPU, GPU, distribuované na viacerých PC)
* Zobrazovanie progresu a odhadovaného času.
* Hľadanie hesla pomocou SAT-solverov na GPU.

Vedúci: RNDr. Richard Ostertág, PhD.
Katedra: FMFI.KI - Katedra informatiky
Vedúci katedry: doc. RNDr. Daniel Olejár, PhD.

Spôsob sprístupnenia elektronickej verzie práce:
bez obmedzenia

Dátum zadania: 22.10.2014

Dátum schválenia: 12.12.2014 prof. RNDr. Branislav Rovan, PhD.
garant študijného programu

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

....

študent vedúci práce