26. Vigenère-Verschlüsselung (SJ 9/10, 11/13)

Anne und Bernie verschlüsseln ihre privaten Nachrichten, damit sie nicht von anderen gelesen werden können. Sie verschlüsseln und entschlüsseln ihre Nachrichten nach dem gleichen Schema und benutzen dabei "CAB" als absolut geheimes Wort.

Anne verschlüsselt eine Nachricht an Bernie:

Geheimwort, so oft wie nötig	CABCABCABCAB
Nachricht ohne Leerzeichen	WANNKOMMSTDU
Verschlüsselte Nachricht	ZBPQLQPNUWEW

Weil das C des Geheimworts der dritte Buchstabe im Alphabet ist, wird der erste Buchstabe der Nachricht (W) um drei Stellen im Alphabet nach hinten verschoben (wird zu Z).

Weil das A des Geheimworts der erste Buchstabe im Alphabet ist, wird der zweite Buchstabe der Nachricht (A) um eine Stelle im Alphabet nach hinten verschoben (wird zu B).

Und so weiter, bis die ganze Nachricht verschlüsselt ist.

Bernie antwortet: XNGOGWKS

Wann werden sie sich treffen?

Gib hier die entschlüsselte Antwort ein (in grossen Buchstaben und ohne Leerzeichen): _____

Stufen	3-4	Leicht	Mittel	Schwer
Stufen	5-6	Leicht	Mittel	Schwer
Stufen	7-8	Leicht	Mittel	Schwer
Stufen	**9-10**	Leicht	**Mittel**	Schwer
Stufen	**11-13**	**Leicht**	Mittel	Schwer

DAS IST INFORMATIK!

Verschlüsselung (Kryptographie) wird gebraucht, um zumindest für einen gewissen Zeitraum sicherzustellen, dass nur befugte Personen Informationen verstehen, die auch Unbefugten in die Hände fallen können – zum Beispiel auf dem Postweg.

Verschlüsselungsverfahren unterscheiden sich darin, wie technisch aufwändig das Verschlüsseln ist. Für die Vigenère-Verschlüsselung braucht man keine Maschine, nur Stift und Papier. Blaise de Vigenère (1523 bis 1596) war ein französischer Diplomat und ein Kryptograf.

Verschlüsselungsverfahren unterscheiden sich darin, wie schwer sie grundsätzlich oder im Einzelfall geknackt werden können (Kryptoanalyse). Die Vigenère-Verschlüsselung galt fast dreihundert Jahre als unknackbar – dann kam Charles Babbage.