

Aufgabe 26. Berechne ohne Taschenrechner

- (a) $2^{(2^{32})} \bmod 11$.
 (b) $14^{(2019^{2019})} \bmod 60$.

Aufgabe 27. (a) Sei n eine natürliche Zahl mit der Eigenschaft, dass $2^n - 1$ eine Primzahl ist. Zeige, dass auch n eine Primzahl sein muss.

Hinweis:

$$x^s - 1 = (x - 1)(1 + x + \cdots + x^{s-1})$$

- (b) Die Umkehrung gilt nicht: Finde die kleinste Primzahl p , sodass $2^p - 1$ keine Primzahl ist.

Aufgabe 28. (a) Beschreibe und berechne einen Diffie-Hellman-Schlüsselaustausch mit den Parametern $p = 29$, $g = 5$, $a = 13$, $b = 11$.

- (b) Zu einem Diffie-Hellman-Schlüsselaustausch seien folgende Daten bekannt:

$$\begin{array}{ll} g = 9 & p = 31 \\ m = 2 & n = 14 \end{array}$$

Bestimme die geheimen Parameter a , b und den Schlüssel r !

Zusatzaufgabe. Am Freitag 12.4. um 14:00 werden auf der Internetseite drei verschlüsselte Texte bekanntgegeben (Satzzeichen sind unverschlüsselt, werden aber mitgezählt):

- Text A² (Deutsch) ist mit einem einfachen Schlüssel der Form

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

verschlüsselt.

- Text B³ (Deutsch) ist mit einem Vigenère-Schlüssel⁴ der Länge drei verschlüsselt.
- Text C⁵ (Englisch) ist mit einem Vigenère-Schlüssel unbekannter Länge verschlüsselt.

Hinweis: Die Methode von Babbage/Kasiski⁶ verwenden, um zuerst die Länge des Schlüssels zu bestimmen.

Für das Kreuz ist mindestens einer der drei Texte durch statistische Häufigkeitsanalyse zu entschlüsseln (Computer!).

Zusätzlich zu den Kreuzen gibt es für jeden Text jeweils 3 Extrapunkte für die erste Lösung, die im Onlinekreuzesystem hochgeladen wird.

Abzugeben ist (in einer ZIP-Datei): 1. der Klartext, 2. der oder die gefundenen Schlüssel, 3. eine kurze Erläuterung, wie die Lösung gefunden wurde und 4. selbst geschriebene Programme oder Scripts, die verwendet wurden.

²<https://www.math.tugraz.at/mathc/diskmath/2019/Uebungsblaetter/Zusatz28A.txt>

³<https://www.math.tugraz.at/mathc/diskmath/2019/Uebungsblaetter/Zusatz28B.txt>

⁴<https://de.wikipedia.org/wiki/Vigenere-Chiffre>

⁵<https://www.math.tugraz.at/mathc/diskmath/2019/Uebungsblaetter/Zusatz28C.txt>

⁶<https://de.wikipedia.org/wiki/Kasiski-Test>