# ENIGMA – das (zu lösende) Rätsel

Die ENIGMA-Maschine ist das wohl faszinierendste kryptografische Gerät. Das liegt daran, dass sie durch die über 150 Billionen Einstellungsmöglichkeiten das sicherste Gerät ihrer Zeit gewesen sein müsste, die Verschlüsselung jedoch bereits vor Ausbruch des zweiten Weltkriegs durch polnische und später dann durch britische Kryptologen fast durchgehend gebrochen wurde. Die britischen Militärs hielten die entzifferten Nachrichten teilweise schneller in den Händen als die deutschen Generäle (1943: ca. 2500 Funksprüche pro Tag). Das lag u. a. daran, dass Alan Turing basierend auf den Ideen des Polen Marian Rejewski Maschinen (sog. Bomben) bauten, um die Nachrichten automatisch zu entschlüsseln. Nicht nur damit setzte Turing sein theoretisches Modell der Turing-Maschine praktisch als Vorläufer eines moderner Computer um, es gipfelte in der Entwicklung des Röhrenrechners COLOSSUS, der für die Entschlüsselung der Nachrichten von Lorenz-Maschinen eingesetzt wurde. Der Lorenz-Maschinen-Code war deutlich komplizierter, mit ihm waren die direkten Befehle Hitlers chiffriert.

## Aufbau und Test der (Papier-) ENIGMA

Unsere ENIGMA ist der voll kompatible Nachbau für die Kriegs-Modelle I, M1, M2 und M3. Das Modell M3 war bis Kriegsende im Einsatz mit Ausnahme der U-Boot-Flotte, die ab Februar 1942 auf die M4 wechselten. Die (Papier-) ENIGMA besteht aus einer von zwei Umkehrwalzen (UKW) und drei aus fünf Walzen. Außerdem sind Ringstellung (Verschiebung innerhalb einer Walze), Steckbrett (Austausch zweier Buchstaben) und Grundstellung zu wählen. Die Umkehrwalze sorgt dafür, dass man mit einer ENIGMA sowohl ver- als auch entschlüsseln kann.

**Für die Papier-ENIGMA müssen stets die grauen Balken auf UKW und Ein-/Ausgabe auf gleicher Höhe sein.**

**Test I ohne Ringstellung und Steckerbrett:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Nr.** | UKW | Walzenlage | Grundstellung |
| 1 | B | I–II–III | A B C |

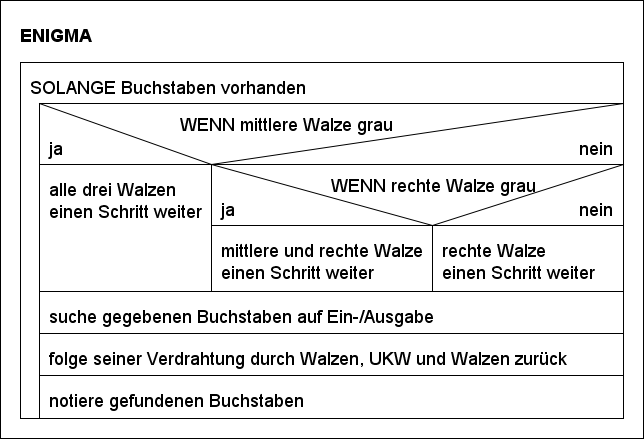
Vorläufiger Algorithmus zur Ver- und Entschlüsselung:

*SOLANGE Buchstaben vorhanden*

1. *Drehe rechte Walze einen Buchstaben weiter (Drehung zum Körper)*
2. *Suche zu gegebenen Buchstabe auf Ein-/Ausgabe*
3. *Folge seiner Verdrahtung durch drei Walzen, UKW und Walzen zurück*
4. *Notiere gefunden Buchstaben*

Übung: Dechiffriere folgende Nachricht: OXBAR SX

Liegt eine längere Nachricht vor, muss die Weiterschaltung der Walzen nach einer vollen Umdrehung berücksichtigt werden, so wie es etwa auch ein Kilometerzähler macht. Leider ist das Verfahren in der ENIGMA nicht ganz so einfach. Das Struktogramm beschreibt es anschaulich. Die Schattierung der Buchstaben auf der linken Walze spielt übrigens keine Rolle.



**Test II ohne Ringstellung und Steckerbrett:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | UKW | Walzenlage | Grundstellung | Geheimtext |
| 2 | B | I–II–III | A B R | UHTZC ZCBVG |
| 3 | B | I–II-III | A D S | PDALD BRZPX |

Die ENIGMA konnte die Buchstabenfolge auf der Walze relativ zur inneren Verdrahtung verschieben. Man bezeichnete dies als Ringstellung und gab es durch Zahlen (01 ⬄ A, 02 ⬄ B, …) an.

Darüber hinaus wurden auf dem Steckerbrett der ENIGMA genau zehn Kabelbrücken gesetzt. Damit tauschten die durch Kabel verbundenen Buchstaben bei der Ein- und Ausgabe ihre Plätze. Die Kabelbrücke AP bedeuteten also, dass nach Eingabe des Buchstaben A dieser in P umgewandelt wurde und P entsprechend in A.

Die Papier-ENIGMA verfügt über Ringe, die einfach den vorhandenen Walzenaufdruck überdecken und entsprechend gedreht werden können. Dazu wird erst der Ring verdreht und dann die Grundstellung eingestellt. Das Steckerbrett wird auf der Ein-/Ausgabe durch manuelles Eintragen der Vertauschungen in die freien Kästchen simuliert.

**Test III mit Ringstellung und Steckerbrett:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | UKW | Walzenlage | Ringstellung | Steckerverbindungen | Grundstellung | Geheimtext |
| 4 | B | I–II–III | 10 14 21 |  | X Y Z | JMINU BZRTW |
| 5 | B | I–II-III | 10 14 21 | AP BR CM FZ GJ IL NT OV QS WX | V Q Q | YMLTO VZUDB IRBPX YTNQ |

## Echte Funksprüche mit der ENIGMA chiffrieren/dechiffrieren (Niveau 1)

Wir sind nun in der Lage unsere ENIGMA vollständig zu bedienen. Jedoch wird es uns nicht gelingen, originale M3-verschlüsselte Nachrichten zu lesen, da jede Nachricht nach festem Muster codiert werden musste. Zum einen gibt es Regeln zum Schreiben von Zahlen, Namen und Satzzeichen, zum anderen ist die Walzengrundstellung nicht tages-, sondern funkspruchabhängig.

**Beispiel:** Der folgende Klartext soll verschlüsselt werden: KEINX WASSE RXDA

**Schlüsseltafel für den aktuellen Tag**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| UKW | Walzenlage | Ringstellung | Steckerverbindungen | Kenngruppen |
| B | I–II–III | 10 14 21 | AP BR CM FZ GJ IL NT OV QS WX | AGP ISO DIN HTM |

Der Schlüssler denkt sich eine **beliebige Grundstellung** aus: z. B. LMA und stellt diese ein. Dann chiffriert er den **frei gewählten Spruchschlüssel**, z. B. TAW. Die ENIGMA gibt JIK zurück. Nun setzt er die ENIGMA auf TAW zurück und chiffriert den Klartext.

Der **Spruchkopf**, bestehend aus Uhrzeit, Anzahl der Zeichen, Grundstellung LMA und chiffrierten Spruchschlüssels JIK wird direkt übertragen. Anschließend folgt der Geheimtext, der jedoch um einen ersten Fünferblock erweitert wird, der eine Permutation der dreistelligen Kenngruppe vorn ergänzt um zwei beliebige Buchstaben beschreibt. Im Beispiel wurde die Kenngruppe ISO permutiert zu SOI und ergänzt vorn um DF.

Spruchkopf: 1230 – 19 – LMA JIK

Nachricht: DFSOI CSGBN QJRXN MTEU

Der Schlüssler am anderen Ende muss nun seine ENIGMA mit den gleichen Tageseinstellungen starten, dann die Grundeinstellung LMA vornehmen, JIK tippen und das Ergebnis als neue Grundstellung verwenden. Dann kann der Nachrichtentext ab dem zweiten Fünferblock dechiffriert werden.

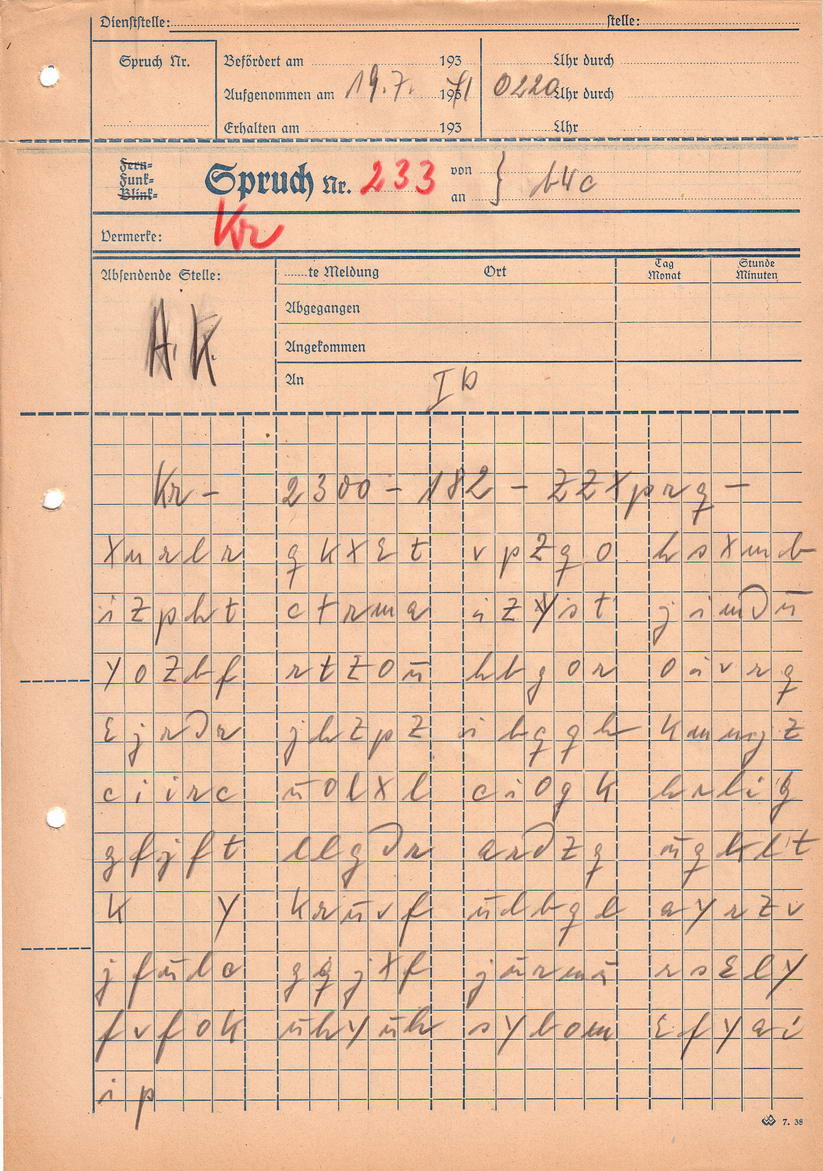
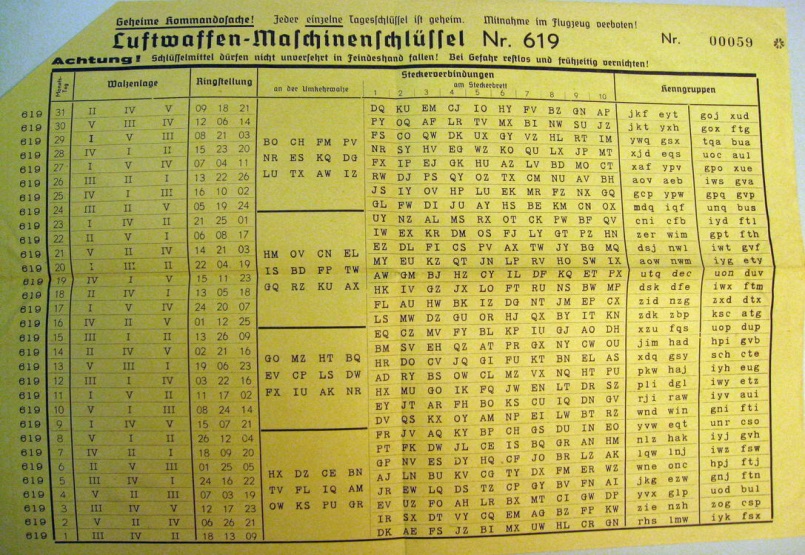
**Test IV: Versuche Dich nun selbst an folgendem Beispiel:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| UKW | Walzenlage | Ringstellung | Steckerverbindungen | Kenngruppen |
| B | II–I–IV | 02 23 14 | AD BP CH FY GJ IK NT OW QL UX | COM EDU ORG BIZ |

Spruchkopf: 1330 – 30 – DAS OSH

Nachricht: KJDUE OOPAM YVZDO HPJOE UCRQH AXSON

## Echte Funksprüche mit der ENIGMA chiffrieren/dechiffrieren (Niveau 2)

Wir sind nun in der Lage unsere ENIGMA vollständig zu bedienen. Es wird uns aber nicht gelingen, Originale M3-Nachrichten zu lesen, da es Regeln zum Schreiben von Zahlen, Namen und Satzzeichen gab und die Walzen­grundstellung vom Codierer festgelegt wurde.

1. Informiere Dich in der geheimen Heeresdienstvorschrift 14 „Schlüsselanleitung zur Schlüsselmaschine Enigma“, Kapitel „IX. Beispiel“ über das Ver- und Entschlüsseln.

Original-ENIGMA-Nachricht: <http://cryptocellar.web.cern.ch/cryptocellar/bgac/19071941_233.pdf>

Luftwaffe-Maschinenschlüssel: <http://cryptocellar.web.cern.ch/cryptocellar/Enigma/Luftwaffen-MSchluessel-Nr619.pdf>

1. Entschlüssle nach dem beschriebenen Verfahren die folgende Nachricht.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **UKW** | Walzenlage | Ringstellung | Steckerverbindungen | Kenngruppen |
| B | II–I–IV | 02 23 14 | AD BP CH FY GJ IK NT OW QL UX | COM EDU ORG BIZ |

Spruchkopf: 1330 – 28 – DAS OSH

Nachricht: KJDUE OOPAM YVZDO HPJOE UCRQH AXSON

1. Verschlüssle den vorbereiteten Klartext KEINX WASSE RXDA, übermittle ihn mit dem Spruchkopf an deinen Nachbarn und lass ihn entschlüsseln. Nutze die folgende Tageseinstellung.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **UKW** | Walzenlage | Ringstellung | Steckerverbindungen | Kenngruppen |
| B | I–II–III | 10 14 21 | AP BR CM FZ GJ IL NT OV QS WX | AGP ISO DIN HTM |

1. Hier ein echtes Beispiel vom 07. Juli 1941, Funkspruch Nr. 18, das entschlüsselt werden soll.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **UKW** | Walzenlage | Ringstellung | Steckerverbindungen | Kenngruppen |
| B | II–IV–V | B U L | AV BS CG DL FU HZ IN KM OW RX | VIS HTZ UZH NJY |

Spruchkopf: 1715 – 195 – BUO IHO

Nachricht:

ENSIV TINIF MFUNK DSPXR KBKQA DAJZN JZUQW CPHTK GQQPB XXBDM NQWKJ BYMOG MYOPT RHCNV ASAAG EZDRC KGVUJ MKLIW CVVPP TSCIL DPLRV PNCAU IMMUD RYMGJ YWNVA DCUCT QGTEJ HGABO SEXCS RDXGO YKWKI WDIDT ZTEPX FGMRD YMDQJ KBOEJ AZLJU PAWMN WYQDG

## Einbruch in die ENIGMA-Verschlüsselung

Dass die ENIGMA-verschlüsselten Nachrichten durch die Briten gelesen werden konnten, gilt als eines der bestbehütetsten Geheimnisse bis in die 70er Jahre des letzten Jahrhunderts. Man geht heute davon aus, dass der Krieg durch das Mitlesen der Nachrichten um zwei Jahre verkürzt wurde! Die Geschichte der Entzauberung liest sich wie ein Spionageroman und wird den vorhandenen Verfilmungen bei weiten nicht gerecht.

Der Weg zur Entschlüsselung kann hier nicht dargestellt, aber ein Beispiel für einen Ansatz gezeigt werden. Zur Vereinfachung wird auf Steckerbrett und Ringstellung verzichtet.

**Experiment 1:** Verschlüssele mit einer freien Einstellung den Buchstaben A mehr als 26-mal. Was stellst Du fest? Warum ist das so?

Die Umkehrwalze hat den Vorteil, dass mit einer Maschine sowohl ver- als auch entschlüsselt werden kann. Leider schränkt die Walze aber auch die Anzahl der Schlüssel erheblich ein. Ein Zeichen wird niemals in sich selbst überführt, da ja sonst der Strom nicht fließen kann.

Bei gleichen Einstellungen chiffrieren und dechiffrieren bedeutet aber, dass ein Buchstabe beim ersten Durchlaufen durch die Kabel in einen anderen umgewandelt wird und dieser beim Durchlaufen durch dieselbe Konfiguration wieder in den Ausgangsbuchstaben. Ein zweimaliges Durchlaufen ergibt also den Ausgangsbuchstaben wieder.

**Experiment 2:** Nehmen wir an, wir hätten ein Alphabet von nur vier Buchstaben. Dann gibt es 4! = 4·3·2·1 = 24 Möglichkeiten der Anordnung. Ergänze in der zweiten und vierten Zeile der Tabelle alle Permutationen von ABCD:

|  |
| --- |
| **ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD** |
| **ABCD ABDC** |
| **ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD** |
|  |

Streiche alle Alphabete, die einen ihrer Buchstaben in sich selbst überführen. Streiche alle Alphabete, bei denen der Ausgangbuchstabe bei zweimaligem Durchlaufen nicht wieder in sich selbst überführt wird. Wie viele Alphabete bleiben übrig.

Für ein Alphabet mit 26 Buchstaben verringert sich so die Anzahl der verwendbaren Permutationen von 26! ≈ 4·1026 auf nur noch rund 8·1012.

**Experiment 3** (Idee von Mavis Lever, Bletchley Park, 1941): Wir kennen (irgendwoher) die Tageseinstellungen und die Walzeneinstellung, aber nicht die Verdrahtung der neuen Umkehrwalze. Wir haben aber folgende Nachricht abgefangen:

----- KJGHW DZAAT OQPDH AWEYS YHDDC CQNNN EUIMA IIMEP HDIBA HQAZR WTKHT JZGDT CTTFS UAREV MHXZG AFXIW NVXPI DOBNR EHRCG DGAIM PHHOV UQWCO JZRZJ SIZDN VWORH MMUMF JDUCV ZRUZC DXFSV ZZFWG NMXZZ WCFUC PAMIW NUXFS SEZTD XUMVN GZUZC AFYBQ SFVWH BYXYX VJTSW DVCAE FTOEM QWFIB NFNHF RJMMQ KDJCN OPINS DFBWI YGGAZ

Was fällt auf?

In der Nachricht fehlt der Buchstabe L. Dies ist bei längeren Nachrichten ungewöhnlich. Miss Lever vermutet, dass der Funker ausschließlich die Taste L gedrückt hat, vielleicht um die feindliche Gegenseite zu täuschen. Miss Lever lag mit ihrer Vermutung richtig und konnte auf die innere Verdrahtung der italienischen ENIGMA-Maschine schließen.

**Fortsetzung Experiment 3:** Rekonstruieren Sie die Verdrahtung der Umkehrwalze, wenn folgende Einstellung an der ENIGMA vorlag:

|  |  |  |  |
| --- | --- | --- | --- |
| **Nr.** | UKW | Walzenlage | Grundstellung |
| 1 | ? | I–II–III | T A B |

# Lösung

## Aufbau und Test der (Papier-) ENIGMA

Nr. 1: jaxge hat 🡪 Ja, geht

Nr. 2: drehe mitte

Nr. 3: drehe alles

Nr. 4: textlesbar

Nr. 5: wirha benes gesch afft

## Echte Funksprüche mit der ENIGMA chiffrieren/dechiffrieren (Niveau 1)

Test IV: xhans xhans xhatx esxka piert

## Echte Funksprüche mit der ENIGMA chiffrieren/dechiffrieren (Niveau 2)

1. -

2. xhans xhans xhatx esxka piert

3. individuelle Lösung in Abhängigkeit vom Schlüssel

4.

ANXRO EMXFU ENFSE QSXAR MXKOR PSXHO EHEXZ WONUL LNULL XSTAR KBESE ZTXAN GRIFF ERSTN AQSTA RKERA RTILL ERIEV ORBER EITUN GDURQ FUEHR BARXH ALTEE INAHM EVORS PAETE NABEN DNICH TFUER MOEGL ICHXV ONXVO NXKES SELXK ESSEL XHAUP TMANN

An LIV Armeekorps, Höhe 200 stark besetzt. Angriff erst nach starker Artillerievorbereitung durchführbar. Halte Einnahme vor späten Abend nicht für möglich. von Kessel, Hauptmann

## Einbruch in die ENIGMA-Verschlüsselung

Experiment 1: Es erscheint niemals A. Das geht nicht, da der Strom so nicht fließen kann.

Experiment 2:

|  |
| --- |
| ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD |
| ~~ABCD ABDC ACBD ACBD ACDB ADBC ADCB BACD~~ BADC BCDA BDAC ~~BDCA~~ |
| ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD |
| ~~CBAD~~ ~~CBDA~~ ~~CABD~~ CADB CDBA CDAB ~~DBCA~~ ~~DBAC~~ DCBA DCAB DABC ~~DACB~~ |

Es bleiben nur drei Alphabete übrig!

Experiment 3: Es gibt kein L (und wenige K). Das Ergebnis entspricht der UKW A.

AE BJ CM DZ FL GY HX IV KW NR OQ PU ST