NEWS

Auf den Spuren von Alan Turing

Summer School der Informatik 2015

17.08.2015 | Dass diese Thematik auch heutzutage nichts an ihrer Faszination verloren hat, stellten Studierende der Informatik bei einem Kinobesuch fest. Inspiriert von oben genannten Film äußerten sie gegenüber Prof. Dr. Christoph Karg den Wunsch, sich im Rahmen einer Summer School mit der Enigma und deren Kryptoanalyse zu beschäftigen. Das Ergebnis war eine auf dem Konzept des projektorientierten Lernens basierende Veranstaltung, die drei Projekte umfasste. Das erste Projekt bestand in der Implementierung der Enigma in Form eines Konsolenprogramms. Anschließend wurde im Rahmen des zweiten Projekts durch die Analyse deutschsprachiger Webseiten eine statistische Datenbank für die Häufigkeiten von in deutschen Texten vorkommenden Buchstaben und Bigramme, Buchstabenpaare, erstellt. Das dritte Projekt befasste sich schließlich mit der Kryptoanalyse der Enigma. Hierzu wurde ein Verfahren von James Gillogly aus dem Jahr 1995 umgesetzt. Das Besondere an dieser Attacke ist der Ansatz, statistische Unregelmäßigkeiten der deutschen Sprache für die Analyse auszunutzen. Durch den Einsatz paralleler Programmierung erstellten die Studenten eine Analysesoftware, die auf einem handelsüblichen Computer für einen mit der Enigma verschlüsselten Geheimtext innerhalb weniger Minuten den entsprechenden Klartext berechnet.

Zusammenfassend waren die während der Summer School zu bearbeitenden Projekte eine Kombination aus Mathematik, Algorithmik und Programmierung. Diese Mischung kam bei den Teilnehmern sehr gut an. Besonders erfreulich war, dass nicht nur Studierende der Informatik, sondern auch ihre Kommilitonen aus der Elektrotechnik dieses Wahlfach nutzten, um ihr Wissen in der Kryptographie zu vertiefen.