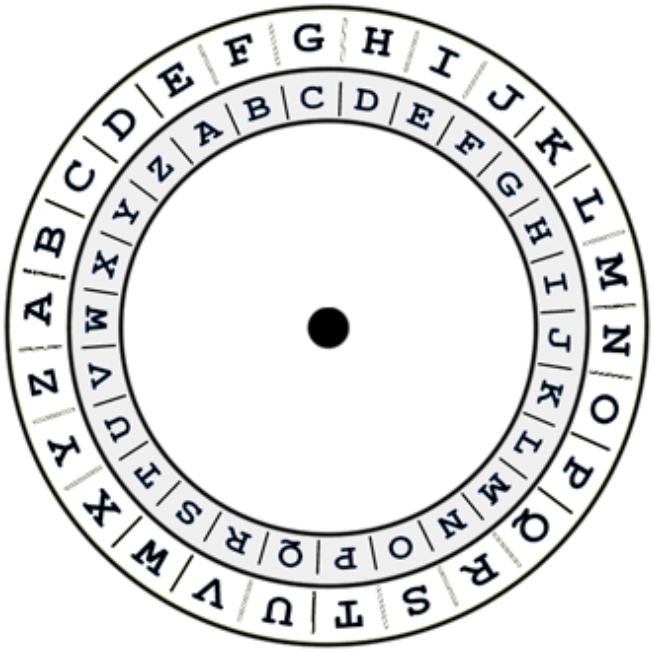
Kryptographie

JQJGKIIAJSENFAHKYDVQAPSWOCWJVWJZANAI

Rotationsverschlüsselung: mitläufig, von außen nach innen



https://blog.supertext.ch/2015/01/top-secret-beruehmte-geheimschriften/ (09.12.2024)

Kryptographie

ATADZBBJARFWEJKZLGOTJURNVHNAONAKSWJB

Rotationsverschlüsselung: gegenläufig, von innen nach außen

https://tibs.at/index.php/content/geheimschriften-im-unterricht-ausgewaehlte-beispiele-der-kryptographie (09.12.2024)

Kryptographie

NWZNUIUZNREAKJTNOEWDMDAEMOSRECGENHAM
JQJGKIIAJSENFAHKYDVQAPSWOCWJVWJZANAI
ATADZBBJARFWEJKZLGOTJURNVHNAONAKSWJB

NUN KOMMEN WIR JEDOCH ZU ETWAS GANZ ANDEREM

Transpositionsverschlüsselung: Skytale

http://www.mathe.tu-freiberg.de/~hebisch/cafe/kryptographie/skytale.html
(09.12.2023)

1. Versuch dreispaltig

N W Z
N U I
U Z N
R E A
K J T
N O E
W D M
D A E
M O S
R E C
G E N
H A M

falsch!

2. Versuch vierspaltig

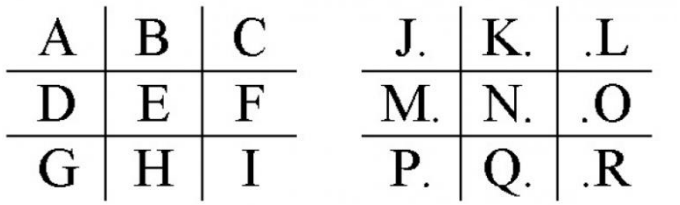
N W Z N
U I U Z
N R E A
K J T N
O E W D
M D A E
M O S R
E C G E
N H A M

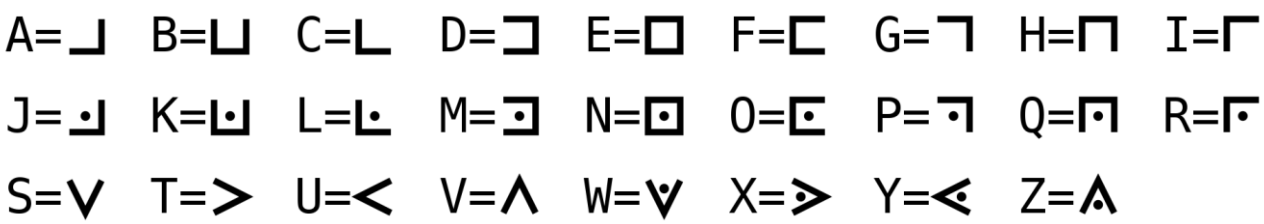
richtig!

Kryptographie

NUNKOMMENWIRJEDOCHZUETWASGANZANDEREM

Freimaureralphabet: Nicht-alphabetische Stellvertreterzeichen





http://www.quadoo.de/freimaurer.html *(09.12.2024)*

Ver- und Entschlüsselung mit dem RSA-Verfahren

RSA: Das erste Verfahren, das die Anforderungen an die Public-Key-Kryptographie erfüllte. Erfunden wurde es 1977 von Ron **Rivest**, Adi **Shamir** und Leonard **Adleman**.

Das Problem: Bob will an Alice eine Nachricht schicken, die niemand sonst entziffern können darf.

1) Alice wählt zwei möglichst große **Primzahlen**, *p* und *q*.
   Der Einfachheit halber nehmen wir aber an, dass Alice ***p = 17*** und ***q = 11*** wählt.
   Diese Zahlen muss sie selbstverständlich geheim halten.

Primzahl: Ganze Zahl, die nur durch 1 und sich selbst teilbar ist. Die erste Primzahl mit mehr als 100 Dezimalstellen, nämlich 157, wurde 1952 gefunden, die letzte (2018) gefundene Primzahl hat 24.862.048 Dezimalstellen.

2) Alice multipliziert die Primzahlen miteinander und erhält als Ergebnis
   N = p x q = 17 x 11 = 187

   Jetzt wählt sie eine weitere Zahl, ***e***, nehmen wir an: ***e = 7***.
   e und *(p-1)* ***x*** *(q-1)* müssen teilerfremd sein!
   Zwei Zahlen sind **teilerfremd**, wenn ihr größter gemeinsamer Teiler 1 ist.
   (p-1) x (q-1) also: *(17-1) x (11-1) = 16 x 10 = 160*
   der größte gemeinsame Teiler von 160 und 7 ist 1, sie sind **teilerfremd**.

3) Jetzt kann Alice die beiden Zahlen ***e (=7)*** und ***N (=187)*** in einem öffentlichen Verzeichnis abdrucken lassen.
   Da diese beiden Zahlen für die Verschlüsselung benötigt werden, müssen sie natürlich allen zugänglich sein, die eine verschlüsselte Mitteilung an Alice schicken wollen. Sie sind der sogenannte **öffentliche Schlüssel**.
   Die Zahl ***e*** ist nicht für Alice reserviert, sie kann auch Bestandteil aller anderen öffentlichen Schlüssel sein.
   Allerdings muss sich ***N*** bei allen Schlüsseln unterscheiden!

nach: Singh, Simon (2012): Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet, aus dem Englischen von Klaus Fritz, 11. Auflage, München: dtv, 436-437.

Ver- und Entschlüsselung mit dem RSA-Verfahren

Das Problem: Bob will an Alice eine Nachricht schicken, die niemand sonst entziffern können darf.

4) Damit eine Mitteilung verschlüsselt werden kann, muss die Mittelung zunächst in eine Zahl umgewandelt werden, ***M***. Beispielsweise kann ein Wort gemäß **ASCII** in eine binäre Zahl umgewandelt werden, die dann zu Verschlüsselungszwecken als Dezimalzahl ***M*** betrachtet werden kann.

ASCII (**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange): Ein Standard zur Umwandlung von alphabetischen und anderen Zeichen in binäre Zahlen.

Dieses ***M*** wird nun verschlüsselt und ergibt den Geheimtext ***C*** nach folgender Formel:

$$\boldsymbol{C = M^e \ (\mathbf{mod}\ p \times q)}.$$

mod = modulo: Teilt man eine natürliche Zahl *a* durch eine natürliche Zahl *m*, so erhält man einen Rest *r*. Für diesen Rest gilt $0 \leq r \leq m - 1$. Die sogenannte Modulo-Funktion liefert zu gegebenen Zahlen *a* und *m* gerade diesen Rest r. Man schreibt auch: $a \ (\mathrm{mod}\ m) = r$.
Beispiel: 7:2 = 3, Rest 1, also 7 (mod 2) = 1

5) Nehmen wir an, Bob will Alice mit dem Buchstaben ***X*** einen symbolischen Kuss schicken. In ASCII wird ***X*** durch 1011000 dargestellt, was der Dezimalzahl 88 entspricht. Daher ***M = 88***. (Die Umrechnung: $1x2^6+0x2^5+1x2^4+1x2^3+0x2^2+0x2^1+0x2^0=64+0+16+8+0+0+0$.)

nach: Singh, Simon (2012): Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet, aus dem Englischen von Klaus Fritz, 11. Auflage, München: dtv, 436-437.

Ver- und Entschlüsselung mit dem RSA-Verfahren

Das Problem: Bob will an Alice eine Nachricht schicken, die niemand sonst entziffern können darf.

6) Um diese Mitteilung zu verschlüsseln, sucht Bob zunächst Alice‘ öffentlichen Schlüssel heraus, also ***N = p x q* = 187** und ***e* = 7**. Diese Zahlen setzt er in die Verschlüsselungsformel ***C* = M^e** (**mod *p* x *q***) ein. Das ergibt für ***M*** = 88: ***C*** = 88^7 (**mod 187**). [88^7 = 40.867.559.636.992] | 88^7 (mod 187) = 11.

7) Bob schickt also seinen Text **M → *C*** = 11, an Alice.

8) Die Exponenten in der **Modul-Arithmetik** sind **Einwegfunktionen**: Man kommt mit dem öffentlichen Schlüssel (***p x q*** und ***e***) sehr leicht von ***M*** zu ***C***, aber bei den im Alltagsbetrieb zur Verfügung stehenden **Primzahlen** mit mehreren hundert Stellen ist es selbst mit den größten heutigen Computer-Netzwerken auch nach Monaten nicht möglich, zurück von ***C*** nach ***M*** zu kommen.

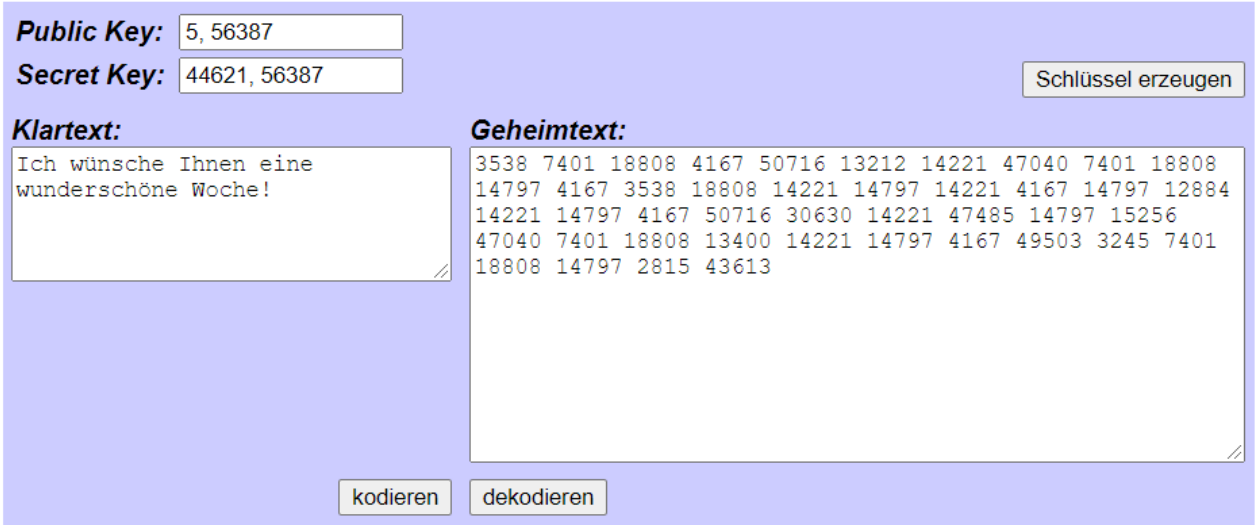
9) Alice jedoch kann die Botschaft entschlüsseln, weil sie ***p*** und ***q*** kennt. Sie berechnet den **Dechiffrierschlüssel *d***, der als **privater Schlüssel** bezeichnet wird.
Die Zahl ***d*** wird mit folgender Formel berechnet:
e* x *d = 1 (mod (*p*-1) x (*q*-1)) → 7 x *d* = 1 (mod 16 x 10) → 7 x *d* = 1 (mod 160) → *d* = 23 [weil 7 x 23 = 161 und das ist 1 (mod 160)]

10) Um Bobs Mitteilung zu entschlüsseln, benutzt Alice nun einfach die folgende Formel:
***M* = C^d (mod 187)** → *M* = 11^{23} (mod 187) [11^{23} = 895.430.243.255.237.372.246.531] | 11^{23} (mod 187) = 88 | = **X**

nach: Singh, Simon (2012): Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet, aus dem Englischen von Klaus Fritz, 11. Auflage, München: dtv, 436-437.

Ver- und Entschlüsselung mit dem RSA-Verfahren

3538 7401 18808 4167 50716 13212 14221 47040 7401 18808 14797 4167 3538 18808 14221 14797 14221 4167 14797 12884 14221 14797 4167 50716 30630 14221 47485 14797 15256 47040 7401 18808 13400 14221 14797 4167 49503 3245 7401 18808 14797 2815 43613

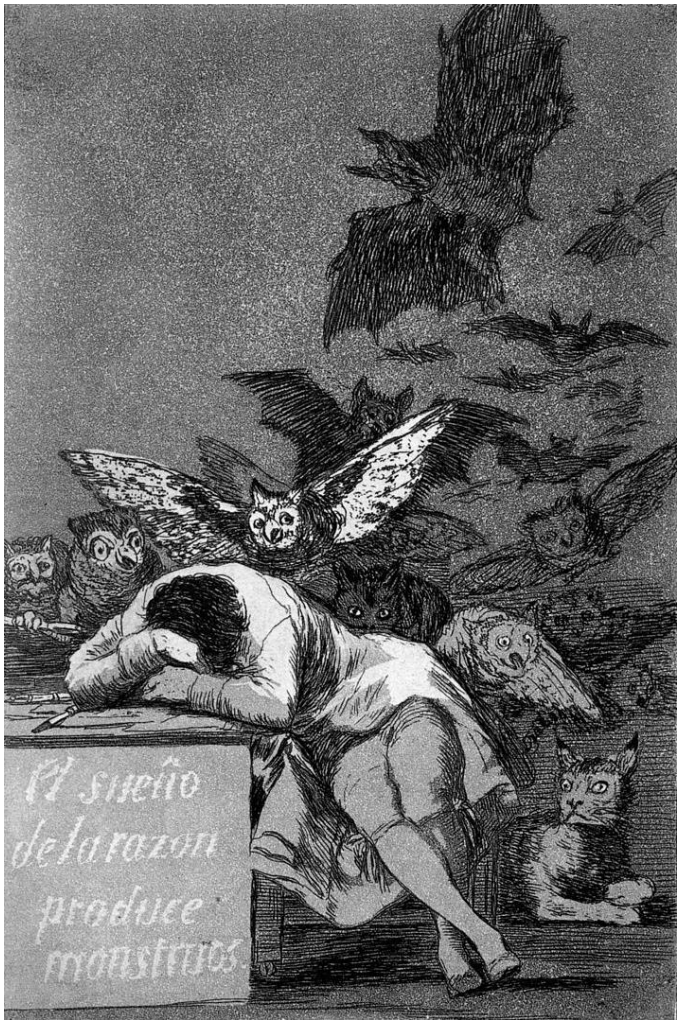


http://www.nord-com.net/h-g.mekelburg/krypto/mod-asym.htm#rsa (09.12.2024)

Aufklärung

„AUFKLÄRUNG ist der Ausgang des Menschen aus seiner selbstverschuldeten Unmündigkeit. Unmündigkeit ist das Unvermögen, sich seines Verstandes ohne Leitung eines anderen zu bedienen. Selbstverschuldet ist diese Unmündigkeit, wenn die Ursache derselben nicht am Mangel des Verstandes, sondern der Entschließung und des Mutes liegt, sich seiner ohne Leitung eines andern zu bedienen. Sapere aude! Habe Mut, dich deines eigenen Verstandes zu bedienen! ist also der Wahlspruch der Aufklärung.“

Immanuel Kant: Was ist Aufklärung? (1784)



Francisco de Goya: Der Schlaf der Vernunft gebiert Ungeheuer (1799)

„Die Kunst, Bücher zu lesen“

Inhaltsanzeige.

Bergk, Johann Adolf (1799): Die Kunst, Bücher zu lesen. Nebst Bemerkungen über Schriften und Schriftsteller, Jena: Hempel, XIII-XVI.

„Die Kunst, Bücher zu lesen“

Vorrede

[...] Unser ganzes Leben soll ein Streben sein, uns **mündig** zu machen. Alle unsere Kräfte sollen **selbsttätig**, und unser Charakter soll **selbstständig** werden. Wir sollen uns weder durch die Natur noch durch Menschen beugen lassen, sondern uns stets als **freie unabhängige Wesen** behaupten. Was wir also tun, und was wir beschließen, muss auf die Entwicklung und auf die Erziehung unserer Kräfte zur **Freiheit** und **Selbsttätigkeit** abzielen, damit wir im Stande sind, den **Forderungen unsrer Vernunft** Folge zu leisten, und damit wir stets unsere **Würde** gegen das blinde Geschick behaupten können. –

Was gibt es nun für ein zweckmäßigeres Mittel, **unsern Geist auszubilden**, als das Bücherlesen? Wo finden wir einen so reichen und so mannigfaltigen Stoff, unsere Kräfte zu üben und uns Interesse für das **Selbstdenken** einzuflößen als in gedankenreichen Büchern? Sind nicht die Schätze der Vorwelt und die Ausbeute unserer Zeitgenossen in diesen **Geistesmagazinen** niedergelegt? Wie viel muss uns also daran gelegen sein, zu wissen, wozu und wie wir Bücher lesen sollen! [...]

Alles Mechanische muss uns ein Gräuel sein, weil wir uns dabei der Materie zum Opfer bringen. [...] Wir müssen uns gewöhnen, unsern Körper als ein Instrument zu betrachten, das der Geist bloß zur Ausführung seiner Zwecke braucht, und das weiter keinen Werth hat, wenn es nicht **im Dienste des Geistes** genutzt wird; dann werden wir uns auch von dem Boden erheben, unsere Blicke gen Himmel richten, und das Leben als eine Schule ansehen, wo wir **frei und mündig** werden sollen. Wer nicht manchmal das Leben verachtet, ist dieses Göttergeschenkes nicht würdig, und wer sich nicht öfters von der Materie losreißt, ahnt nicht die **hohe Bestimmung**, die ihm die Gottheit aufgegeben hat. Wenn wir also das Leben aus moralischen Gesichtspunkten betrachten, so werden wir weder die Gefahr noch die Mühe achten, die es uns kostet, uns von einer Last zu befreien, die uns entehrt, und uns von Fesseln loszureißen, die uns die Spanne unsers Daseins als das höchste Ziel ansehen lassen.

Bergk, Johann Adolf (1799): Die Kunst, Bücher zu lesen. Nebst Bemerkungen über Schriften und Schriftsteller, Jena: Hempel, IV-X ; Hervorhebungen: J.T.).

„Die Kunst, Bücher zu lesen“

Vorrede

In Ideen muss der Mensch leben lernen, und **nach Idealen** muss er sein Streben formen. Durch diese allein gibt er zu erkennen, dass er höherer Abkunft ist, das er kein Sohn des Staubes, sondern ein **Götterkind** ist. Wer noch nicht in der **Unendlichkeit** einheimisch ist, wird weder sich noch die Natur richtig beurteilen lernen. Wer noch nicht **im Lande der Ideale**, welche **die edelsten Produkte der Menschheit** sind, lebt, wandelt noch im Finstern: er schweift in einem Labyrinthe umher, woraus er keinen Ausgang findet, und er wird kein Ziel gewahr, dessen Erreichung seine Arbeit krönt. Er dreht sich in ewigen Kreisen umher, und ist ein **Spielball des Schicksals**, das ihn wie jede andere Sache behandelt, weil er die Welt und die Menschen nicht mit den **Augen der Vernunft** betrachtet, sondern alles nach bloßen Begriffen modeln will.

Mein Zweck bei dieser Arbeit war, das Bücherlesen aus einem Gesichtspunkte zu betrachten, der seinen Ursprung in der **Vernunft** hat. Ich wollte es als eine Bildungsanstalt zur **Erweckung unserer Anlagen** und zur **Vervollkommnung unserer Kräfte** angesehen wissen. Ich ging darauf aus, dem Leser zu zeigen, wie er sich durch das Lesen **Selbsttätigkeit der Denkkraft**, und **Selbstständigkeit des Charakters** erwerben könne. Er sollte sich zwar Materialien einsammeln, aber sich nicht von ihnen unterjochen lassen, sondern sie frei beherrschen, und als Ausgebemünze ansehen lernen; denn was nützt uns ein Reichtum an Kenntnissen, den wir nicht **zu unserm Wohl und zum Heil unserer Nebenmenschen** gebrauchen können! Wir sind bei allem Überflusse lebendig tot und gleichen dem Geizigen, der sammelt, um zu sammeln. Welch‘ eine nichtswürdige Beschäftigung dies für Menschen sei, kann jeder daraus abnehmen, dass alle Stoffe, die der Mensch einsammelt, bloß zu **Erreichung von Vernunftzwecken** bestimmt seien, und dass alle Sachen den Menschen als **mit Freiheit begabten Wesen** dienen sollen.

Bergk, Johann Adolf (1799): Die Kunst, Bücher zu lesen. Nebst Bemerkungen über Schriften und Schriftsteller, Jena: Hempel, IV-X ; Hervorhebungen: J.T.).

„Die Kunst, Bücher zu lesen“

Vorrede

Das Lesen soll uns zur **Selbsttätigkeit** erziehen; alle Anlagen sollen durch dasselbe erweckt, und alle Kräfte sollen durch dasselbe vervollkommnet werden. Die Bücher sind deshalb zur **Beförderung unserer Mündigkeit** sehr tauglich, weil sie reich an interessanten und mannigfaltigen Stoffen sind, und weil sie dem Leser auch eine Kenntnis von dem verschaffen, wohin seine Augen nicht reichen, und sein Fuß nicht tritt.

Sie verbinden **mit Anschauung zugleich Gedanken**, und **mit Empfindungen Ideale**; die Welt und die Natur hingegen umringt uns bloß mit Anschauungen, wodurch zwar unsere Sinnlichkeit befriedigt, aber nur auch zu oft die Tätigkeiten unsers Verstandes und unserer Vernunft erstickt werden.

Die Bücher muntern uns zum Denken auf, zeigen uns den Weg, den wir gehen müssen, um Aufschluss über uns und über die Welt zu erhalten. Sie setzen mehrere Kräfte zugleich in Tätigkeit, und verursachen uns durch ein solches Spiel ein **Vergnügen**, das ein Reizmittel zu neuen Anstrengungen ist. Sie sind also für denjenigen, der sich selbst bilden muss, oder der noch nicht an Kopf und Herz mündig worden ist, ein zweckmäßigeres Bildungsmittel als irgendeines, das wir selbst **zu unserm Heile** nutzen können.

Bergk, Johann Adolf (1799): Die Kunst, Bücher zu lesen. Nebst Bemerkungen über Schriften und Schriftsteller, Jena: Hempel, IV-X ; Hervorhebungen: J.T.).

„Die Kunst, Bücher zu lesen“

Inhaltsanzeige

I. Über **Bücher und Schriftstelle**r
II. Was heißt **Bücher lesen**?
III. Was versteht man unter der **Kunst, Bücher zu lesen**?
IV. Welches ist der **Zweck des Lesens**?
V. Welche **Vermögen und Kräfte** besitzt der Mensch **von Natur**?
VI. Auf welche Art und durch welche Mittel kann der Mensch **seine Anlagen und Kräfte entwickeln und ausbilden**?
VII. Über **schöne Künste**
VIII. Was hat die **Lektüre schöner Kunstwerke** für einen Zweck?
IX. Wie muss man schöne Kunstwerke lesen, um den **Geschmack zu bilden**?
X. Was haben **Romane** für einen Zweck?
XI. Wie muss man **Romane** lesen?
XII. Wie müssen **Romane** beschaffen sein, welche für Muster des Geschmacks gelten sollen?
XIII. Wie muss man **schlechte Romane** lesen, und welchen Nutzen hat die Lektüre desselben?
XIV. Über **Ritter- und Geisterromane**
XV. Über **Geschichts- und historisch-politische Romane**
XVI. Über **moralische Erzählungen**
XVII. Über **empfindelnde und mystische Romane**
XVIII. Über **laszive Romane**
XIX. Bemerkungen über einige **Romanschriftsteller**

Bergk, Johann Adolf (1799): Die Kunst, Bücher zu lesen. Nebst Bemerkungen über Schriften und Schriftsteller, Jena: Hempel, XIII-XVI ; Hervorhebungen: J.T.).

„Die Kunst, Bücher zu lesen“

Inhaltsanzeige

XX. Welches ist der Zweck der Lektüre von **Lustspielen**, und wie muss man dieselben lesen?
XXI. Welches ist der Zweck der Lektüre von **Schauspielen**, und wie muss man diese lesen?
XXII. Warum liest man **Trauerspiele** und wie muss man diese lesen?
XXIII. Bemerkungen über **Lust- Schau- und Trauerspieldichter**
XXIV. Welches ist der Zweck der Lektüre von **Gedichten**, und wie muss man diese lesen?
XXV. Bemerkungen über **Dichter und Gedichte**
XXVI. Mit welchen Werken der schönen Künste muss die **Jugend** den Anfang ihrer Lektüre machen?
XXVII. Welches ist der Zweck der Lektüre von **philosophischen Werken**, und wie muss man diese lesen?
XXVIII. Auf welche Weise und in welcher Ordnung muss man **Kants Schriften** studieren?
XXIX. Bemerkungen über **philosophische Schriftsteller**
XXX. Warum liest man **vermischte Schriften**, und wie muss man dieselben lesen?
XXXI. Bemerkungen über **Schriften vermischten Inhalts**
XXXII. Welchen Zweck hat die Lektüre von **Geschichtswerken**, und wie muss man sie lesen?
XXXIII. Bemerkungen über **Geschichtsschreiber**
XXXIV. Wie muss man wissenschaftliche Werke in der **Theologie, Jurisprudenz, Arzneiwissenschaft usw.** lesen?
XXXV. Warum liest man **periodische Schriften**, und wie muss man sie lesen?
XXXVI. Bemerkungen über **periodische Schriften**
XXXVII. Warum studiert man **alte Sprachen**, und wie muss man die alten Klassiker lesen?
XXXVIII. Bemerkungen über einige **Hilfsmittel bei dem Bücherlesen**.
XXXIX. Über das **lesende Publikum**.
XL. Beschluss

Bergk, Johann Adolf (1799): Die Kunst, Bücher zu lesen. Nebst Bemerkungen über Schriften und Schriftsteller, Jena: Hempel, XIII-XVI ; Hervorhebungen: J.T.).

„Die Kunst, Bücher zu lesen“

Beschluss

Der Leser muss ein Buch **wie ein geschickter Künstler** behandeln, der an seinen Stoffen so lange arbeitet und bildet, bis er ein herrliches Werk daraus gemacht hat. Er muss sich **kühn durch jedes Hindernis** und durch jede Schwierigkeit hindurch arbeiten, um seine Kräfte zu üben, und sich durch Aussicht auf Gewinn **Lust zur Selbsttätigkeit** in sich erwecken. Alles Lesen muss auf die Auferweckung unserer Kräfte abzielen, und wir müssen uns in den Stand setzen, jedes Buch, das Erscheinungen des menschlichen Geistes enthält, so viel, als möglich, **in uns wieder zu erneuern**, welches vorzüglich der Zustand ist, wo wir an Kultur und Kenntnissen am meisten gewinnen. Wir müssen über jeden Stoff, den wir bearbeiten, die Oberhand zu gewinnen suchen, und **wir müssen herrschen**, so viel Schwierigkeiten auch zu besiegen sind.
Die Lektüre darf **kein Betäubungsmittel unserer Kräfte, sondern ein Reiz für ihre Tätigkeit** sein. Kopf und Herz müssen durch sie mündig werden, und unsere Menschheit muss über unsere Tierheit den Sieg davon tragen. **Veredelt, selbsttätig und freier** müssen wir die Lektüre jedes Buches zu verlassen und unserer Sinnes- und unserer Denkungsart das Gepräge des **Edelmutes** und der **Originalität**, der **Humanität** und der **Freiheit** aufzudrücken streben.

Bergk, Johann Adolf (1799): Die Kunst, Bücher zu lesen. Nebst Bemerkungen über Schriften und Schriftsteller, Jena: Hempel, 415-416. (Die Schreibweise ist durchgehend normalisiert; Hervorhebungen: J.T.).