KRYPTOLOGIE – VERSCHLÜSSELUNG UND CODEKNACKEN IM WANDEL DER ZEITEN

LUKAS RIEGLER

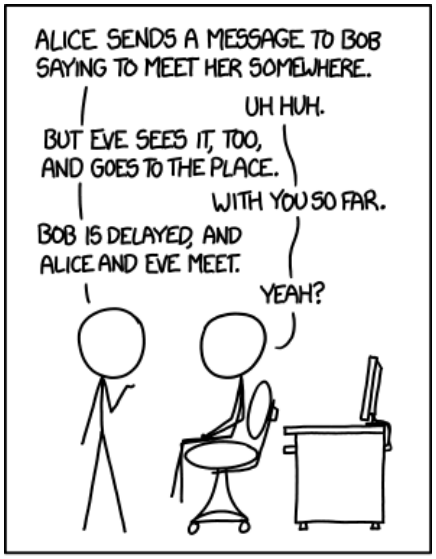
Die Kunst der sicheren Verschlüsselung und Übertragung von Informationen stellt ein seit Jahrtausenden anhaltendes Katz-und-Maus-Spiel zwischen Kryptographen und Kryptoanalytikern dar. Dass vermeintlich sichere Verschlüsselungsmethoden doch geknackt werden konnten, hat ohne Zweifel eine historisch gewichtige Rolle gespielt. Aber kann es überhaupt so etwas wie beweisbar sichere Verschlüsselungen geben?

Die Mathematik hat sich zu einem Standbein moderner Verschlüsselungsverfahren entwickelt. Beim Aufrufen von Websites (https), wenn Dokumente digital unterschrieben werden oder bargeldlos gezahlt wird, findet Zahlentheorie ihre tagtägliche Anwendung.

Ziel des Workshops ist es, ausgewählte Themen der Kryptologie für den Einsatz im Schulbereich aufzubereiten.

Dazu zählen:

- Monoalphabetische Verschlüsselung (z.B.: Caesar-Verschlüsselung)
- Polyalphabetische Verschlüsselung (z.B.: Vigenère-Verschlüsselung)
- Verschlüsselungsmaschinen (z.B.: Enigma)
- Public-Key-Kryptographie und digitale Signaturen (z.B.: RSA-Verfahren)
- Quantenkryptographie



https://xkcd.com/1323/

Literatur

[1] Singh, S.: *The Code Book: Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Anchor Books, 2000.

[2] Ertel, W.: *Angewandte Kryptographie*, Fachbuchverlag Leipzig, 2001.

[3] Holden, J.: *The Mathematics of Secrets*, Princeton University Press, 2017.