Kryptologie

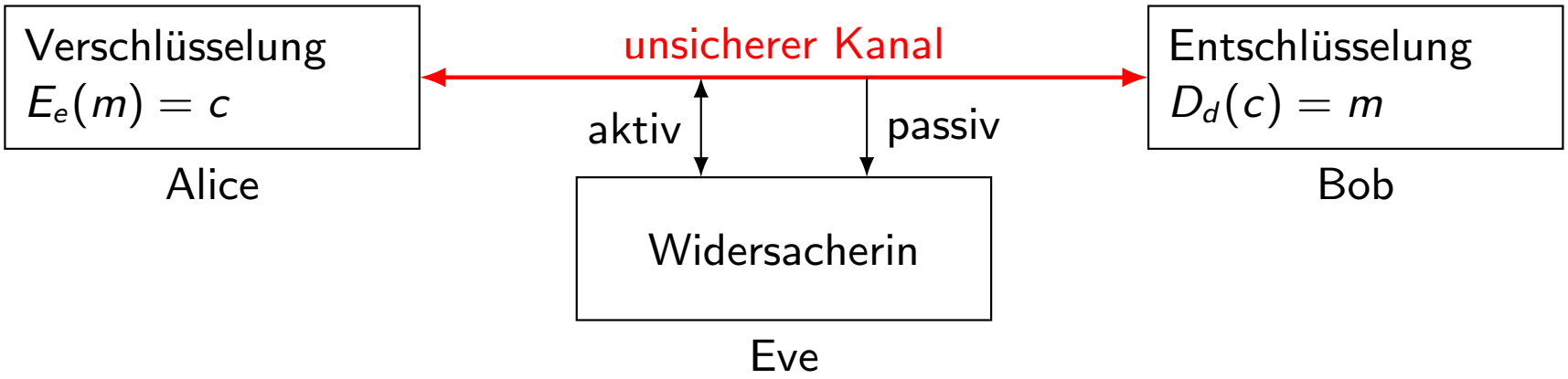
Theorie (Kurz)

Was ist Kryptologie

Die Kryptologie umfasst die Entwicklung und Analyse von Verfahren zur sicheren Kommunikation und Datenübertragung. Ihre Hauptaufgaben sind

- Informationssicherheit: Verschlüsselung und Entschlüsselung von Informationen
- Datenintegrität: Schutz der Informationen vor unbemerkter Veränderung
- Authentifizierung: Bezeugen der Echtheit eines Benutzers oder eines Systems
- Verbindlichkeit: Der Urheber einer Nachricht kann seine Urheberschaft (gegenüber Dritten) nicht abstreiten.

Verschlüsselte Kommunikation



E: Encryption function
D: Decryption function

e: encryption key
d: decryption key

m: message
c: cipher text

Kryptographisches System

Ein *kryptographisches System* (*Kryptosystem*) besteht aus der Menge aller ...

- zulässigen Klartexte $\mathcal{M}$ (*message*),
- verschlüsselten Texte $\mathcal{C}$ (*ciphertext*),
- Schlüssel $\mathcal{K}$ (*key*),
- Verschlüsselungsfunktionen $E_e \colon \mathcal{M} \to \mathcal{C}$ mit $e \in \mathcal{K}$ (*encrypt*),
- Entschlüsselungsfunktionen $D_d \colon \mathcal{C} \to \mathcal{M}$ mit $d \in \mathcal{K}$ (*decrypt*)

mit der Eigenschaft, dass für jeden Schlüssel $e \in \mathcal{K}$ ein Schlüssel $d \in \mathcal{K}$ existiert, so dass für jeden Klartext $m \in \mathcal{M}$ gilt: $D_d(E_e(m)) = m$.

Kurz: Zu jeder Verschlüsselung mit einem Schlüssel e gibt es eine Entschlüsselung mit einem Schlüssel d, mit dem man aus dem Geheimtext den Klartext zurückgewinnen kann.

Kryptographie und Kryptoanalyse

Je nach Blickwinkel unterscheidet man die Kryptologie in die Teilbereiche

- Kryptographie: Entwickeln kryptographischer Systeme und
- Kryptoanalyse: Analysieren und Testen kryptographischer Systeme.

Prinzip von Kerkhoffs

Der niederländische Linguist und Kryptologe Auguste Kerckhoffs (1835–1903) formulierte im Jahr 1883 einen Grundsatz der modernen Kryptographie, welcher besagt, dass die Sicherheit eines (symmetrischen) Verschlüsselungsverfahrens auf der Geheimhaltung des Schlüssels und nicht auf der Geheimhaltung des Verschlüsselungsalgorithmus beruhen soll.

Verschlüsselungsklassen

Kryptographische Systeme lassen sich grob in zwei Klassen einteilen

- Substitutionschiffren: Systeme, bei denen Zeichen oder Zeichengruppen durch andere Zeichen bzw. Zeichengruppen ersetzt werden.
- Transpositionschiffren: Systeme, bei denen die Zeichen einer Nachricht umsortiert (*permutiert*) werden.

Moderne kryptographische Systeme verwenden Substitutionen und Transpositionen um Klartexte in Geheimtexte zu transformieren.

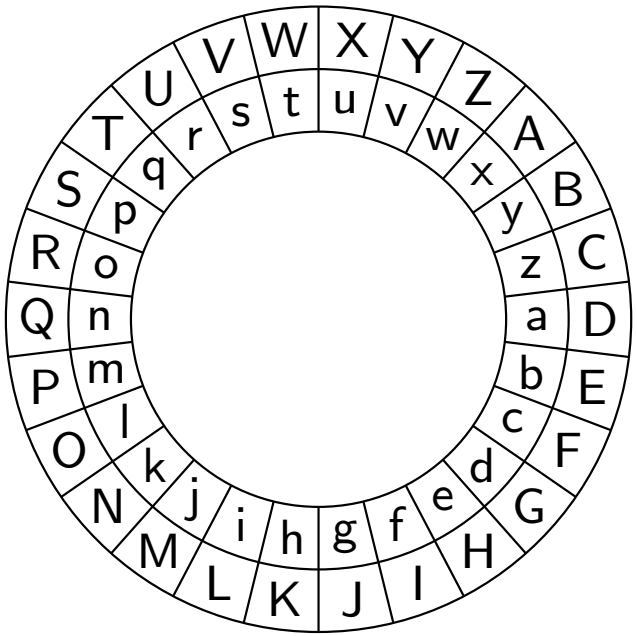
Substitutionschiffren

- Bei einer monographischen Substitution wird *ein* Klartextzeichen durch *ein* Geheimtextzeichen ersetzt.
- Bei einer polygraphischen Substitution wird eine Klartextzeichengruppe durch eine Geheimtextzeichengruppe (gleicher Länge) ersetzt.

Wenn ein Klartextzeichen an jeder Position durch *dasselbe* Geheimtextzeichen ersetzt wird, ist die Substitution monoalphabetisch. Andernfalls wird sie polyalphabetisch genannt, weil bei jeder Ersetzung ein „anderes Alphabet“ verwendet wird.

Cäsar-Chiffre

Die älteste Substitutionschiffre, die Julius Cäsar zugeschrieben wird, ordnet jedem lateinischen Klartextbuchstaben (zyklisch) den um drei Positionen weiter rechts stehenden Geheimtextbuchstaben zu: a $\to$ D, b $\to$ E, . . . , z $\to$ C.



Dieses Kryptosystem ist monographisch und monoalphabetisch. Auch wenn man eine andere der übrigen 24 sinnvollen Rotationen verwendet ist, es nach spätestens 25 Versuchen geknackt.

Das Verfahren von de Vigenère (1523–1596)

Hierzu schreibt man Schlüssel so lange bündig unter oder über den Klartext, bis beide Zeilen gleich lang sind.

Dann „addiert“ man die beiden Texte spaltenweise indem man ihre Zeichennummern modulo der Alphabetlänge berechnet.

Folgendes Beispiel zeigt, wie der Text `'TOPSECRET'` mit dem Schlüssel `'KRYPTO'` verschlüsselt wird.

```
    TOPSECRET
+   KRYPTOKRY
-------------
=   DFNHXQBVR
```

Mit den Zeichenummern

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	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

folgt z. B., dass $\mathtt{T} + \mathtt{K} \Rightarrow (19 + 10) \bmod 26 = 3 \Rightarrow \mathtt{D}$

Vigenère-Quadrat

Mit Hilfe des Vigenère-Quadrats, kann man ohne Rechnung ver- und entschlüsseln.

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

Kryptoanalyse

Da derselbe Klartextbuchstabe oft über einem anderen Schlüsselbuchstaben steht, ist die Vigenère-Chiffre ein *monographisches* und *polyalphabetisches* Verschlüsselungsverfahren. Es ist aber sehr unsicher, da es bei genügend Text wie folgt angegriffen werden kann:

- Um die Schlüsselwortlänge zu bestimmen, sucht man nach identischen kurzen Geheimtexstücken. Denn wenn ein oft vorkommendes Wort per Zufall an mehreren Stellen über den gleichen Schlüsselwortzeichen steht, erzeugt es dort dieselbe Geheimtextsequenz. Dann sucht man eine natürliche Zahl n, welche viele dieser Abstände teilt. Diese Zahl ist ein Kandidat für die Schlüsselwortlänge.
- Danach weiss man welche der Geheimtextzeichen mit dem gleichen Schlüsselwortbuchstaben verschlüsselt wurden und hat es jetzt mit mehreren monoalphabetischen Verschiebechiffren zu tun, die sich mit Ausprobieren oder einer Häufigkeitsanalyse leicht entschlüsseln lassen.

One-Time-Pad

Indem man einen Schlüssel verwendet der aus einer Folge zufälliger Zeichen besteht und so lange wie der Klartext ist, erhält man ein Verfahren, das informationstheoretisch sicher ist; also ausser der Länge des Klartextes keine Rückschlüsse auf den Klartext erlaubt. Dafür muss der Schlüssel folgende Eigenschaften haben:

- Er muss aus kryptographisch guten Zufallszahlen bestehen.
- Er darf nur einmal gebraucht werden.

One-Time-Pad

Indem man einen Schlüssel verwendet der aus einer Folge zufälliger Zeichen besteht und so lange wie der Klartext ist, erhält man ein Verfahren, das informationstheoretisch sicher ist; also ausser der Länge des Klartextes keine Rückschlüsse auf den Klartext erlaubt. Dafür muss der Schlüssel folgende Eigenschaften haben:

- Er muss aus kryptographisch guten Zufallszahlen bestehen.
- Er darf nur einmal gebraucht werden.

Das Verfahren hat dennoch einige gewichtige Nachteile:

- Der Schlüssel muss sicher transportiert werden.
- Es müssen genügend gute Schlüssel vorhanden sein.

Transpositionschiffren

Zur Erinnerung: Eine Transposition bedeteut in der Kryptographie die Permutation (Umstellung) der Zeichen.

Für die *Spaltentransposition* schreibt man den Text so unter den Schlüssel, dass die Zeilen (evtl. mit Ausnahme der letzten) gleich lang wie der Schlüssel sind. Danach wird der Text in alphabetischer Reihenfolge der Schlüsselbuchstaben von oben nach unten neu zusammengesetzt. Kommt ein Zeichen mehrfach vor, liest man die linke Spalte vor der rechten.

SARNEN
ANGRIF
FIMMOR
GENGRA
UEN

$\Rightarrow$

A	E	N	N	R	S
NIEE	IOR	RMG	FRA	GMNN	AFGU

Kryptoanalyse

Das Verfahren bietet in dieser Form keine grosse Sicherheit.

Wenn man aber auf den so verschlüsselten Geheimtext eine weitere Spaltentransposition anwendet, kann man die Sicherheit erhöhen wenn die Länge des zweiten Schlüssels teilerfremd zur Länge des ersten Schlüssels ist. Man spricht dann von einer *doppelten Spaltentransposition*. Denoch kann auch dann das Verfahren gebrochen werden.

Diffie-Hellman-Merkle-Schlüsselaustausch

Das Problem: Wie können zwei Kommunikationspartner über einen unsicheren Kanal einen gemeinsamen Schlüssel für die Verschlüsselung von Nachrichten erzeugen, ohne diesen direkt auszutauschen?

Asymmetrische Kryptosysteme

Lösung: Wir benötigen eine Berechnungsvorschrift (Funktion) die aus einer Zahl x (dem „Geheimnis“) eine Zahl y berechnet und idealerweise folgende Eigenschaften hat:

- $x \longrightarrow y$ soll „leicht“ berechenbar sein.
- $y \longrightarrow x$ soll „schwer“ berechenbar sein.

Damit können wir einen unsicheren Kanal verwenden, um das „verschlüsselte“ Geheimnis y zu übertragen. Denn auch wenn der Angreiferin y in die Hände fällt, so muss sie für die Rekonstruktion von x so viel Zeit, oder Ressourcen aufwenden, dass das Geheimnis x für sie wertlos wird.

Multiplikative prime Restklassengruppen

Stellen wir für eine Primzahl p alle möglichen Produkte der Zahlen $1 \leq a < p$ modulo p in einer Tabelle zusammen, erkennen wir:

- Für alle $a, b \in \mathbb{Z}_p^*$ gilt $a \cdot b \in \mathbb{Z}_p^*$.
- Für alle $a, b, c \in \mathbb{Z}_p^*$ gilt $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- Es gibt ein $e \in \mathbb{Z}_p^*$, so dass $e \cdot a = a \cdot e = a$ für alle $a \in \mathbb{Z}_p^*$.
- Für jedes $a \in \mathbb{Z}_p$ gibt es ein $b \in \mathbb{Z}_p$ mit $a \cdot b = b \cdot a = e$
- Für alle $a, b \in \mathbb{Z}_p^*$ gilt $a \cdot b = b \cdot a$

e wird *neutrales Element* der Multiplikation $(*)$ genannt und b mit $a \cdot b = e$ heisst *inverses* Element von a (aka a^{-1}).

Eine Menge mit dieser Struktur ist eine *(kommutative) Gruppe*.

Ein Element $a \in \mathbb{Z}_p^*$ ist ein erzeugendes Element (oder Erzeuger) von $\mathbb{Z}_p^*$, wenn die Potenzen $(a^1 \bmod p)$, $(a^2 \bmod p)$, $\ldots$, $(a^{p-1} \bmod p)$ alle Elemente von $\mathbb{Z}_p^*$ erzeugen.

Beispiel: $\mathbb{Z}_5^*$

$\mathbb{Z}_5^*$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

neutrales Element: $e = 1$

inverse Elemente: $1^{-1} = 1$ denn $1 \cdot 1 = 1$
$2^{-1} = 3$ denn $2 \cdot 3 = 1$
$3^{-1} = 2$ denn $3 \cdot 2 = 1$
$4^{-1} = 4$ denn $4 \cdot 4 = 1$

$1^1 = 1,\ 1^2 = 1,\ a^3 = 1,\ a^4 = 1 \quad \Rightarrow \quad 1$ ist nicht erzeugend

$2^1 = 2,\ 2^2 = 4,\ 2^3 = 3,\ 2^4 = 1 \quad \Rightarrow \quad 2$ ist erzeugend

$3^1 = 3,\ 3^2 = 4,\ 3^3 = 2,\ 3^4 = 1 \quad \Rightarrow \quad 3$ ist erzeugend

$4^1 = 4,\ 4^2 = 1,\ 4^3 = 4,\ 4^4 = 1 \quad \Rightarrow \quad 3$ ist nicht erzeugend

Diskretes-Logarithmus-Problem

Sei p eine ungerade Primzahl und a ein erzeugendes Element von $\mathbb{Z}_p^*$. Für ein $b \in \mathbb{Z}_p^*$ ist der *diskrete Logarithmus* von b zur Basis a die eindeutige ganze Zahl x mit $0 \leq x \leq p-2$, so dass $b = a^x \bmod p$.

Das Bestimmen von x aus gegebenem p, a und b wird das *Diskrete-Logarithmus-Problem* (DLP) genannt. In der Theorie handelt es sich um ein einfaches Problem, denn wir müssen solange $a^x \bmod p$ für $x = 0, 1, \ldots$ berechnen, bis wir b erhalten. Dies ist jedoch nicht effizient, da $O(p)$ Multiplikationen benötigt werden. Da kein kein effizienter Algorithmus bekannt ist, beruht die Sicherheit verschiedener kryptographischer Verfahren beruht auf der Schwierigkeit des DLP.

Beispiel

Bestimme $\log_3 5$ in $\mathbb{Z}_7^*$

Suche einen Exponenten x, so dass $3^x \bmod 7 = 5$

Probieren: $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$

Also $\log_3 5 = 5$, denn $3^5 \bmod 7 = 5$

Das DHM-Protokoll

1. Alice und Bob einigen sich „öffentlich“ auf eine grosse Primzahl p und einen Generator g von $\mathbb{Z}_p^*$.
2. Alice und Bob wählen jeweils eine geheime Zufallszahl a bzw. b aus der Menge $\{1, 2, \ldots, p-1\}$.
3. - Alice berechnet $A = g^a \bmod p$ und sendet A an Bob.
   - Bob berechnet $B = g^b \bmod p$ und sendet B an Alice.
4. - Alice berechnet mit B von Bob $K_1 = B^a \bmod p$.
   - Bob berechnet mit A von Alice $K_2 = A^b \bmod p$.

Die von Alice und Bob berechneten Zahlen sind gleich, denn

$$K_1 = B^a \bmod p = \left(g^b\right)^a \bmod p = g^{b \cdot a} \bmod p$$

$$K_2 = A^b \bmod p = \left(g^a\right)^b \bmod p = g^{a \cdot b} \bmod p$$

$$\text{Kommutativität} \Rightarrow g^{b \cdot a} = g^{a \cdot b} \Rightarrow K_1 = K_2$$

Beispiel

Zeige, wie Alice und Bob den gemeinsamen Schlüssel berechnen, nachdem sie sich auf die Primzahl $p = 13$ sowie den Generator $g = 2 \in \mathbb{Z}_{13}^*$ geeinigt haben. Alice wählt als geheime Zufallszahl $a = 5$ und Bob wählt $b = 8$.

A berechnet $g^a \bmod p$ $2^5 \bmod 13 = 6$	sendet 6 $\longrightarrow$	B erhält $g^a \bmod p = 6$
A erhält $g^b = 9 \bmod p$	$\longleftarrow$ sendet 9	B berechnet $g^b \bmod p$ $2^8 \bmod 13 = 9$
A berechnet $(g^b)^a \bmod p$ $9^5 \bmod 13 = 3$		B berechnet $(g^a)^b \bmod p$ $6^8 \bmod 13 = 3$
A verwendet symm. Verfahren mit Schlüssel $k = 3$	Nachrichten $\longleftrightarrow$	B verwendet symm. Verfahren mit Schlüssel $k = 3$

Obwohl Eve die Primzahl p, den Generator g und die gesendeten Zahlen a und b kennt, kann sie wegen der Schwierigkeit des DLP die geheimen Exponenten a und b nicht bestimmen, die es braucht, um den gemeinsamen Schlüssel zu berechnen.

Berechnung modularer Potenzen

Im Gegensatz zum diskreten (=modularen) Logarithmus ist das berechnen modularer Potenzen effizient mit dem *Square-and-Multiply Algorithmus* berechenbar.

Zuerst halten wir fest, dass für ein Produkt von zwei Zahlen

$$(a \cdot b) \bmod m = (a \bmod m) \cdot (b \bmod m)$$

gilt womit die Produkte am Ende immmer kleiner als m sind.

Um zum Beispiel $x = 5^{22} \bmod 7$ zu berechnen, Zerlegen wir zuerst den Exponenten in eine Summe von Zweierpotenzen.

$$22 = 16 + 4 + 2, \text{ denn } 5^{22} = 5^{16+4+2} = 5^2 \cdot 5^4 \cdot 5^{16}$$

Dann berechnen wir durch Quadrieren schrittweise die Potenzen 5^1, 5^2, 5^4, 5^8, 5^{16}, bis zum grössten Zweierpotenz-Exponenten. Anschliessend müssen wir nur noch schrittweise die Potenzen mit den oben bestimmten drei Zweierpotenz-Exponenten multiplizieren.

Berechnung modularer Potenzen

Im Gegensatz zum diskreten (=modularen) Logarithmus ist das berechnen modularer Potenzen effizient mit dem *Square-and-Multiply Algorithmus* berechenbar.

Zuerst halten wir fest, dass für ein Produkt von zwei Zahlen

$$(a \cdot b) \bmod m = (a \bmod m) \cdot (b \bmod m)$$

gilt womit die Produkte am Ende immmer kleiner als m sind.

Um zum Beispiel $x = 5^{22} \bmod 7$ zu berechnen, Zerlegen wir zuerst den Exponenten in eine Summe von Zweierpotenzen.

$$22 = 16 + 4 + 2, \text{ denn } 5^{22} = 5^{16+4+2} = 5^2 \cdot 5^4 \cdot 5^{16}$$

Dann berechnen wir durch Quadrieren schrittweise die Potenzen 5^1, 5^2, 5^4, 5^8, 5^{16}, bis zum grössten Zweierpotenz-Exponenten. Anschliessend müssen wir nur noch schrittweise die Potenzen mit den oben bestimmten drei Zweierpotenz-Exponenten multiplizieren.

$$5^1 \bmod 7 = 5 \qquad x = 1$$
$$x = 1$$

Berechnung modularer Potenzen

Im Gegensatz zum diskreten (=modularen) Logarithmus ist das berechnen modularer Potenzen effizient mit dem *Square-and-Multiply Algorithmus* berechenbar.

Zuerst halten wir fest, dass für ein Produkt von zwei Zahlen

$$(a \cdot b) \bmod m = (a \bmod m) \cdot (b \bmod m)$$

gilt womit die Produkte am Ende immmer kleiner als m sind.

Um zum Beispiel $x = 5^{22} \bmod 7$ zu berechnen, Zerlegen wir zuerst den Exponenten in eine Summe von Zweierpotenzen.

$$22 = 16 + 4 + 2, \text{ denn } 5^{22} = 5^{16+4+2} = 5^2 \cdot 5^4 \cdot 5^{16}$$

Dann berechnen wir durch Quadrieren schrittweise die Potenzen 5^1, 5^2, 5^4, 5^8, 5^{16}, bis zum grössten Zweierpotenz-Exponenten. Anschliessend müssen wir nur noch schrittweise die Potenzen mit den oben bestimmten drei Zweierpotenz-Exponenten multiplizieren.

$$5^1 \bmod 7 = 5 \qquad x = 1$$
$$x = 1$$