

## Veranstalter

DANTE e. V.  
Postfach 10 18 40  
69008 Heidelberg

☎: +49 (6221) 2 97 66  
Fax: +49 (6221) 16 79 06

Wilhelm-Schickard-Institut für Informatik  
Sand 13  
72076 Tübingen

**Anmeldung:**  
<http://cms.dante.de/herbst2008>  
mv39@dante.de  
oder schriftlich an DANTE e. V.

DANTE, Deutschsprachige Anwendervereinigung  $\TeX$  e.V., wurde am 14. April 1989 in Heidelberg gegründet. Der Zweck des wissenschaftlichen Vereins ist die Betreuung und Beratung von  $\TeX$ -Benutzern im gesamten deutschsprachigen Raum. Außerdem werden Entwicklungen im Bereich von  $\TeX$ ,  $\LaTeX$ , METAFONT, Bib $\TeX$ , ... national und international initiiert, gefördert und koordiniert.

## Zeitplan

Freitag 12.9. 2008:

19:00 Uhr Vorabendtreff im Casino, Wöhrdstraße 25

Sonnabend 13.9.:

8:30 Ausgabe Tagungsunterlagen  
8:45 Begrüßung  
9:00–10.15 39. Mitgliederversammlung von DANTE e. V.  
10:30–12.30 Tutorien und Vorträge  
13:00 Mittagspause  
14.30–17.00 Tutorien und Vorträge  
19:00 Abendtreff im „Ratskeller“, Haaggasse 4

5.3.5 Die Reduktion des Grundschlüssels

Die so genannten Rundenschlüssel sind wie der Grundschlüssel prinzipiell frei wählbar, müssen jedoch für einen chiffrierten Text bekannt sein, sonst kann keine Dechiffrierung erfolgen.  $K_i$ ,  $i = 1, 2, \dots, 16$  seien die einzelnen Rundenschlüssel, die aus dem 64-Bit Grundschlüssel bestimmt werden und  $v_i$ ,  $i = 1, 2, \dots, 16$  sowie PC1 und PC2 folgende Hilfsgrößen:

$$v_i = \begin{cases} 1 & \text{für } i \in \{1, 2, 9, 16\} \\ \text{andernfalls} & \end{cases} \quad (5.54)$$

$$PC1: (0, 1)^{16} \rightarrow (0, 1)^{28} \times (0, 1)^{28} = C_0 \times D_0 \quad (5.55)$$

$$C_i = v_i \times \text{shift links}(C_0) \quad (5.56)$$

$$D_i = v_i \times \text{shift links}(D_0) \quad (5.57)$$

$$PC2: C_i \times D_i = (0, 1)^{28} \times (0, 1)^{28} \rightarrow (0, 1)^{56} = K_i \quad (5.58)$$

Die Funktion PC1 ordnet einer Matrix mit 8 × 8 Elementen (64 Bit) zwei Matrizen mit jeweils 4 × 7 Elementen (28 Bit) zu, wobei die letzte Spalte (6, 16, 24, 32, ...) unberücksichtigt bleibt, die beim Schlüssel ja den Paritätsbits entspricht (vgl. Gl. 5.38). Die Funktion PC2 ordnet zwei 4 × 7 Matrizen einer 8 × 6 Matrix zu, was nach einem festen Schema erfolgt:

$$\begin{pmatrix} 63 & 62 & 61 & 60 & 59 & 58 & 57 & 56 \\ 55 & 54 & 53 & 52 & 51 & 50 & 49 & 48 \\ 47 & 46 & 45 & 44 & 43 & 42 & 41 & 40 \\ 39 & 38 & 37 & 36 & 35 & 34 & 33 & 32 \\ 31 & 30 & 29 & 28 & 27 & 26 & 25 & 24 \\ 23 & 22 & 21 & 20 & 19 & 18 & 17 & 16 \\ 15 & 14 & 13 & 12 & 11 & 10 & 9 & 8 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 7 & 15 & 23 & 31 & 39 & 47 & 55 \\ 63 & 6 & 14 & 22 & 30 & 38 & 46 \\ 54 & 62 & 5 & 13 & 21 & 29 & 37 \\ 45 & 61 & 4 & 12 & 20 & 28 \end{pmatrix}$$

Denormalisierte Matrizen sind natürlich schlecht zu merken, sodass die verkürzte Schreibweise gewählt wird:

$$PC1 \rightarrow \begin{pmatrix} C_0 \\ D_0 \end{pmatrix} = C_0 \times D_0 \quad (5.60)$$

5.3.5 Data Encryption Standard

Abbildung 5.3: Bildung des Rundenschlüssels  $K_i$

Den formalen Ablauf zur Bestimmung des Rundenschlüssels zeigt anschaulich Abb. 5.3. Das Prinzip für  $C_i$  ist relativ leicht zu erkennen:

- Beginnend mit dem 0. Platz (unten rechts) ergeben die ersten vier Elemente von  $D_0$  und  $C_0$  zusammen die vierte Spalte der 8 × 8 Matrix (60, 52, 44, 36) die ersten Elemente von  $D_i$  und 28, 20, 12, 4 die ersten von  $C_i$ .
- Nach dem zugeordneten Element Nr. 4 kommt bei  $C_i$  das 61. Element der 8 × 8 Matrix. Das nächste Element ist das um 8 Plätze kleinere Element, das dann folgende das 16 Plätze kleinere usw. Wird diese Platznummer negativ, dann wird einfach mit dem 61 + 1. Element weitergemacht, bis wieder durch die Verringerung um 8 Plätze eine negative Zahl erreicht wird und es dann mit dem 61 + 2. Platz weitergeht usw. bis die Matrix  $C_i$  gefüllt ist (Abb. 5.6).

Für  $D_i$  verläuft dies analog, wenn beachtet wird, dass nach den ersten vier Elementen mit der Platznummer 59 der 8 × 8 Matrix weitergemacht wird, bei negativer Platznummer der neue „Startwert“ 59 – 1 ist, der nächste bei ständiger Verringerung um 8 Plätze 59 – 2 usw.

Schriftbild und spezielle Zeichen

- Punkte und Satzzeichen: normale Eingabe ...
- Fortsetzung: oder Auslassungspunkte über die linke Seite ...
- Leerzeichen nach Zeichenblöcken: ...

Quellen

- Was ist gemeint?
- Konventionen
- Variablen
- Nachweise
- Was ist CVT?
- Bibliografie
- Literatur
- Externe Writing
- Druckarbeiten an einem Dokument

Linguistik

99 A 198

Die über die ganze Welt, je nach den auftretenden Anreißungen, sich aus-  
 lers ausgewählte Abh.,<sup>115</sup> Jena 1921<sup>4</sup>. Below rühmt ihn etwas zurückhaltender, deutet aber an, daß Marx wichtigste Erkenntnisse ihm verdanke.<sup>116</sup> Neupublikationen sind unterwegs.<sup>117</sup> Scheler erinnert vielfach an ihn.<sup>118</sup> Dagegen hat ihn leidenschaftlich und eindrucksvoll Schmitt-Doroni „a. a. O.“ bekämpft.<sup>119</sup> In Wahrheit sind seine Schriften sehr verschiedenartig (Lehre vom Gegensatz 1804; Vorl. über deutsche Lit. 1807; Elemente der Staatskunst 1809; Vermischte Schriften<sup>120</sup> 1817). Die Elemente ins-  
 a-a : A: eine Abhängigkeit Marsens von ihm und ähnlichen Schriftstellern an.  
 b-b : A: Schelers Mischung von Rittertum, Literatur und Katholizismus hat bei ihm ihre volle Analogie.  
 c-c : A: Schmitt-Doroni... Die politische Romantik.  
 d-d : A: (Lehre vom Gegensatz 1804; Vorlesungen über deutsche Literatur 1807; Elemente der Staatskunst 1809; Vermischte Schriften<sup>121</sup> 1817) sehr verschiedenartig die „Elemente“

115 Vgl. Othmar Spann: Vorwort zu Die Herdflamme. Sammlung der gesellschaftswissenschaftlichen Grundwerke aller Völker und Zeiten. I. Band. Adam H. Müller. Die Elemente der Staatskunst (1922).

116 Vgl. Georg von Below: Die deutsche Geschichtsschreibung von den Befreiungskriegen bis zu unseren Tagen (1916), S. 172–175.

117 Vgl. u. a.: Johannes Höfer: Adam Müller und Metternich (1922); Benno Innendorfer: Adam Müller und die Staatslehre (1922); Friedrich Lenx: Über Adam Müllers Staats- und Gesellschaftslehre (1922); Gustav Seidler-Schmid: Adam Müller. Von der Bedeutung seiner Lehren für unsere Zeit (1922); Otto Weinberger: Adam Müller (1922).

118 Vgl. z. B. Max Scheler: Vom Ewigen im Menschen (1920), S. 161.

119 Vgl. Carl Schmitt-Doroni: Politische Romantik (1919), z. B. S. 112 f.; „Das Normale im Juristischen wie im moralischen Sinne ist ihm inkommensurabel. Einem normativen Begriff gegenüber versagt die Gegenständlichkeit; die normale Sexualität ist nicht der Indifferenzpunkt von Sadismus und Masochismus, der Mut eines tapfern Mannes nicht die höhere Einheit von Depression und Exaltation, der vernünftig geordnete Staat nicht eine Synthese aus Anarchie und Despotie. Adam Müllers amoralisches Verständnis für alles und sein Gegenteil, seine Sucht, überall zu vernichten, seine „weltumfassende Toleranz“, vor der Grenz erschrocken, weil dann nichts mehr übrig blieb, was man lieben und rechtfertigen lassen konnte, seine unmännliche Passivität, zu der er Burkes, de Maistres und Bonalds Abneigung gegen das künstliche „Machen“ umzubiegen verstand, sein gefühlmäßig im Grunde immer mit allem einverstanden, alles gutheilender Pantheismus, sind wohl auch individualpsychologisch aus seiner weiblichen, pflanzenhaften Natur zu erklären, für den romantischen Ästhetizismus waren sie aber die geeignete psychische und physische Disposition, weil sie das Subjekt ganz an seinen Affekt und die mit der Verarbeitung des Affekts sich begnügende ästhetische Produktivität wies.“

柳宗元 《漁翁》

漁翁夜傍西巖宿，  
曉汲清湘燃楚燭。  
煙銷日出不見人，  
欸乃一聲山水綠。  
迴看天際下中流，  
巖上無心雲相逐。

柳宗元 《漁翁》

漁翁夜傍西岩宿，  
曉汲清湘燃楚燭。  
煙銷日出不見人，  
欸乃一聲山水綠。  
迴看天際下中流，  
巖上無心雲相逐。

A poem by Liú Zōng Yuán (柳宗元, 773–819), displayed on the left with traditional characters and on the right using “simplified” characters. The  $\TeX$  CJK package interfaces nicely with Emacs/Mule, so that different character sets (Big5 for traditional characters, GB2312 for “simplified” characters) can be mixed within the same file. This is especially useful in this case, since the character 欸 is not part of the GB2312 character set, so I substituted the correct Big5 character on the right hand side. The input file was exported using the Emacs function c-jk-wr:t-e-€:1:e supplied by the CJK package and the resulting file was processed with pdf $\TeX$ .

Computer Modern – AvantGarde – Helvetica – Times – Palatino – NewCenturySchoolbook – Bookman – ZapfChancery – CharterBT – Concrete – CM Bright – Luximono – PX Roman – Utopia – CM Typewriter – Courier

**L<sup>A</sup>T<sub>E</sub>X** Sophisticated professional typesetting for business and academic publishing

Where to get  $\TeX$

- The  $\TeX$  Users Group (TUG) distributes a free copy of the  $\TeX$  Live CD-ROM and a free copy of the entire CTAN archive on CD-ROM to all members annually. Many local and national user groups also do something similar; check with your nearest group (see TUG Web site for address).
- All the public-domain and open-source implementations are available for free download from CTAN.
- You can buy a copy with commercial support from any of the vendors listed below.

TUG membership for 2008 is \$65 a year for individuals, \$15 for students and OAPs, and \$25 for non-member subscriptions to publications only. See <http://www.tug.org> for details of discounts and other charges. Institutional rates for 2008 are \$500, which includes up to seven individual member subscriptions. Membership includes the quarterly journal  $\TeX$ news, and discounts of conference and training courses.

CTAN: The Comprehensive  $\TeX$  Archive Network is an online Internet archive of all  $\TeX$  and  $\TeX$ Live software. There is a searchable index and catalogue at <http://www.ctan.org>, <http://www.ctan.ac.uk>, and <http://www.ctan.org>. There is also a two-monthly email newsletter, the  $\TeX$ Live  $\mathcal{Z}$ ine, and some extensive FAQs listed at <http://www.tug.org>.

Online and other support: Internet-based support uses the comp.text.tex Usenet newsgroup (available in German as de.comp.text.tex). There is also a two-monthly email newsletter, the  $\TeX$ Live  $\mathcal{Z}$ ine, and some extensive FAQs listed at <http://www.tug.org>.

Vendors: See <http://www.tug.org> for details of vendors and their products.

Technical Requirements:  $\TeX$  runs on all current computing platforms. The most common implementations are: Microsoft Windows, MS-DOS, Amiga, Linux & other Unix, Apple Macintosh. Implementation: Free:  $\TeX$ ,  $\LaTeX$ ,  $\text{Meta}\TeX$ ,  $\text{Ly}\omega$ . Commercial: see adjacent list. Free:  $\text{am}\TeX$ ,  $\text{dv}\TeX$ . Commercial:  $\text{Amiga}\TeX$ . Free:  $\text{tu}\TeX$ ,  $\text{ly}\omega$ . Commercial:  $\text{O}\mathcal{Z}\mathcal{T}\mathcal{E}\mathcal{X}$ . Free:  $\text{t}\mathcal{E}\mathcal{X}$ ,  $\text{ly}\omega$ . Commercial:  $\text{TeX}\text{Live}$ . Contact the  $\TeX$  Users Group for details (see adjacent).

Hardware:  $\TeX$  will run even on quite old machines, but a 66MHz processor or above is recommended. You should have at least 220Mb of memory; more if you aim to do complex work or very long documents. You need approximately 300Mb of hard disk space depending on the implementation and the options you choose (a minimal installation takes about 75Mb; maximum is about 500Mb). A printer is needed if you want paper output, but  $\TeX$  will generate PostScript™ and PDF™ files for sending to other people or to photo-imaging or laser typesetting equipment.

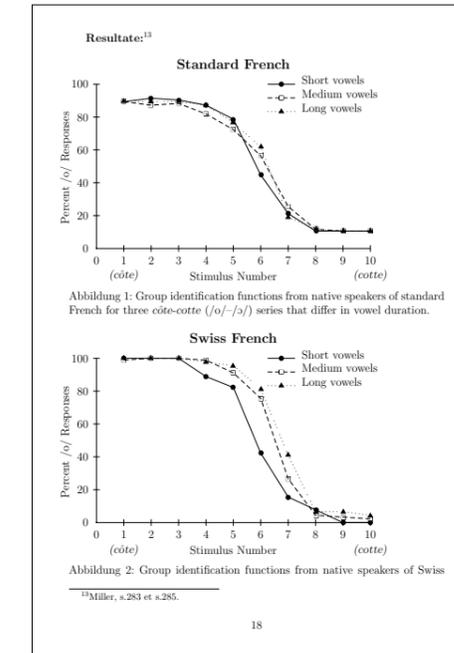
Software: You need an editor for maintaining your documents; there is a selection included on the  $\TeX$  Live CD-ROM. A copy of Ghostscript/Ghostview or similar is needed to view PostScript or PDF output (included on the  $\TeX$  Live CD-ROM). A graphics editor or manipulation program is needed if you want to create or modify images.

The ultimate in portable typesetting:  $\TeX$  runs on any computer and produces timely, accurate, publication-quality output on desktop printers and commercial typesetters. It's completely free, and has been the tried and tested solution for over 20 years.  $\TeX$  is in use by leading publishers, documentation specialists, and technical and academic users worldwide.

What they say about  $\TeX$ : I was getting increasingly exasperated with the limitations presented by wordprocessing programs when  $\TeX$  came into my life and allowed me to do all those things I previously could only dream of, from unusual symbols to complicated layout. I strongly recommend it to anybody interested in producing a professional-looking document. Peter Hobbins, *Robertson & Ryan*. I use  $\TeX$  and  $\text{Meta}\mathcal{Z}$  not only because I need them to create my presentations, lecture notes and papers but also because it's fun! Entering a math equation in  $\text{Flow}\mathcal{Z}$  is a pain in the neck, with  $\text{port}\mathcal{Z}$  and  $\text{M}\mathcal{Z}$  it is a lot easier because you can change the style of what is to be displayed. I have a lecture class from which I generate a lecture presentation and lecture notes all from the same source. I can add text which appears in one or both of the documents. Marc van Dongen, *Computer Science*.

$\TeX$  is available in UCC from the Electronic Publishing Unit, Computer Centre, 4th Floor, Kings Building (email: e1@ucc.ac.uk).

Let this leaflet convince you, then get in touch with your nearest supplier or the contact for your local User Group (see address in panel). They will be happy to discuss your requirements. You're also very welcome to come to any of the User Group events and meet other users.



F. Gegenüberstellung ausgewählter Berufsbezeichnungen

Deutsche Berufsbezeichnung	Belgisch	Österreichisch	Frankreich	Italienisch	Japanisch	Polnisch	Russisch	Schwedisch	Schweizer
magistrat	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (f. fem.)	magistrat	magistrat	magistrat	magistrato	magistrato	magistrat	magistrant	magistrant	magistrat
magistrat (m. m.)	magistrat	magistrat	magistrat	magistrato					