Fachkurs des Krypt Det in Bern

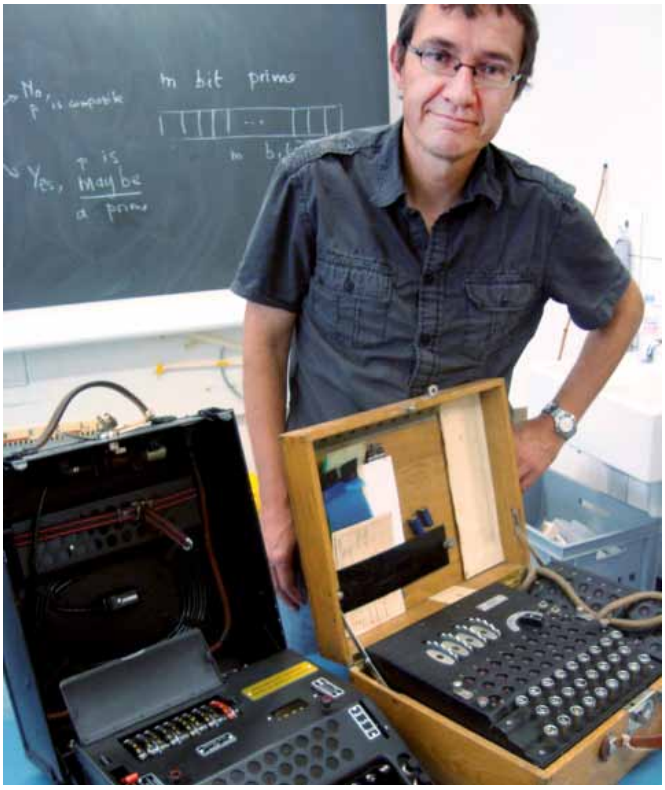
Die Suche nach der perfekten Verschlüsselung

Hört man das Wort Kryptologie, denkt man möglicherweise an eine «trockene» Wissenschaft. Tatsächlich dreht sich auch an heissen Sommertagen in den Räumen der Universität Bern bei den Kryptologen der Schweizer Armee viel um Zahlen, Buchstaben und Formeln. Es steckt allerdings viel mehr dahinter – und das ist faszinierend.

Text und Bilder: Wm Mathias Germann, Komm Team FU Br 41

Domink Schatzmann und François Weissbaum stellen hohe Anforderungen an ihre Kryptologen.

Kryptologen arbeiten mit der neuesten Technologie – die alten Geräte waren Vorreiter der Verschlüsselung.



«Diese alten Chiffriermaschinen sind faszinierend», sagt François Weissbaum. Er ist noch immer von der «Nema» (links, 1960–1990 im Einsatz) und «Enigma» (1940–1970 im Einsatz) angetan.

Codes, Passwörter, Logins – im täglichen Leben bedienen wir uns diverser Zahlen- und Buchstabenkombinationen. Sei es, um Mobiltelefone zu entsperren, E-Mails abzurufen, Geld abzuheben oder um mittels E-Banking unsere Rechnungen zu bezahlen. Dabei müssen wir darauf achten, dass Dritte nicht an unsere «geheimen» Wörter gelangen. Eine möglichst komplizierte und zufällige Aneinanderreihung von Zeichen ist dabei eine wichtige Voraussetzung, um Missbrauch vorzubeugen.

«Leider sind viele Leute aber nicht allzu kreativ», bedauert François Weissbaum. Häufig würden Namen, Geburtstage oder simple Zahlenkombinationen benützt, erklärt er. Weissbaum muss es wissen: Im Beruf setzt sich der promovierte Mathematiker täglich mit der Thematik Kryptologie auseinander – auch für die Schweizer Armee.

Eine Verteidigungsarmee – auch hier

Doch was ist Kryptologie überhaupt? Einfach gesagt, ist es jene Wissenschaft, die sich mit Informationssicherheit beschäftigt. Nicht nur im zivilen Leben ist sie essenziell, sondern natürlich auch im Militär. Kryptologen arbeiten dabei eher im Hintergrund, meist an Computern. Man bekommt in der Regel weder sie noch ihre Arbeit zu sehen.

Als wissenschaftlicher Mitarbeiter der «IS Krypt» (Informationssicherheit und Kryptologie) ist Weissbaum beim Bund angestellt, wobei hauptsächlich das VBS sein Auftraggeber ist. Beim 45-Jährigen dreht sich dabei (fast) alles um ein Wort: Verschlüsselung.

So auch an den heissen Sommertagen im August 2012, als er innerhalb des Fachkurses der Kryptologen die AdA an der Universität Bern schult, ihnen Aufgaben und Herausforderungen stellt. «Viele meinen, dass es nur darum gehe, geheime Codes zu entschlüsseln», sagt Weissbaum. Dem sei nicht so. Vielmehr habe die Schweizer Armee das Ziel, Verschüsselungsverfahren zu analysieren und zu zertifizieren, um zu verhindern, dass andere – im Ernstfall ein Gegner – die eigenen Kommunikationsinhalte dechiffrieren können. «Wir sind auch diesbezüglich eine klassische Verteidigungsarmee», ergänzt Dominik Schatzmann. Der «Chef Kryptologen-Detachement (Krypt Det)» hat Informations- und Elektrotechnik studiert und ist Weissbaums rechte Hand während des dreiwöchigen Fachkurses. Im Gegensatz zu ihm ist der 31-Jährige aber nicht beruflich für die Armee tätig. «Ich absolviere einen ganz normalen WK», erzählt er und schmunzelt.

Genau diese Tatsache ist für die Armee Gold wert. Dank dem Milizsystem bringen er und alle anderen Kryptologen ihr im zivilen Leben angeeignetes Fachwissen in die Armee ein. Doch was sind das für AdA? «Es sind studierte Mathematiker, Physiker, Elektroingenieure und Informatiker, die sich umteilen lassen», erklärt Weissbaum. Eine Kryptologen-RS gibt es nicht.

Nicht so trocken, wie man meint

Jährlich würden 10 bis 20 neue Leute zum Team stossen, insgesamt seien immer gegen 60 AdA einsatzfähig, rechnet Weissbaum vor. Die Anforderungen, um überhaupt zum Armee-Kryptologen umgeteilt werden zu können, sind hoch: Es gibt einen Einführungskurs und eine Prüfung, die man bestehen muss. «Etwa einen Drittel aller Bewerber müssen wir zurückweisen», sagt Schatzmann.

Wer es allerdings schafft, dem winkt eine sehr spannende und herausfordernde militärische Arbeit. Der persönliche Austausch untereinander ist dabei nicht nur angenehm, sondern äusserst wichtig. In Gruppen eingeteilt, bringt im Fachkurs jeder sein spezifisches Fachwissen ein, um innerhalb eines Projekts zur Lösungsfindung beizutragen. Meistens dreht sich dabei alles um die erwähnten Verschlüsselungsverfahren.

Eine «Enigma» – nur etwas komplizierter

Im zweiten Weltkrieg waren Chiffriergeräte mechanische oder, wie im Fall der berühmten deutschen «Enigma», elektromechanische Maschinen. «Enigma» bestand aus einer Eingabetastatur, verschiedenen Rotoren und einer Ausgabeeinheit. Jeder dieser Rotoren war für eine bestimmte Buchstabensubstitution besorgt. Alle Rotoren zusammen bewirkten das Ersetzen eines Klartextbuchstabens durch einen Chiffratbuchstaben. Die Aufgabe der Kryptanalysten der Alliierten bestand darin, möglichst effizient den für eine chiffrierte Meldung verwendeten Schlüssel herauszufinden. Im Fall der «Enigma» bedeutet das, dass man die Substitutionen der einzelnen Rotoren kennt.

Das Prinzip des Chiffrierens und Dechiffrierens ist auch heute noch das gleiche wie vor 70 Jahren. Weissbaum erklärt: «Heute arbeiten wir mit modernsten und leistungsstärksten Computern, aber in der Theorie hat sich kaum etwas verändert. Ein Verschlüsselungsverfahren gilt dann als sicher, wenn es einem Gegner unmöglich ist, mit der ihm zur Verfügung stehenden Rechenpower innert nützlicher Frist an den Schlüssel zu kommen. Mit den heutigen technischen Mitteln ist das Entschlüsseln der ‹Enigma› ein Kinderspiel.»

Für den Fall der Fälle vorgesorgt

Die Schweizer Armee ist dank ihren Kryptologen bestens auf den Ernstfall vorbereitet, durch Übungen, Schulungen und Weiterbildungen. «Der Feind hört mit», war eine Kampagne des Deutschen Reichs zur Abwehr von Spionage und Sabotage. Nein, dies ist momentan bei der Schweiz nicht der Fall. Gut zu wissen, dass wir gerüstet wären, sollte er eintreffen. ■

Wie werde ich Kryptologe?

Wollen Sie Ihr Fachwissen in Informatik und Mathematik im Kryptologen-Detachement einbringen? Dann bewerben Sie sich!

Voraussetzung ist, dass Sie ein Hochschul- oder Fachhochschulstudium in Mathematik, Informatik, Elektrotechnik oder Physik abgeschlossen haben, jünger als 30 Jahre sind und noch mindestens 60 Dienstage leisten müssen.

Qualifizierte Kandidaten werden zu einem Gast-WK im Krypt Det aufgeboten und besuchen einen Einführungskurs in Kryptologie. Am Ende des dreiwöchigen Kurses absolvieren sie eine mündliche Fachprüfung. Das Bestehen dieser Prüfung ist eine notwendige Voraussetzung für eine anschliessende Umteilung ins Krypt Det.

Mehr Informationen zum Bewerbungsprozess finden Sie unter www.kryptdet.ch.