Verschlüsselung mittels Multiplikation und Knacken des Codes

PFZ: $264 = 2^3 \cdot 3 \cdot 11$.

Gib einige Produkte an, die 264 als Ergebnis haben: $(2 \cdot 3) \cdot (2^2 \cdot 11) = 6 \cdot 44$;

$(11 \cdot 3) \cdot (2^3) = 33 \cdot 8$; $(2) \cdot (2^2 \cdot 3 \cdot 11) = 2 \cdot 132$

I) Multiplikation und Faktorisierung im Vergleich

1. *Multipliziere:*

Aufgabe	Ergebnis	Benötigte Zeit
$15 \cdot 2 \cdot 3 \cdot 5 =$	450	
$23 \cdot 753 =$	17319	individuell
$5236 \cdot 2358 =$	12346488	

2. *Faktorisiere:*

	PFZ	Benötigte Zeit
204	$2^2 \cdot 3 \cdot 17$	
1815	$3 \cdot 5 \cdot 11^2$	
2323	$23 \cdot 101$	individuell
13261	$89 \cdot 149$	
107800	$2^3 \cdot 5^2 \cdot 7^2 \cdot 11$	

3.

Erkenntnis:

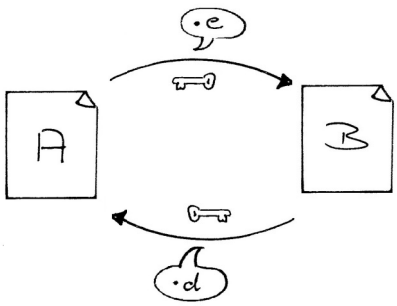
Zum Faktorisieren benötigt man wesentlich längere Zeit als zum Multiplizieren. Besonders aufwändig ist es, wenn die Faktoren Primzahlen sind. Das Problem verschärft sich, je größer die Primzahlfaktoren werden.

II) Ver- und Entschlüsseln durch modulare Multiplikation

Das selbe Verfahren wie oben wird nun durchgeführt, aber mit „modulo-Zahlen“

- *Die Botschaft A wird durch Multiplikation mit einer Zahl e verschlüsselt.*

- *nach Abschnitt I) wird entschlüsselt mittels Division des Geheimtextes B durch die Verschlüsselungszahl e. Vom Rechnen mit reellen Zahlen weißt du, dass man eine Division auch als Multiplikation mit dem Kehrwert von e ausführen kann: $5 : 3 = 5 \cdot \frac{1}{3}$. Den „Kehrwert von e“ nennt man auch das „multiplikative Inverse von e“ und man schreibt dafür allgemein oft e^{-1}. Da es sich bei uns hier um die Entschlüsselungszahl handelt (Entschlüsselung = „decryption“) verwenden wir für das Inverse von e den Buchstaben d.*



Mathematische Betrachtung:

Verschlüsselung von A durch Multiplikation mit einer Zahl e: $B = (A \cdot e) \mod n$.

Entschlüsselung durch Multiplikation mit deiner Zahl d (Vermerke auf der rechten Seite in Stichworten, was bei den jeweiligen Umformungen vorgenommen wird, also Gedanken, Rechenregeln,...): *(wobei „d“ das multiplikative Inverse von e ist)*

$(B \cdot d) \mod n$	Verschlüsseln: $B = (A \cdot e) \mod n$ einsetzen
$= ((A \cdot e) \mod n \cdot d) \mod n$	$d < n$, also $d = d \mod n$, Regel mod. Mult.
$= (A \cdot e \cdot d) \mod n$	Regel modulare Multiplikation
$= (A) \mod n \cdot (e \cdot d) \mod n$	$e \cdot d = 1 \mod n$
$= A \mod n$	Botschaft A < Modul n[1]
$= A$	

1 Dies muss generell gelten, da sonst keine Eindeutigkeit. Bsp: CÄSAR mit mod13 statt mod26: „A“ = „N“

Bestimme die Entschlüsselungszahl d zu gegebenen e und n

Tipp: Eine Tabellenkalkulation erleichtert die Erzeugung der Reihen und den Vergleich

n	e	d
32	9	*25*
33	5	*20*
47	13	*29*
124	33	*109*
124	83	*3*
213	85	*208*