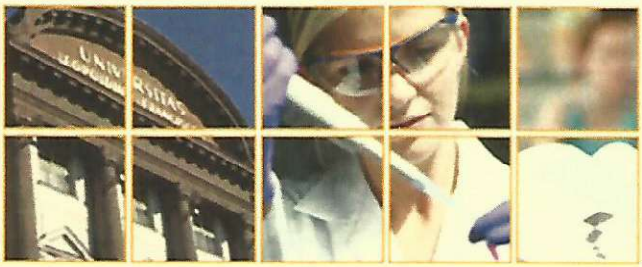
Leopold-Franzens-Universität

universität innsbruck



KAISERSCHILD-STIFTUNG

Dr. Hans Riegel-Fachpreis Mathematik 2017

URKUNDE

Der

1. Preis

ergeht an **Herr Andreas Mair,**

betreut von Mag.Mag. Georg Jud

für die Vorwissenschaftliche Arbeit zum Thema

Verschlüsselungsmethoden im Informationszeitalter.

Univ. Prof. Dr. Franz Pauer
Universität Innsbruck

Marco Alfter
Vorstandsvorsitzender Kaiserschild-Stiftung

Preisverleihung Haribo-Preis, 15. September 2017

Sehr geehrte Preisträgerinnen und Preisträger, sehr geehrte Damen und Herren!

Das Thema der vorwissenschaftlichen Arbeit von Herrn Andreas Mair war „Verschlüsselungsmethoden im Informationszeitalter und ihre Anwendungsbereiche". Er war Schüler des Gymnasiums des Zisterzienserstiftes in Stams und wurde von Direktor Mag. Georg Jud betreut.

Wegen eines Auslandsaufenthaltes kann Herr Mair leider nicht zur Preisverleihung kommen.

Sichere Datenübertragung und Verschlüsselung sind aktuelle Themen nicht nur der öffentlichen Diskussion sondern auch der Forschung in Mathematik und Informatik. Wenn Sie im In- oder Ausland bei einem Bankomaten Geld abheben, müssen Sie ihren Geheimcode eingeben. Aus Sicherheitsgründen wird dieser aber nicht direkt an ihre Bank weitergeleitet sondern gleich im Bankomat verschlüsselt. Und zwar so: Es sind zwei große Zahlen vorgegeben, die öffentlich bekannt sein können. Ihr Geheimcode wird mit der ersten Zahl potenziert und der Rest dieser Potenz nach Division mit Rest durch die zweite Zahl berechnet. Das Ergebnis wird weitergeleitet und die Bank kann diese Zahl dann entschlüsseln. Die zweite Zahl ist das Produkt von zwei großen Primzahlen. Jede und jeder, der die zweite Zahl in diese zwei Primfaktoren zerlegen kann, kann die Nachricht entschlüsseln. Aber das Zerlegen einer genügend großen Zahlen in Primfaktoren ist sehr, sehr schwer. Alle Computer unserer Welt würden dafür gemeinsam mehr als hundert Jahre brauchen.

Dieses Verfahren zur Verschlüsselung (RSA-Verfahren nach dessen Entdeckern Rivest, Shamir und Adleman) wurde erst vor 40 Jahren entwickelt. Es hat aber bereits den Weg in den Mathematikunterricht der berufsbildenden höheren Schulen gefunden. Es ist also falsch anzunehmen, dass es im Bereich der Mathematik, der in den Schulen unterrichtet wird, seit hundert Jahren nichts Neues mehr gäbe.

In seiner Arbeit stellt Herr Mair den RSA-Algorithmus und andere Verschlüsselungsverfahren vor. Er geht auch auf verschiedene Anwendungsbereiche der Verschlüsselungsverfahren, zum Beispiel elektronische Unterschrift oder elektronisches Geld, ein.

Das Thema ist sehr aktuell und betrifft wichtige Anwendungen der Mathematik im Alltag.

Der Autor hat es sehr engagiert bearbeitet, ich gratuliere Herrn Mair zu seinem ersten Preis!