KIT-Professor Jörn Müller-Quade (rechts) und Secorvo-Chef Dirk Fox

Die Code-Knacker

2012 wäre der Brite Alan Turing 100 Jahre alt geworden. Jörn Müller-Quade und Dirk Fox erzählen von einem Genie, das die moderne Informatik mitbegründet hat

Alan Turing war ein komischer Kauz. Wenn der Engländer Fahrrad fuhr, hatte er immer eine Gasmaske auf – er litt an schlimmem Heuschnupfen. Eine andere Anekdote: Als seine Fahrrad-Kette einmal aus der Führung sprang, reparierte er sie nicht, sondern berechnete einen Algorithmus, um rechtzeitig anzuhalten – und die Kette wieder einzusetzen. Aber Turing war auch der Mann, dessen Berechnungen den Zweiten Weltkrieg mitentschieden – und der Mann, der die Grundlagen für die heutige Informatik schuf.

Turing, sein Wirken und die Geschichte der Kryptographie waren Thema einer Veranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si). Während Jörn Müller-Quade, Professor am KIT und Leiter des Kompetenzzentrums für Angewandte Sicherheits-Technologie (KASTEL), über Turing referierte, gab Dirk Fox, Chef des Sicherheitsdienstleisters Secorvo, einen Überblick über die Historie.

Fox geht dabei ins 16. Jahrhundert zurück, als die Intrige gegen Elisabeth I. aufflog, weil der englische Geheimdienstchef Sir Walsingham es schaffte, die Substitutionschiffre der Babington-Verschwörer um die schottische Königin Maria Stuart zu entschlüsseln. Die hatten Buchstaben durch Zeichen ausgetauscht. Durch eine Häufigkeitsanalyse der Buchstaben in abgefangenen Nachrichten dechriffierte Walsinghams Geheimsekretär die Chiffre der Verschwörer. Das kostete der Schottin, die auch zeitweise französische Königin war, den Kopf. Fox: „Ironischerweise hatte ein Jahr zuvor der französische Diplomat Blaise de Vigenère eine nach ihm benannte Chiffrierung entwickelt, die für Jahrhunderte als nicht zu knacken galt."

Erst 300 Jahre später entschlüsselte der preußische Offizier Friedrich Wilhelm Kasiski die Vigenère-Chiffre. Das stürzte die Kryptographie zunächst in die Krise. „Im Ersten Weltkrieg griffen Deutsche wie Alliierte wieder auf Codebücher zurück." 1923 entwickelte Arthur Scherbius dann die Enigma, die als unknackbar galt. Zumindest im Deutschen Reich.

Turing war der wichtigste Kopf einer Abteilung von Tausenden Mitarbeitern, die jahrelang an der Entschlüsselung der Enigma arbeitete. „Das Brechen der Enigma ist für viele Historiker einer der kriegsentscheidenden Momente", erklärt Fox.

Turing war aber nicht nur Kryptoanalytiker, sondern auch ein begnadeter Mathematiker, der nach dem Krieg den Turing-Test entwickelte und dadurch die Entwicklung der künstlichen Intelligenz mit anstieß. Das von ihm entwickelte Berechenbarkeitsmodell der Turingmaschine bildet eines der Fundamente der theoretischen Informatik. „Sie ist das Standardmodell für die Berechenbarkeit, welcher Algorithmus schnell und welcher nicht schnell ist", erklärt Müller-Quade und fügt an: „Vor Turing war es nicht klar, was Berechenbarkeit überhaupt bedeutet. Man konnte es nicht formal fassen, zu was die Mathematik überhaupt in der Lage ist." Seit Turing ist das anders. ***rs***

KA-IT-Si
Karlsruher IT-Sicherheitsinitiative

Mehr Informationen über die Geschichte der Kryptographie und einen Überblick über die Veranstaltungen der KA-IT-Si erhalten Sie online unter www.ka-it-si.de

Foto: Jigal Fichtner