

SchülerKrypto 2014 am 14.11.2014

Nun zum 4. Mal nahmen auf Einladung der Deutschen Bank – und von ihr gesponsert – am 14.11.2014 insgesamt 26 Schülerinnen und Schüler der Leistungskurse Mathematik der Eichendorffschule Kelkheim an der „SchülerKrypto 2014“ teil. Auch 6 Schüler der Main-Taunus-Schule in Hofheim nahmen an diesem Seminar zum mathematischen und informatorischen Verständnis der Ver- und Entschlüsselung von Nachrichten teil. Das Seminar fand in den Rechner- und Gruppenräumen der Eichendorffschule statt. Dozenten und Trainer dieser Schülerkrypto waren die Mitarbeiter/innen der Sicherheitsabteilung der Deutschen Bank Fr. Cristina Balasoiu, Fr. Dr. Sibylle Hick, Hr. Dr. Michael Schneider und Hr. Oliver Dörler sowie Prof. Dr. Arno Wacker und Hr. Nils Kopal von der Universität Kassel.

Nach einer kurzen Einführung in die Bedeutung der Kryptologie für den Datenaustausch und insbesondere für die Sicherheit im elektronischen Bankwesen wurde das Programm des Tages vorgestellt: Einführende Vorträge in die Kryptographie wechselten sich jeweils mit 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“ solcher 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 dem Rechner gestützten Kryptoanalyse-Tool CrypTool 2.0 zu erproben. 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 seinem 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. Es wäre sehr schön, wenn diese Veranstaltung auch für künftige Mathematikurse ermöglicht werden könnte.



Die Dozenten und 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.