SchülerKrypto 2013 am 07.11.2013

Nun zum 3. Mal nahmen auf Einladung der Deutschen Bank – und von ihr gesponsert – am 07.11.2013 insgesamt 30 Schülerinnen und Schüler der Leistungskurse Mathematik der Eichendorffschule Kelkheim an der „SchülerKrypto 2013“ teil. Erstmalig dabei waren auch 15 Schülerinnen und Schüler der Main-Taunus-Schule in Hofheim an diesem Seminar zum mathematischen und informatorischen Verständnis der Ver- und Entschlüsselung von Nachrichten.

Das Seminar fand wie im letzten Jahr in den Rechner- und Gruppenräumen der Eichendorffschule statt.

Prof. Bernhard Esslinger, Leiter der Krypto-Abteilung der Bank und Professor an der Uni Siegen, begrüßte die Gruppe und stellte kurz die Bedeutung von Verschlüsselungstechnik für viele Bereiche des Alltags dar wie z. B. Fernsehen, Internet und Online-Banking. Er zeigte weiter auf, welche Rolle die Informations- und Sicherheitstechnik in einem weltweit operierenden Konzern wie der Deutschen Bank spielt, und ermutigte die Schülerinnen und Schüler, die MINT-Fächer (Mathematik, Informatik, Naturwissenschaften und Technik) als Berufsperspektive in den Blick zu nehmen. Auch zu den aktuellen Fragen in Blick auf die Abhör- und Entschlüsselungsaktiviäten der NSA gab er interessante Antworten.

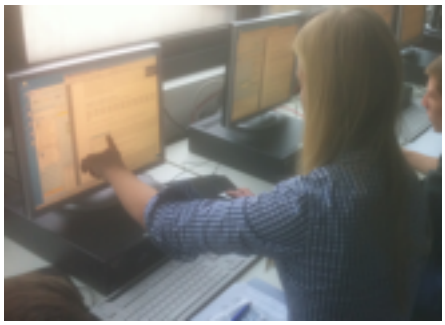
Frau Dr. Sibylle Hick, Frau Nina Ginap und Hr. Oliver Doerler, Mitarbeiter/innen in der Krypto-Abteilung der Bank, stellten anschließend das Programm des Tages vor: Zwei einführende Vorträge in die Kryptographie wechselten sich jeweils mit zwei zwei praktischen Übungen zu Entschlüsselungsaufträgen ab.

Zur Einführung in die Verschlüsselung wurden die bereits in der Antike bekannten Verfahren „Caesar“ und „Skytale“ vorgestellt und Strategien und Techniken zum „Knacken“ solch verschlüsselter Botschaften diskutiert. Dabei konnten die Schülerinnen und Schüler das erste Mal zeigen, wie gut sie kombinieren und wie schnell sie rechnen können. Nach diesen Einführungen gingen die Gruppen in die bereitgestellten Rechnerräume, um an den einführenden Beispielen das Handling mit einem Rechner gestützten Kryptoanalyse-Tool zu erproben. Dabei arbeiteten die Schüler mit den Open-Source-Tools CrypTool 1.4 und CrypTool 2.0. Unterstützt wurden Sie dabei u. a. von Dr. Arno Wacker, Dozent an der Uni Kassel, der dort Vorlesungen zur Kryptographie hält und die Entwicklung von CrypTool 2.0 leitet. Die ersten beiden

Entschlüsselungsaufträge wurden mit Bravour erledigt und die schnellsten Entschlüsseler erhielten erste Buchpreise.

Für das leibliche Wohl sorgte zwischenzeitlich das Schülercafe der Eichendorffschule sowie in der Mittagspause diverse Pizzen.

Die maschinelle Verschlüsselung wurde am Beispiel der Enigma, der von den Deutschen im Zweiten Weltkrieg verwendeten Verschlüsselungsmaschine, vorgestellt. Kleine Animationen verdeutlichten die entsprechenden Prinzipien, und Filmausschnitte zeigten, welche Bedeutung und welchen Umfang die Maßnahmen der Alliierten zur Entschlüsselung hatten.



Die Verschlüsselung mit Computern wurde anhand der Entstehung des DES (Data Encryption Standard) und anschließend mit dem AES (Advanced Encryption Standard) dargestellt. Die Rolle der Geheimdienste, die Anforderungen in den Ausschreibungen sowie die technischen Prinzipien wurden ausführlich in der Theorie entwickelt. Deutlich wurde dabei, dass die Sicherheit des ganzen Prozesses letztlich an der Sicherheit des verwendeten Schlüssels hängt und ein Kernproblem aller Verschlüsselungsfragen die Beantwortung der Frage ist: Wie kann der Schlüssel selbst sicher übertragen werden?

Nach den symmetrischen Verfahren wurde mit einer Demonstration das Problem des Schlüsselaustausches gezeigt. Dabei wird die eigentliche Nachricht mit dem Schlüssel des Senders „zugeschlossen“ und verschickt, der Empfänger seinerseits „verschließt“ die Nachricht ebenfalls mit seinem Schlüssel und sendet diese an den Sender zurück. Der Sender öffnet mit seinen Schlüssel sein „Schloss“ und schickt die noch immer mit dem Empfängerschlüssel „verschlossene“ Nachricht wieder an den Empfänger. Dieses praktische Beispiel zeigte, dass es möglich ist, eine Nachricht auch ohne vorherigen Schlüsselaustausch zu übertragen.

Im Anschluss an das Schlüsselaustauschproblem wurde mit RSA noch ein asymmetrisches Verfahren vorgestellt, bei dem ein öffentlicher und ein privater Schlüssel mit Hilfe zweier sehr großer Primzahlen generiert werden und das Verfahren so lange sicher ist, wie die Faktorisierung sehr großer Zahlen eine genügend lange Zeit braucht. Dies ist mit den heutigen Schlüssellängen gegeben, so dass das RSA-Verfahren als sicher gilt. Im Gegensatz zu den symmetrischen Verfahren werden also

bei den asymmetrischen Verfahren zwei Schlüssel verwendet, wobei der öffentliche Schlüssel für die Verschlüsselung zwischen den Kommunikationspartnern ausgetauscht wird, während der private Schlüssel nur seinem Inhaber bekannt ist.

Im Anschluss an die Theorie gab es wieder Arbeits- und Entschlüsselungsaufträge, die mit den Krypto-Tools zu erledigen waren, und es konnten weitere Buchpreise gewonnen werden.

Sowohl in der Arbeit während des ganzen Tages als auch in der Feedback-Runde zum Abschluss wurde deutlich, dass das Thema Verschlüsselung die Schülerinnen und Schüler sehr fasziniert hat, und festgestellt, dass es toll wäre, wenn diese Veranstaltung auch für künftige Mathematikkurse ermöglicht werden könnte.

Die Trainer ihrerseits gaben den Schülern ein großes Kompliment mit auf den Heimweg: Sie hätten nicht erwartet, dass diese so schnell die Aufgaben lösen und so gut mit den Tools umgehen können. Sie luden Interessierte ein, an der Weiterentwicklung der Tools mitzuarbeiten.