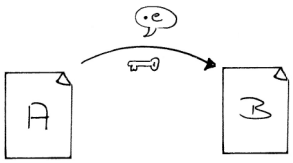
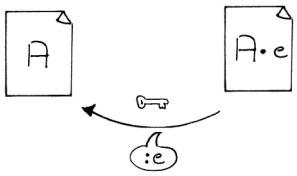
Verschlüsselung mittels Multiplikation und Knacken des Codes

Zunächst das Prinzip ohne Verwendung der modulo-Rechnung

Der Codierer multipliziert Botschaft A mit Zahl e und erhält Geheimbotschaft B.



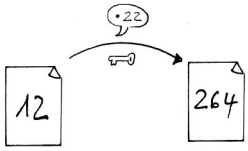
Also: Der Hacker hat die Geheimbotschaft B abgefangen. Nun will er den Klartext A haben, weiß aber nur, dass der Verschlüssler multipliziert hat: B = A · e.



Das Produkt A · e muss der Hacker nun wieder finden, um A bestimmen zu können. Anders gesagt: er muss B als Produkt darstellen („faktorisieren“) und es anschließend durch e dividieren.

Allerdings ist das Problem für ihn zunächst nicht unbedingt eindeutig lösbar...

Bsp.: Die Botschaft lautet 12. Sie wird mit e = 22 verschlüsselt. Die Geheimbotschaft lautet also 12 · 22 = 264.



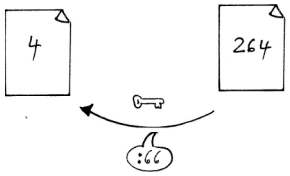
Nun weiß der Hacker nur, dass er 264 in ein Produkt zerlegen muss. Alle möglichen Produkte, die 264 liefern, sind in der Primfaktorzerlegung (PFZ) von B abzulesen:

264 = 2 · 2 · 2 · 3 · 11. Verwende die PFZ für die folgende Aufgabe:

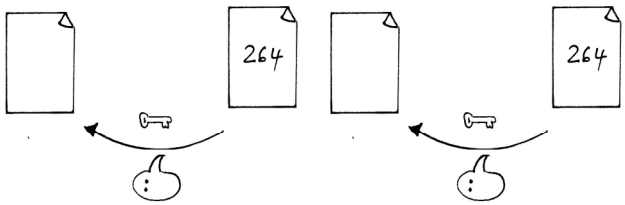
Gib einige Produkte an, die 264 als Ergebnis haben: _____

Die Entschlüsselung erfolgt nun durch Division durch eine Zahl d, die Teiler von 264 ist.

Vermutet der Hacker als Verschlüsselungszahl z.B. d = 2·3·11 = 66, so erhielte er den Klartext durch die Entschlüsselung 264 : 66 = 4.



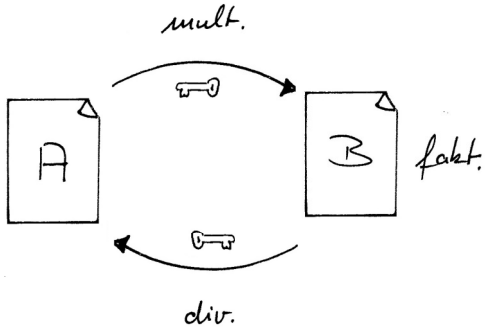
Gib zwei weitere mögliche Entschlüsselungen an:



Man müsste also z.B. (mit großen Teilen der Botschaft) mögliche Schlüssel probieren, bis sich ein vernünftiger Text ergibt.

Auf jeden Fall:

der Codierer muss **multiplizieren,**
der Hacker **faktorisieren**, um durch Division entschlüsseln zu können!



I) Multiplikation und Faktorisierung im Vergleich

Nimm eine Stoppuhr. Stoppe die Zeit, die du für die Rechnungen unten benötigst und notiere sie jeweils. Setzt du bei einer Aufgabe öfters an, so notieren die Einzelzeiten deiner Versuche und addiere sie, wenn du die Aufgabe gelöst hast.

1. ***Multipliziere:***

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

2. ***Faktorisiere:*** *Erzeuge die Primfaktorzerlegung (PFZ) der unten stehenden Zahlen, d.h. stelle sie als Produkt dar, wobei die Faktoren lediglich Primzahlen sind. Manche Aufgaben werden länger dauern als andere. Gehe im Zweifelsfall weiter und versuche dich am Ende mit denen, die du noch nicht geschafft hast (Vergiss nicht, die Zeiten der einzelnen Aufgaben ggf. zu addieren!).*

	PFZ	Benötigte Zeit
204		
1815		
2323		
13261		
107800		

3. *Vergleiche die Zeiten, die sich bei 1. vs. 2. und innerhalb 2. zwischen den einzelnen Aufgaben ergaben:*

   1. vs. 2. - Wozu brauchst du lange/Was geht schnell?

   Innerhalb 2. - Für welche Aufgaben brauchst du lange, welche sind schnell erledigt? Betrachte die Zahlen, die sich bei der Lösung ergeben: An was liegt das?

Erkenntnis:

Begriff: Die modulare Multiplikation ist eine sogenannte **„Einwegfunktion“**: dies bezeichnet einen Vorgang, der in eine Richtung sehr einfach vorzunehmen ist, aber nicht (oder zumindest nur sehr schwer) rückgängig gemacht werden kann.

In der Realität arbeitet man mit großen Primzahlen,

weil hier die Faktorisierung schwierig ist, wie wir schon früher gesehen haben. Einige Zitate dazu:

„Ein 39stelliges Produkt aus zwei Primzahlen (jeweils 20stellig) wird von aktuellen Rechnern und einer entsprechenden Software in weniger als einer Sekunde in die beiden Faktoren zerlegt. Bei 41 Stellen beträgt die benötigte Zeit schon ca. 8 Minuten, bei 43 Stellen 19 Minuten... In der Praxis verwendet man 150-stellige Prim***faktoren***, was 300-stellige Produkte ergibt, die zerlegt werden müssen.“

http://www.dkruse.de/dokumente/netzwerke/Sicher3_Asymm_Verschluesselung.pdf, ausgelesen 13.5.2020

„[...] Als erste RSA-Challenge rief RSA Data Security 1991 einen Wettbewerb ins Leben, in dem es um das Zerlegen von Primzahlprodukten in ihre beiden Faktoren ging. Gelingt eine solche Faktorisierung, dann kommt dies dem Knacken eines RSA-Schlüssels gleich. Die erste Zahl, die der Veranstalter im März 1991 vorgab, hatte 100 Stellen (330 Bits) und wurde daher als RSA-100 bezeichnet. […] Mit 663 Bit ist RSA-200 bis heute die längste Zahl, die öffentlich faktorisiert wurde. […] Falls Sie selbst aktiv werden wollen, können Sie sich an RSA-704 versuchen, für deren Faktorisierung 30.000 Dollar ausgesetzt sind. Bei Redaktionsschluss dieses Artikels hatte noch niemand den Preis für sich beansprucht. Hier ist die Zahl (bevor Sie loslegen, bitte die Korrektheit auf der Internetseite des Wettbewerbs überprüfen):

74037563479561712828046796097429573142593188892312890849362326389727650340282662768919964196251178439958943305021275853701189680982867331732731089309005525051168770632990723963807867100860969625379346505637963 59 [...]“

www.heise.de, ausgelesen 23.4.2020 unter Bezug auf Klaus Schmeh: Kryptografie. Verfahren, Protokolle, Infrastrukturen. Dpunkt Verlag, Heidelberg 2007, *www.schmeh.org*

„Die Zahl $M_{82589933}=2^{82589933}-1$ ist eine Primzahl. Sollte sie der Überprüfung durch unabhängige Rechner standhalten, wäre sie damit die größte bisher gefundene Primzahl. Ausgeschrieben hätte sie über 24 Millionen Dezimalstellen; zum Vergleich: in den gesammelten Werken von William Shakespeare befinden sich nach Schätzungen lediglich 4 bis 5 Millionen Buchstaben!

Bisher sind 50 Mersenne-Primzahlen bekannt, die kleinsten unter ihnen sind $M_2=2^2-1=3$, $M_3=2^3-1=7$ und $M_5=2^5-1=31$. Die größte bisher bekannte ist $M_{77232917}=2^{77232917}-1$. Sollte $M_{82589933}$ die Folgetests bestehen, wäre sie die 51. gefundene Mersenne-Primzahl. Der bisherige Rekord von $M_{77232917} = 2^{77232917}-1$ [...] würde um das 101.660.674-fache überboten worden sein.“

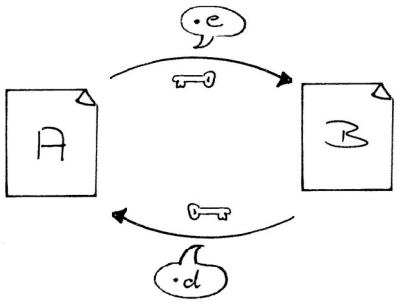
https://www.mathematik.de/dmv-blog/2471-neue-gr%C3%B6%C3%9Fte-primzahl-entdeckt
(Artikel vom 10.12.2018, ausgelesen 04.04.2020)

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: $B = (A \cdot e) \bmod n$.

Entschlüsselung durch Multiplikation mit deiner Zahl d (Vermerke auf der rechten Seite in Stichworten, was bei den jeweiligen Umformungen zur nächsten Zeile vorgenommen wird, also Gedanken, Rechenregeln,...):

$(B \cdot d) \bmod n$ _____

$= ((A \cdot e) \bmod n \cdot d) \bmod n$ $d < n$, also _____

$= (A \cdot e \cdot d) \bmod n$ _____

$= (A) \bmod n \cdot (e \cdot d) \bmod n$ _____

$= A \bmod n$ _____

$= A$ _____

Wie bestimmt man eine Entschlüsselungszahl d?

Benötigt wird das multiplikative Inverse von e (in mod), mit dem dann die Geheimbotschaft B multipliziert wird. Aus der Bedingung an das multiplikative Inverse: e · d = 1 (mod n) folgt die Konstruktionsvorschrift für d: „Gehe die e-Reihe und die n-Reihe durch, bis du auf Elemente stößt, für die gilt: e · d = c · n + 1.

→ d ist eine Entschlüsselungszahl bezüglich mod n."

Im Beispiel:

e = 5 ; n = 33

Gesucht ist also eine Zahl d mit 5 · d = c · 33 + 1.

Gehe 33-er-Reihe durch:	*33*	*66*	*99*	*132*
addiere „1"	*34*	*67*	*100*	*133*

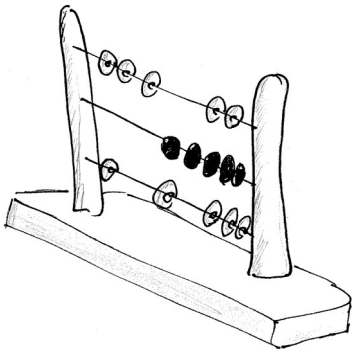
Untersuche „33er + 1": „Welche Zahl ist Vielfaches von 5?" → „100"

100 = 5 · 20 → 5 · 20 = 1 mod 33 → für e = 5 : Ein mögliches d ist d = 20.

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	
33	5	
47	13	
124	33	



Beispiel: Verschlüsseln und entschlüsseln mit modularer Multiplikation

- *Denke dir einen kurzen Satz als Botschaft aus:* _____

_____

- *Verschlüssle ihn mit Hilfe einer selbst gewählten Schlüsselzahl e (mod n). (Tipp: Benutze hierzu die Rechenregeln von Blatt „Rechenregeln in modulo") :*
- *Tausche mit jemandem Geheimnachricht und Schlüssel e (mod n)*
- *Bestimmt die Entschlüsselungszahl d (mod n) und dechiffriert eure Nachrichten.*