Vorschlag für ein **W-Seminar**
im Fach
Mathematik

Lehrkraft: Andreas Schewiola **Leitfach: Mathematik**

Rahmenthema: Top Secret – Verschlüsselte Botschaften (Kryptographie)

Zielsetzung des Seminars und Begründung des Themas

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 letzten Jahrhundert zur rigorosen und auf Mathematik basierenden Wissenschaftsdisziplin. Mit den Kommunikationsmöglichkeiten des Internets wurden kryptographische Verfahren unverzichtbar – sei es beim Internetbanking, beim Versenden von Emails, beim PayTV oder einfach nur beim Mobiltelefonieren.

Ausgehend von historischen Beispielen wird der ewige Wettlauf der Ver- und Entschlüssler betrachtet. Oft genug war der Gang der Geschichte davon beeinflusst, wer von beiden gerade die Nase vorne hatte. Die mathematischen Methoden der historischen sowie der aktuellen Ver- und Entschlüsselungstechniken werden verständlich dargestellt, analysiert und erprobt. Für die aufwändige und langwierige Rechenarbeit soll dann der Computer zum Einsatz kommen, teilweise mit kleinen selbst entwickelten Programmen, teilweise mit einer bereitgestellten Software.

Das mathematische Anforderungsniveau für die verschiedenen Seminararbeiten ist recht unterschiedlich – die Spanne reicht von eher „einfacher“ Mathematik bis zu anspruchsvollen Anwendungen der Mathematik. Einige Seminararbeitsthemen haben auch hauptsächlich historischen Charakter, andere Themen haben ihren Schwerpunkt in der Informatik.

Mögliche Themen für die Seminararbeiten:

1. Darstellung und Klassifizierung historischer Verschlüsselungsverfahren
2. Umsetzung klassischer Verschlüsselungstechniken in Programmen, z. B. Skytala, Caesar-Verschlüsselung
3. Vigenère-Chiffre und dessen Kryptoanalyse
4. Programmierung einer Chiffriermaschine Enigma
5. Experimentieren mit verschiedenen Systemen mit dem Werkzeug „Cryptool“
6. Der Data Encryption Standard
7. Advanced Encryption Standard (AES)
8. Der RSA-Algorithmus
9. Email-Verschlüsselung (PGP)
10. Quantenkryptographie
11. Primzahlen und ihre Rolle in der modernen Kryptographie
12. Wie Codes und deren Entschlüsselung den Gang der Geschichte beeinflussten
13. Die Verschlüsselungsmaschine „Enigma“ im 2. Weltkrieg
14. Internetsicherheit
15. Gibt es perfekte Sicherheit eines Kryptosystems?
16. Digitale Signaturen

gymnasiale OBERSTUFE in bayern

Vorschlag für ein **W-Seminar** im Fach **Mathematik**

Halb-jahre	Monate	Tätigkeit der Schülerinnen/Schüler und der Lehrkraft	geplante Formen der Leistungserhebung
11/1	Sept. - Dez.	Hinführende Beispiele (Cäsar, Vigenère) Einführung in das Modulorechnen Historische Entwicklung Andeutung der modernen, asymmetrischen Verfahren Methodentraining und Einführung in die Arbeitsweise zur Erstellung einer wissenschaftlichen Arbeit, insbesondere - Recherchieren und Exzerpieren, - Präsentieren, - formale Anforderungen an die Seminararbeit	Unterrichtsbeiträge, Rechenschaftsablagen möglich: Stegreifaufgabe, fachlicher Abschlusstest
	Jan. - Feb.	Stellung der Themen und erste Recherche der Seminarteilnehmer Unterstützung durch Lehrkraft, Einzelgespräche; Einweisung in EDV-Werkzeuge Anfertigen eines zeitlich strukturierten Arbeitsplans	
11/2	März -Juli	Darstellung der ersten Ergebnisse durch die Seminarteilnehmer in Form eines Kurzreferats (Zielsetzung der Arbeit, bisherige Ergebnisse, Probleme und Schwierigkeiten, Diskussion möglicher Lösungen), Aufzeigen der Verbindungen zwischen den einzelnen Themen, Feedback zum Referat individuelle Beratungsgespräche, gemeinsame Beratungsgespräche nach Bedarf Weiterarbeit an Seminararbeiten	Referat, Handout für die Seminarteilnehmer (Wert wird auf eine verständliche Darstellung gelegt!) Beteiligung an der Diskussion möglich: Vorbereitung und Qualität der Beratungsgespräche
12/1	Sept. - Nov.	Jeder Seminarteilnehmer informiert abermals über seinen Arbeitsstand, ggf. im Seminarplenum. Einzelgespräch: Abschlussbesprechung	
	Dez. - Jan.	Abschlusspräsentationen Gespräch über gezeigte Leistungen	Seminararbeit, Präsentation