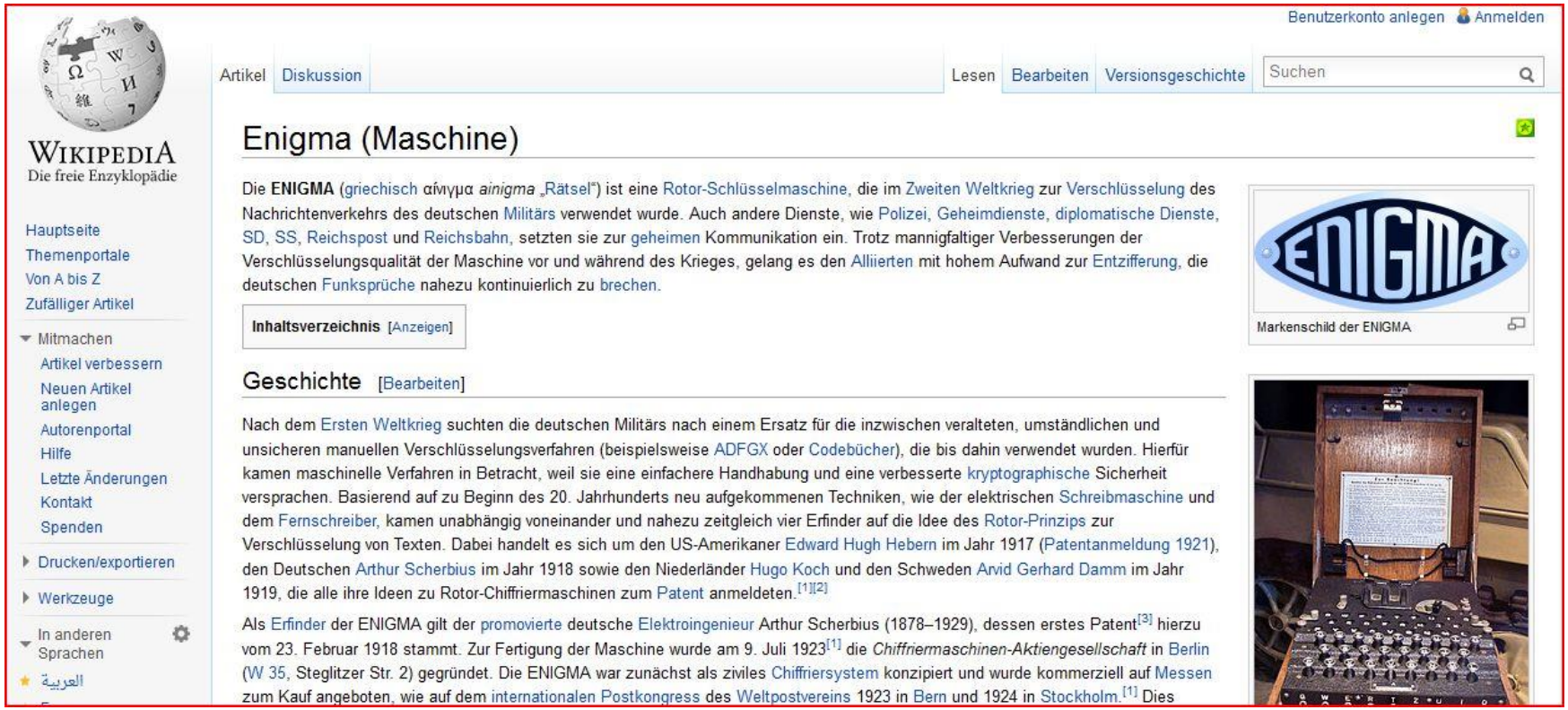
Enigma

Lehrmeister Wikipedia



Benutzerkonto anlegen Anmelden

Artikel Diskussion Lesen Bearbeiten Versionsgeschichte Suchen

WIKIPEDIA
Die freie Enzyklopädie

Hauptseite
Themenportale
Von A bis Z
Zufälliger Artikel

Mitmachen
Artikel verbessern
Neuen Artikel anlegen
Autorenportal
Hilfe
Letzte Änderungen
Kontakt
Spenden

Drucken/exportieren

Werkzeuge

In anderen Sprachen
العربية

Enigma (Maschine)

Die **ENIGMA** (griechisch αἴνιγμα *ainigma* „Rätsel") ist eine Rotor-Schlüsselmaschine, die im Zweiten Weltkrieg zur Verschlüsselung des Nachrichtenverkehrs des deutschen Militärs verwendet wurde. Auch andere Dienste, wie Polizei, Geheimdienste, diplomatische Dienste, SD, SS, Reichspost und Reichsbahn, setzten sie zur geheimen Kommunikation ein. Trotz mannigfaltiger Verbesserungen der Verschlüsselungsqualität der Maschine vor und während des Krieges, gelang es den Alliierten mit hohem Aufwand zur Entzifferung, die deutschen Funksprüche nahezu kontinuierlich zu brechen.

Markenschild der ENIGMA

Inhaltsverzeichnis [Anzeigen]

Geschichte [Bearbeiten]

Nach dem Ersten Weltkrieg suchten die deutschen Militärs nach einem Ersatz für die inzwischen veralteten, umständlichen und unsicheren manuellen Verschlüsselungsverfahren (beispielsweise ADFGX oder Codebücher), die bis dahin verwendet wurden. Hierfür kamen maschinelle Verfahren in Betracht, weil sie eine einfachere Handhabung und eine verbesserte kryptographische Sicherheit versprachen. Basierend auf zu Beginn des 20. Jahrhunderts neu aufgekommenen Techniken, wie der elektrischen Schreibmaschine und dem Fernschreiber, kamen unabhängig voneinander und nahezu zeitgleich vier Erfinder auf die Idee des Rotor-Prinzips zur Verschlüsselung von Texten. Dabei handelt es sich um den US-Amerikaner Edward Hugh Hebern im Jahr 1917 (Patentanmeldung 1921), den Deutschen Arthur Scherbius im Jahr 1918 sowie den Niederländer Hugo Koch und den Schweden Arvid Gerhard Damm im Jahr 1919, die alle ihre Ideen zu Rotor-Chiffriermaschinen zum Patent anmeldeten.[1][2]

Als Erfinder der ENIGMA gilt der promovierte deutsche Elektroingenieur Arthur Scherbius (1878–1929), dessen erstes Patent[3] hierzu vom 23. Februar 1918 stammt. Zur Fertigung der Maschine wurde am 9. Juli 1923[1] die *Chiffriermaschinen-Aktiengesellschaft* in Berlin (W 35, Steglitzer Str. 2) gegründet. Die ENIGMA war zunächst als ziviles Chiffriersystem konzipiert und wurde kommerziell auf Messen zum Kauf angeboten, wie auf dem internationalen Postkongress des Weltpostvereins 1923 in Bern und 1924 in Stockholm.[1] Dies

Enigma einfach

Enigma einfach (Varianten)

Es gibt 26! oder 403.291.461.126.605.635.584.000.000 verschiedene Kombinationsmöglichkeiten für eine Codierscheibe.
Sender und Empfänger müssen sich also über das verwendete „Modell“ einig sein.

Enigma einfach (Pocket Decoder)

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	s	l	z	u	w	n	x	d	i	c	q	h	e	j	f	t	k	o	y	r	b	m	p	v	g

oder:

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
s	l	z	u	w	n	x	d	i	c	q	h	e	j	f	t	k	o	y	r	b	m	p	v	g	a

oder 24 weitere Möglichkeiten, wie die Ringe zueinander stehen können.
Sender und Empfänger müssen sich also über die Einstellung der Scheiben einig sein.

Enigma einfach

Um ein Rätsel, dass mit dem Pocket Decoder *verschlüsselt* wurde zu entschlüsseln, muss ich im Listing

1) Einen Hinweis finden, dass der „Pocket-Decoder“ als Codierscheibe benutzt wurde

und

2) Den Hinweis auf die Stellung der Scheiben finden.

Enigma

Um einen Enigma-verschlüsselten Text zu entschlüsseln, brauchen wir zunächst eine Enigma. Hier hilft uns Wikipedia wieder einmal weiter…

Weblinks [Bearbeiten]

Exponate

- Orte, an denen authentische Enigma-Maschinen zur Schau gestellt werden, englisch

Simulationen der Maschine

- Windows, ENIGMA I, M3 und M4 realitätsnah visualisiert, englisch
- Windows, weitere Varianten wie ENIGMA G und ENIGMA T sowie NEMA und SIGABA, englisch
- MAC OS, englisch
- RISC OS, englisch

Simulationen der Verschlüsselung

- Papier-Enigma (PDF; 84 kB), Papier-Version der Enigma-Verschlüsselung
- Javascript, browserübergreifend

Enigma

Vereinfacht gesagt ist das „Monstrum“ ENIGMA nichts weiter, als eine Schreibmaschine, bei der das „Signal“ der gedrückten Taste durch 4 verschiedene Pocket-Decoder wandert, ehe eine Ausgabe erfolgt.

Wir suchen im Listing also nur den Schlüssel, wie wir die Enigma einstellen müssen.
Nur bei der Enigma ist er etwas „komplizierter“ als „A=S“ beim Pocket-Decoder.

Enigma M3 - Schlüssel

Ein Enigma-Schlüssel besteht in der Regel aus diesen 5 Elementen:

- Umkehrwalze
- Walzenlage
- Ringstellung
- Steckbrett
- Grundstellung

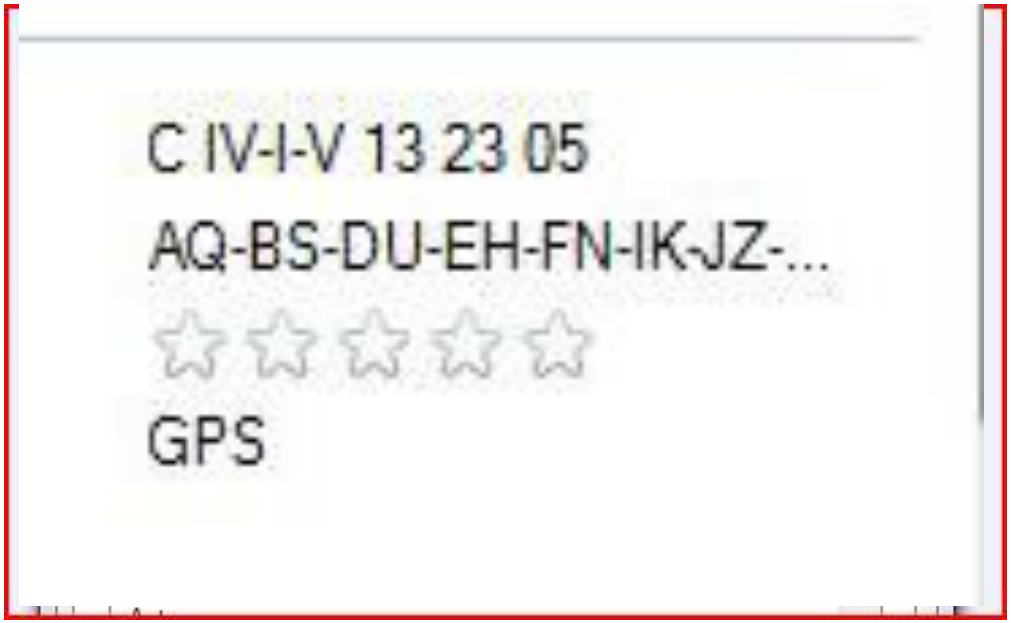
Diese Einstellungen wollen wir anhand eines Beispiels mit der Javascript basierten „Universalenigma“ anschauen.

Beispiel

Das Listing enthält diese JPG-Datei:

yvucg
vqorf
qmbxe
thtfu
vhpce

In den Dateieigenschaften finden wir dies:



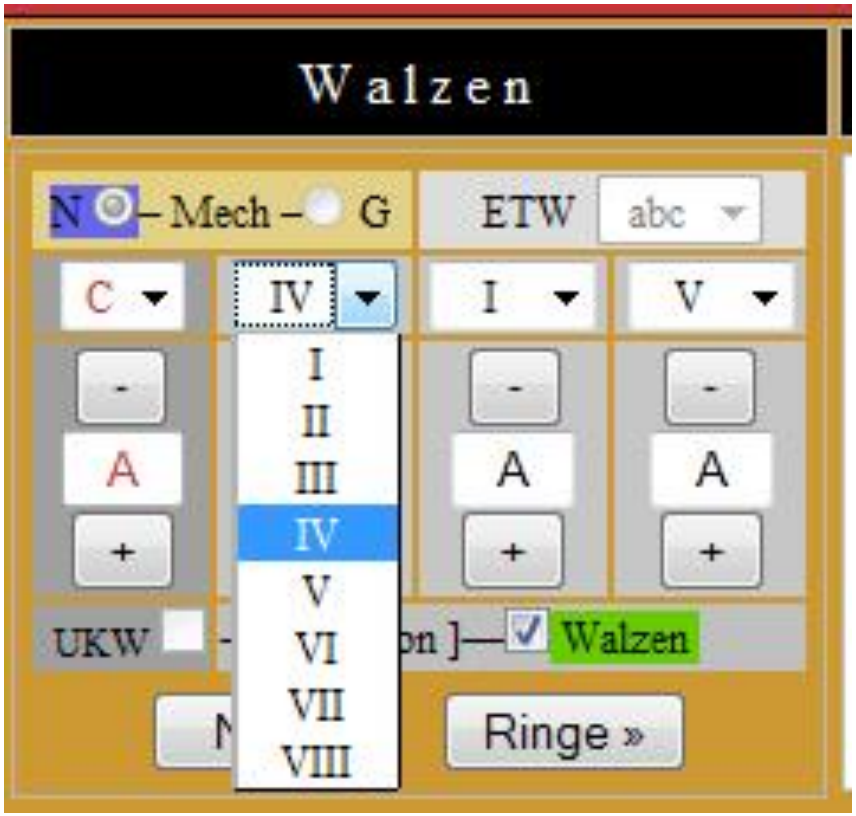
Das sieht seltsam aus, das schauen wir uns genauer an.

Enigma M3 - Schlüssel

- Umkehrwalze (UKW) – eine der vier „Pocket-Decoder“
  Die Simulatoren bieten im Normalfall die gebräuchlichen Umkehrwalzen B und C an.

Enigma M3 - Schlüssel

- Walzenlage – die drei weiteren „Pocket-Decoder.“
  Die Enigma M3 verfügt über 8 verschiedene dieser Walzen, von denen jeweils 3 zum Einsatz kommen. Üblicherweise wird die Walzenlage anhand von römischen Zahlen dargestellt.



Enigma M3 - Schlüssel

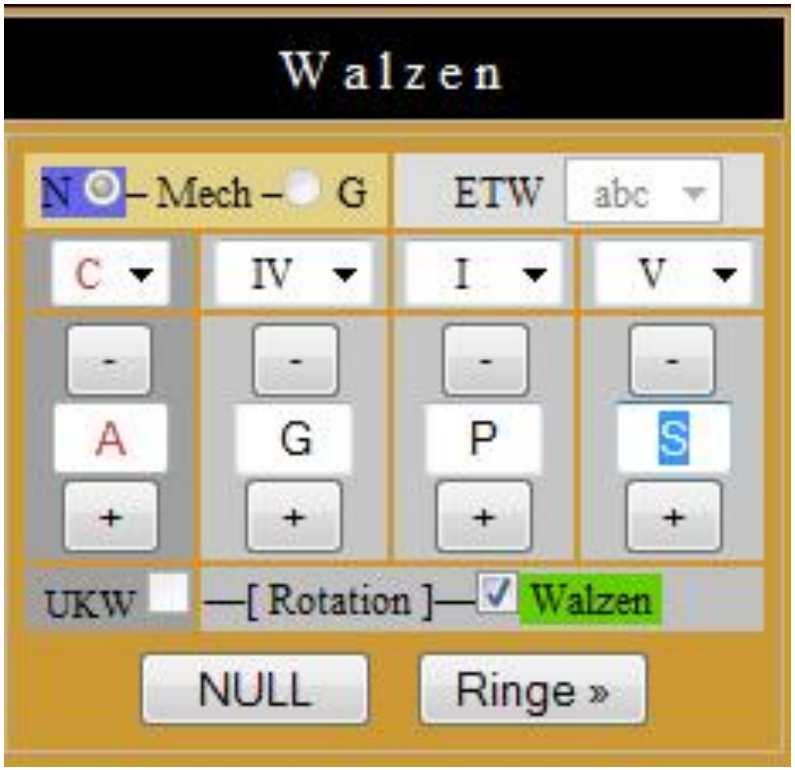
- Ringstellung – die Einstellung des jeweiligen Pocket-Decoders Die Umkehrwalze steht „fest“. Daher besteht dieser Teil des Schlüssels in der Regel aus drei Zahlen im Bereich von 1-26, kann aber ggf. auch mit A-Z angegeben sein. Hier besteht dann jedoch Verwechslungsgefahr zur „Grundstellung“ (s.u.)

Enigma M3 - Schlüssel

- Steckbrett – auf dem Steckbrett werden bis zu 10 Buchstabenpaare noch einmal extra miteinander vertauscht. So wird zum Beispiel aus jedem getippten A im innern der Maschine ein Q und aus jedem Q ein A. Normalerweise werden die Steckbrettverbindungen als Buchstabenpaare angegeben.

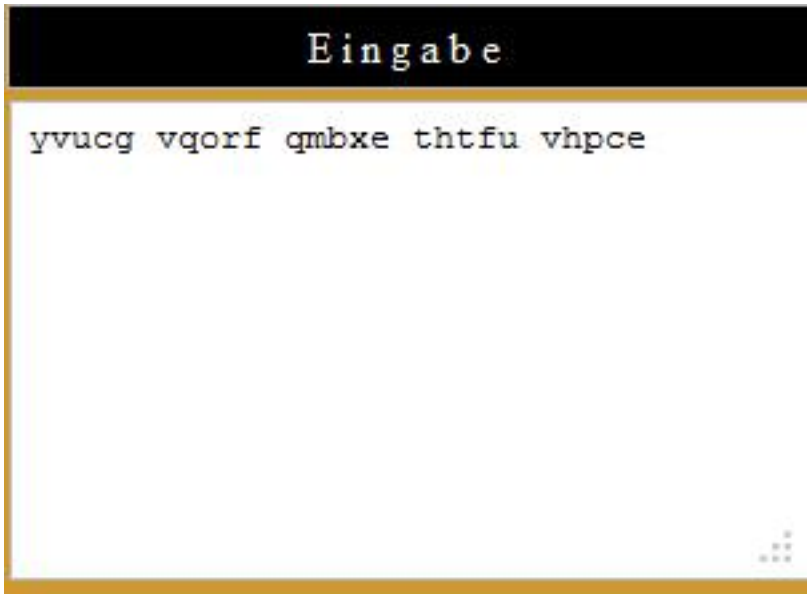
Enigma M3 - Schlüssel

- Grundstellung – da sich die Walzen der Walzenlage mit jedem Tastendruck weiter bewegen, ist eine Grundstellung anzugeben. Normalerweise werden hier drei Buchstaben angegeben.

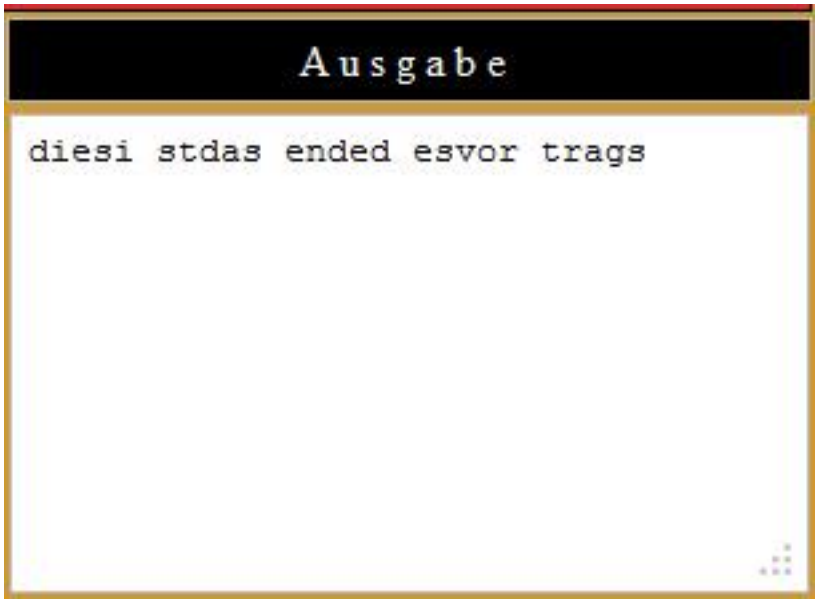


Enigma M3 - Schlüssel

So wird aus:



schließlich:



Und wenn wir dann noch „sinnvolle“ Worte Bilden:

Dies ist das Ende des Vortrags.