

Gewinner des Dr. Hans Riegel-Facharbeitspreises

Von Heinz Kalenberg

21. September 2018, 00:00

Wettbewerbe

Preis der Dr. Hans Riegel-Stiftung



Die Förderung von Nachwuchskräften der MINT-Fächer ist eines der herausragenden Ziele der Dr. Hans Riegel-Stiftung. Aus diesem Grund werden jährlich auf Landesebene die besten Facharbeiten in den MINT-Fächern ausgezeichnet.

Moritz Brand ist in diesem Jahr ein Preisträger von unserer Schule. Er wurde für die zweitbeste Arbeit in Mathematik mit dem Dr. Hans Riegel-Facharbeitspreis geehrt. Moritz hat sich in seiner Facharbeit intensiv mit Verschlüsselungstechniken, insbesondere dem RSA-Verfahren und asymmetrischen Verschlüsselungen, beschäftigt. In der Laudatio zu seiner Arbeit wurde besonders die gelungene und verständliche Darstellung komplexer mathematischer Sachverhalte gelobt.

Wir gratulieren Moritz zu seinem schönen Ergebnis



Verschlüsselungen

Einfache Verschlüsselungen verwenden eine monoalphabetische Verschlüsselungstechnik. Dabei wird jedem Buchstaben eindeutig ein anderes Zeichen zugeordnet. Wenn Moritz seiner Freundin Jane eine verschlüsselte Nachricht übermitteln möchte, so müssen sich beide auf einen Schlüssel einigen, den Moritz zum Verschlüsseln und Jane zum Entschlüsseln verwendet.

Eine besonders einfache Verschlüsselung ist die Caesar-Verschlüsselung, bei der alle Buchstaben um eine festgelegte Zahl (z.B. 3) verschoben werden: Aus A wird also D, aus B wird dann E, aus C wird F u.s.w....

PDWKH LVW XHEHDOO ist aus einem Originaltext durch Verschiebung um 3 entstanden. Wenn man den Schlüssel (Verschiebung um 3) kennt, ist es nicht so schwierig den Text zu entschlüsseln. Aber auch, wenn man den Schlüssel nicht kennt, kann man etwas längere Texte leicht durch eine Häufigkeitsanalyse entschlüsseln. Da in der deutschen Sprache das E am häufigsten vorkommt, schaut man, welches Zeichen im verschlüsselten am meisten auftaucht. Dieses Zeichen entspricht dann dem E. Mit den übrigen Buchstaben verfährt man entsprechend.

Heute spielt die Verschlüsselung bei Nachrichtenübermittlungen über das Internet eine große Rolle. Überall können Hacker lauern, die wichtige wirtschaftliche oder politische Informationen abgreifen wollen. Hier kommt die RSA-Verschlüsselung ins Spiel.

Moritz möchte wieder eine Nachricht an Jane verschicken, Jane wohnt aber mittlerweile in Amerika und beide wissen zunächst nicht so genau, wie sie den Schlüssel vereinbaren sollen, denn ihnen ist klar, dass Frank ihre gesamte Korrespondenz vollständig abhört.

Und nun kommt das Verblüffende der RSA- Verschlüsselung; eine Eigenschaft, die man eigentlich nicht glauben kann:

Jane sendet Code- Informationen an Moritz.

Moritz verschlüsselt mithilfe dieser Informationen seine Nachricht und sendet diese verschlüsselte Nachricht an Jane.

Frank, der die gesamte Korrespondenz abgehört hat, schafft es selbst unter Einsatz der weltweit zur Verfügung stehenden Rechnerkapazitäten nicht, die Nachricht zu entschlüsseln.

Jane aber schmeißt ihren Computer an und schon huscht ein freudiges Lächeln über ihr Gesicht als sie die Nachricht von Moritz liest.

Frank hat also die gesamte Korrespondenz zwischen Moritz und Jane abgehört, also auch den Austausch der Schlüssel und dennoch ist er nicht in der Lage den Text zu entschlüsseln.

Wundersame Welt der Mathematik.