gymnasiale OBERSTUFE in bayern

Formular zur Beantragung eines **W-Seminars**

Lehrkraft: Brandl

Leitfach: Mathematik

Rahmenthema: Verschlüsselte Botschaften – Kryptographie

Zielgruppe: mathematisch interessierte Schülerinnen und Schüler

Zielsetzung und Beschreibung des Seminars:

Yqbw gkp Ugokpct?

Diesen Geheimtext kann man vielleicht noch entziffern: jeder Buchstabe wurde um 2 Stellen im Alphabet verschoben. Das Y kommt also von einem W.

17635 # 30934 # 01258 # 30016 # 25219 # 26840 # 32952 # 29497 # 25219 # 29044 # 26840 # 25925 # 32952 # 29497 # 10275 # 12935 # 31240

Der gleiche Geheimtext – nun aber mit einem modernen Verfahren verschlüsselt, das die Primzahlen 211 und 167 benutzt. Die Mathematik garantiert, dass dieses Verfahren viel sicherer ist als das erstgenannte. Das ist wohl die Antwort auf die Frage: Wozu ein Seminar mit diesem Thema?

Obwohl die Kryptographie eine lange und komplexe Geschichte hat, entwickelte sie sich erst im 20. Jahrhundert zur rigorosen und auf Mathematik basierenden Wissenschaftsdisziplin. Mit den Kommunikationsmöglichkeiten des Internets wurden kryptographische Verfahren unverzichtbar und allgemein genutzt. Insbesondere an diesem Beispiel zeigt sich, dass Mathematik die wesentliche Grundlage für moderne Kommunikationsformen und deren sichere Nutzung ist. Lange Zeit als „nutzlos“ erachtete Sätze der Zahlentheorie, wie Fermats kleiner Satz, finden nun sogar die Beachtung von Geheimdiensten.

Ein Hauptaugenmerk der Seminararbeiten und insbesondere der Präsentationen liegt auf einer verständlichen Darstellung der zugrundeliegenden mathematischen Konzepte. In diesem Seminar werden den Schüler(inne)n nicht nur grundlegende Arbeitstechniken für das Studium aller mathematisch-naturwissenschaftlicher Fachrichtungen vermittelt, sondern sie erhalten auch Einblicke in mathematische Begriffe und Strukturen, wie sich auch in der universitären Mathematik der Anfangssemester auftauchen.

Dieses Seminar eignet sich zur fachübergreifenden Zusammenarbeit mit Informatik.

Mögliche Formen der Leistungserhebung:

Rechenschaftsablage, bewertetes Gespräch, Schriftlicher Test, Präsentation von Recherche-Ergebnissen, konkrete Organisations- und Planungsleistungen, Exposé

Mögliche Themen für die Seminararbeiten: (bitte 6 Themen angeben)

1. Darstellung und Klassifizierung historischer Verschlüsselungsverfahren
2. Umsetzung klassischer Verschlüsselungstechniken in Programmen, z. B. Skytala
3. Vigenère-Chiffre und dessen Kryptoanalyse
4. Die Enigma
5. Der Data Encryption Standard (DES)
6. Der RSA-Algorithmus

Weitere Bemerkungen zum geplanten Verlauf des Seminars:

Ggf. Einführung in das Textsatzprogramm LaTeX