ASYMMETRISCHE VERSCHLÜSSELUNG

Cäsar und die modulare Arithmetik

Welcher Zusammenhang besteht zwischen dem Cäsar-Verfahren und der Modulo-Rechnung? Bearbeite dazu folgende Aufgaben.

1. *Ergänze die Cäsar-Tabelle für den Schlüssel s=9 (Erinnerung: Wir verschieben nach links.)*

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

2. *Verschlüssle nun: G U T verschlüsselt mit s=9:* _____
3. *Statt mit Buchstaben arbeiten wir nun mit Zahlen. Die Verschlüsselung soll durch eine Rechenoperation ausgedrückt werden. Ordne dazu jedem Buchstaben zunächst eine Zahl zu, beginnend bei 0.*

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

0 1

4. *Verschlüssle nun mit dem folgenden Verfahren:*
   Schreibe den Buchstaben als Zahl → addiere den Schlüssel → schreibe als Buchstaben
   - G → → →
   - U → → →
   - T → → →

5. *Beschreibe, welches Problem bei U und T auftritt.*
6. *Beschreibe, wie man das Problem mit Hilfe der modulo-Rechnung lösen kann.*
7. *Stelle einen einzigen Term auf, mit dem sich die Nummer des verschlüsselten Buchstaben aus der Nummer des unverschlüsselten Buchstaben berechnen lässt (auch für die Problemfälle)*

   _____

8. *Stelle ebenso einen Term für die Entschlüsselung auf. Überprüfe deine Formel für obiges Beispiel.*

   _____

9. *Erinnere dich an die Regel: Statt den Kryptotext mit den Schlüssel zu <u>ent</u>schlüsseln kann man den Kryptotext mit (26 - Schlüssel) <u>ver</u>schlüsseln.*
   Was bedeutet das in der Modulo-Rechnung?
10. *In welchen anderen Krypto-Verfahren, die du kennengelernt hast, findet sich die Modulo-Rechnung wieder?*
11. *Verschlüssele SUPER mit dem Schlüssel 15 im Cäsar-Verfahren herkömmlich und mit Hilfe der Modulo-Rechnung.*