Lösung

Die richtige Antwort ist LASAGNA:

Bestellung	L	A	S	A	G	N	A
Dreh-Zahl	3	1	4	1	5	9	2
Geheime Botschaft	O	B	W	B	L	W	C

Die Bestellung bekommt man mit Hilfe der Geheimscheibe heraus, indem man für jeden Buchstaben der Botschaft den inneren Ring gemäss der Dreh-Zahl nach links dreht. Nun sucht man den Buchstaben der Botschaft auf dem inneren Ring. Der Buchstabe der Bestellung ist dann der passende Buchstabe auf dem äusseren Ring.

Dies ist Informatik!

Anna verschlüsselt ihre Bestellungen, damit nur ihr Lieblings-Koch sie versteht. Verschlüsselung ist eines der ältesten Anliegen der Menschheit. Schon immer hat es Gründe dafür gegeben, Botschaften so zu übermitteln, dass nur die gewünschten Empfänger sie verstehen können. Es gibt viele verschiedene Verschlüsselungsverfahren. Aber immer gehören zwei Algorithmen dazu, nämlich einer zum Verschlüsseln und einer zum Entschlüsseln und beide benötigen für ihre Arbeit den zur Botschaft gehörigen Schlüssel.
Eines der einfachsten Verschlüsselungsverfahren geht auf Julius Cäsar zurück: Hier ist der Schlüssel eine Zahl, die eine Verschiebung im Alphabet angibt. Der Schlüssel 3 bedeutet z.B., dass der Buchstabe A einer Nachricht mit D verschlüsselt wird und B mit E usw. – und dass der Buchstabe D als A zu entschlüsseln ist, E als B usw. Beim Verschlüsseln und Entschlüsseln nach dieser Methode hilft die „Cäsar-Scheibe“, die in dieser Biberaufgabe beschrieben ist.
Verschlüsselungsverfahren, die für eine Botschaft nur einen Schlüssel verwenden, sind vergleichsweise unsicher. Das weiss Anna anscheinend, denn sie benutzt für jeden Buchstaben einen anderen Schlüssel – ganz ähnlich wie beim Verfahren von Vigenère. In diesem Verfahren wiederholen sich die Dreh-Zahlen bei längeren Botschaften; so wird der Schlüssel nicht zu lang. Aber auch dieses Verschlüsselungsverfahren ist bei längeren Botschaften letztlich unsicher.

Stichwörter und Webseiten

Kryptographie, Polyalphabetische Verschlüsselungsverfahren, Caesar-Verschlüsselung, Vigenère-Verschlüsselung

- `https://de.wikipedia.org/wiki/Caesar-Verschlüsselung`
- `https://de.wikipedia.org/wiki/Polyalphabetische_Substitution`

