Begleitprotokoll

Name des Schülers: Sebastian Hirnschall
Thema der Arbeit:
Funktionsweise und Schwachstellen von kryptographischen Hashfunktionen
Name der Betreuungsperson: Mag. Christian Filipp

Datum	Vorgangsweise, ausgeführte Arbeiten, verwendete Hilfsmittel, aufgesuchte Bibliotheken,...
01.12.2016	Empirischer Teil der Arbeit fertiggestellt
05.12.2016	Abschnitt 2.1 Kryptographische Hashfunktionen -Definition -Beweis -Literatur: Stinson und Schneier -Bibliothek: TU Wien
06.12.2016	Änderung an Abschnitt 2.1
08.12.2016	Abschnitt 2.1 Kryptographische Hashfunktionen -Theorem -Beweis -Abschnitt 2.1 fertiggestellt
10.12.2016	-Bruteforce Code optimiert -Änderungen an Abschnitt 2.1
12.12.2016	-Literaturverzeichnis mit Biblatex
15.01.2017	Abschnitt 3.1 MD4 -Beschreibung des MD4 Algorithmus
16.01.2017	Abschnitt 3.1 MD4 -Angriffe -Schwachstellen
17.01.2017	Abschnitt 3.2 MD5 -MD5 Schritte -MD5 Änderungen zu MD4 (Rivest-rfc1320)
18.01.2017	Abschnitt 3.1 MD4 -Beispielrechnung - händisch

22.01.2017	Eine frühe Fassung -SHA -Bitoperatoren -Abschnitt 2 geändert -Unterschiede SHA MD5 -Markow-Kette Änderung -Bruteforce Code erklärt -Anhang -Kapitel Verwendung gestrichen um 60Tsd. Zeichen nicht zu überschreiten

Datum	Besprechungen mit der betreuenden Lehrperson, Fortschritte, offene Fragen, Probleme, nächste Schritte
22.06.2016	über Sommer: -Theorieteil (Bücher aus TU und Vorträge) -praktischer Teil über Vorträge Aufbau: 1. Hashfunktionen (was? + Programmcode, Funktionen, Schwachstellen) 2. Angriffsmethoden (Vergleich, Muster der PW) Analye bereits im Laufen ca.50:50 (Theorie - Praxis)
29.09.2016	-Vorstellen der LaTex-Vorlage (selbst erstellt) – ist O.K. -Besprechen der Zitierweise: direkte Zitate (eingerückt und kursiv) =>genaues Zitieren in Literaturverzeichnis -Indirekte Zitate: mit Zusatz („Vergleiche“) -selbst erstellte Abbildungen + Code mit Hinweis darauf -In Kopfzeile reicht Hauptkapitel -Formulierung mit „man“ und „ich“ möglichst vermeiden (ausgenommen mathematische Erklärungen) -Zeichenzählen von PDF zu normalem Text (da sonst Sourcecode nicht mitgezählt werden würde)

12.01.2017	-Definitionen, Beweis und Protokoll (5 Schritte) direkt aus Buch übernommen (Hinweis darauf in Fußnote) -bereits besprochen: kryptographischen Hashfunktionen und praktischer Teil (Hash entschlüsseln + Theorie zu Markow-Ketten) -noch zu erledigen: Funktionsweise von Hash-Funktionen und Hashfunktionen im Vergleich -bis 31.1.: Endfassung ->Rückmeldung bis 3.2. -letzter Abgabetermin: 17.2. (in 3 fach gebundener Ausfertigung) -Termin zur Besprechung der Präsentation: 2.3. / 13: 20 (Columbus)

Die Arbeit hat eine Länge von 57 890 Zeichen.

Datum, Ort

Sebastian Hirnschall