Das Motto der LUG Walsrode für das Jahr 2012

PC und Privatsphäre

PC und Privatsphäre

Vortragsreihe zur Kryptologie

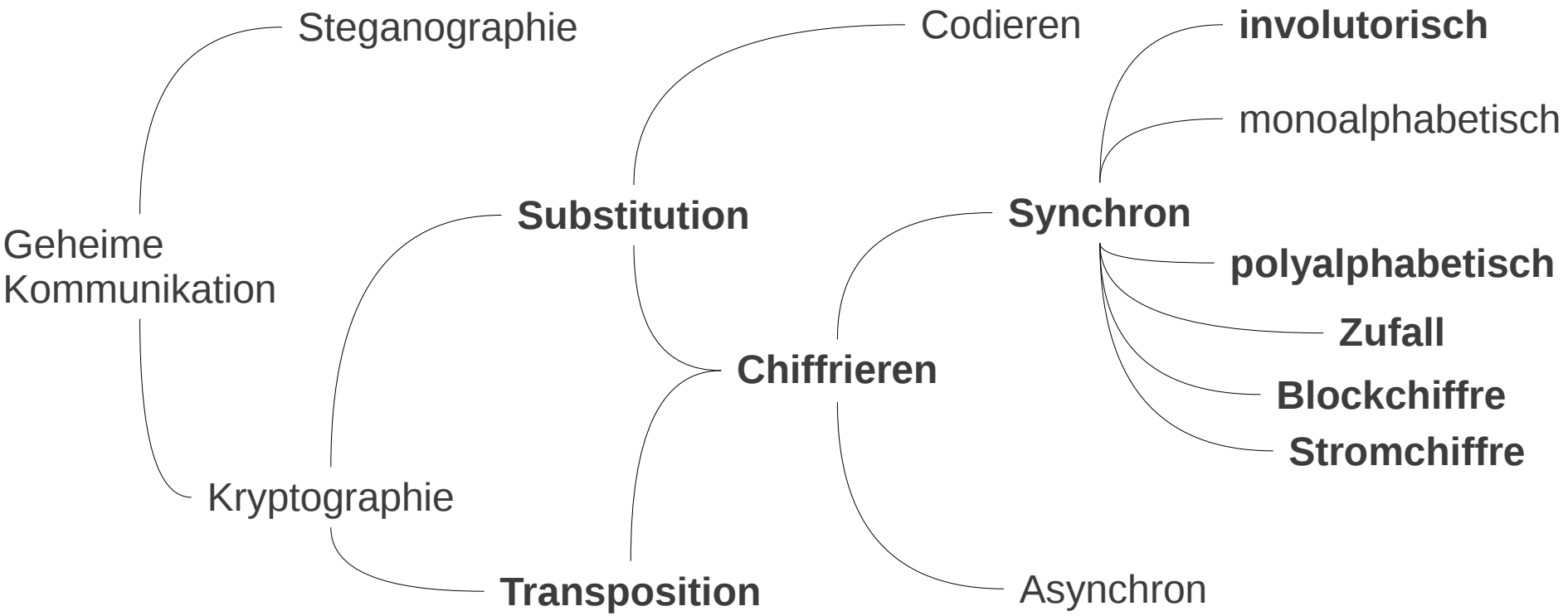
1. Geschichte der Kryptographie
2. Synchrone Verschlüsselung
3. **Enigma, Funktionsweise und Scheitern**
4. Verschleierung, Steganographie
5. Prim und Zufall
6. Asynchrone Verschlüsselung
7. Hash und Signaturen
8. Hybride Verschlüsselung

(9. Angriff auf WEP-LAN)

PC und Privatsphäre

Motivation und Ziel:
Sensibilität und Interesse wecken

Enigma



Quelle: Simon Singh, Codes, 2004 (ergänzt)

Enigma

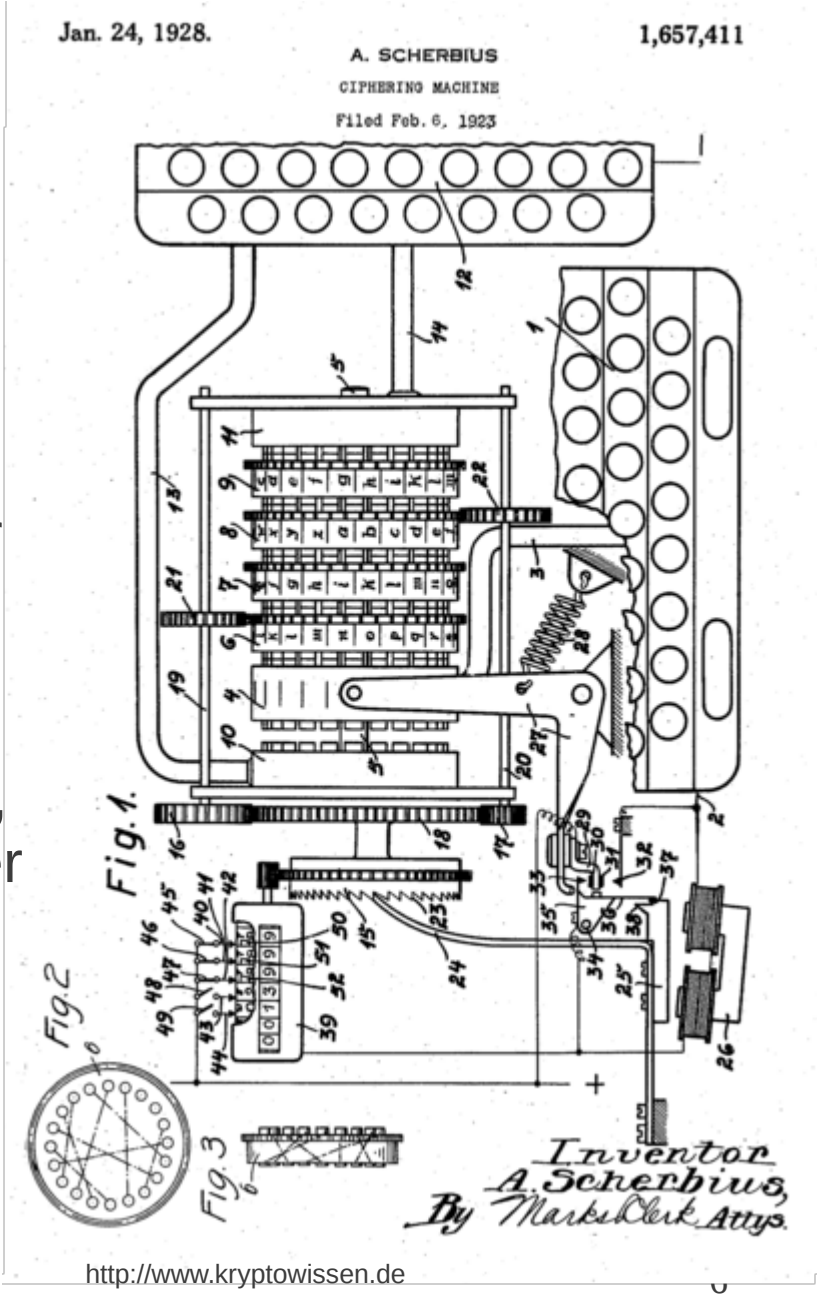
Funktion und Scheitern

- Geschichtlicher Überblick
- Aufbau
- Bedienung
- Online-Demo (Simulation)
- Scheitern
- Bedeutung für den Gebrauch von Kryptographie

Enigma

Geschichtlicher Überblick

Die erste Enigma wurde bereits 1918 von Arthur Scherbius patentiert. Neben anderen Entwicklungen auf diesem Gebiet stellt die Engima den Beginn der maschinellen Verschlüsselung dar. Die Funktionsweise der Enigma war Aufgrund des Patentes weltweit bekannt. Das Grundprinzip der Maschine beruhte auf elektrisch und mechanisch miteinander verschalteten Chiffrier-Scheiben, Walzen genannt. Das Grundprinzip ähnelt der bereits bekannte Vigenére-Verschlüsselung mit nun mehreren Tabellen.



Enigma

Anfänglich war das deutsche Militär überhaupt nicht von der Notwendigkeit einer solchen Maschine überzeugt.

Erst als Winston Churchill 1923 sein Buch „The World Crisis“ mit brisanten Details zur deutschen Kryptographie veröffentlichte und ein weitere Bericht aus England auch Inhalte und Methoden nennen konnte, wurde eine Untersuchung eingeleitet, die zum Ergebnis hatte, daß die Enigma die besten Voraussetzungen für die Erfüllung der künftigen kryptographischen Aufgaben hätte.

Und es war eine einheimische Entwicklung.

Enigma

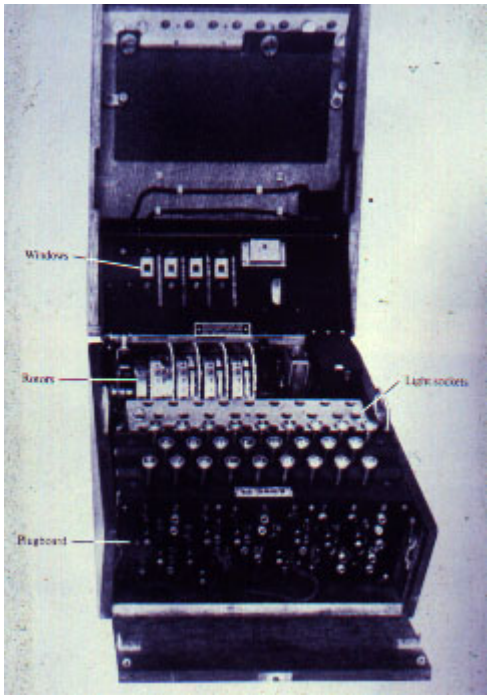
Zwischen 1918 und der ersten militärischen Serienproduktion 1925 hat die Enigma viele Veränderungen erfahren. Die für uns interessante Version ist die Enigma I, bestehend aus einem Steckfeld, einem Tastenfeld, dem Lampenfeld und den Walzen.

Quelle: http://forums.hexus.net/hexus-news/71866-enigma-cipher-machine-sale-now-ebay.html

Enigma

Aufbau

Das Augenfälligste an der Enigma sind die drei Rotoren (auch Walzen genannt). Einzelne Variante der Maschine hatten auch vier Walzen. Die Walzen konnten ausgetauscht werden. Ähnlich einem mechanischen Kilometerzähler bewegten sich die Walzen mit jeden Tastenanschlag weiter. Die rechte Walze drehte sich mit jedem Anschlag um eine Position weiter, die mittlere Walze wurde durch einen Mitnehmer der rechten Walze bewegt und die linke Walze schließlich durch den Mitnehmer der mittleren Walze.
Des weiteren gab es ganz links noch eine starre Walze, die als Umkehrwalze oder Reflektor diente.



http://www.turing.org.uk/turing/scrapbook/ww2.html

Enigma

Die Walzen

Jeder Walze war beidseitig mit jeweils 26 elektrischen Kontakten bestückt.
Im Inneren waren die Walzen unregelmäßig verdrahtet.
Diese Verdrahtungen sind das eigentliche Geheimnis der Enigma.
Für die hier behandelte Enigma kamen fünf verschieden verdrahtete Walzen (I, II, III, IV und V) zu Einsatz.

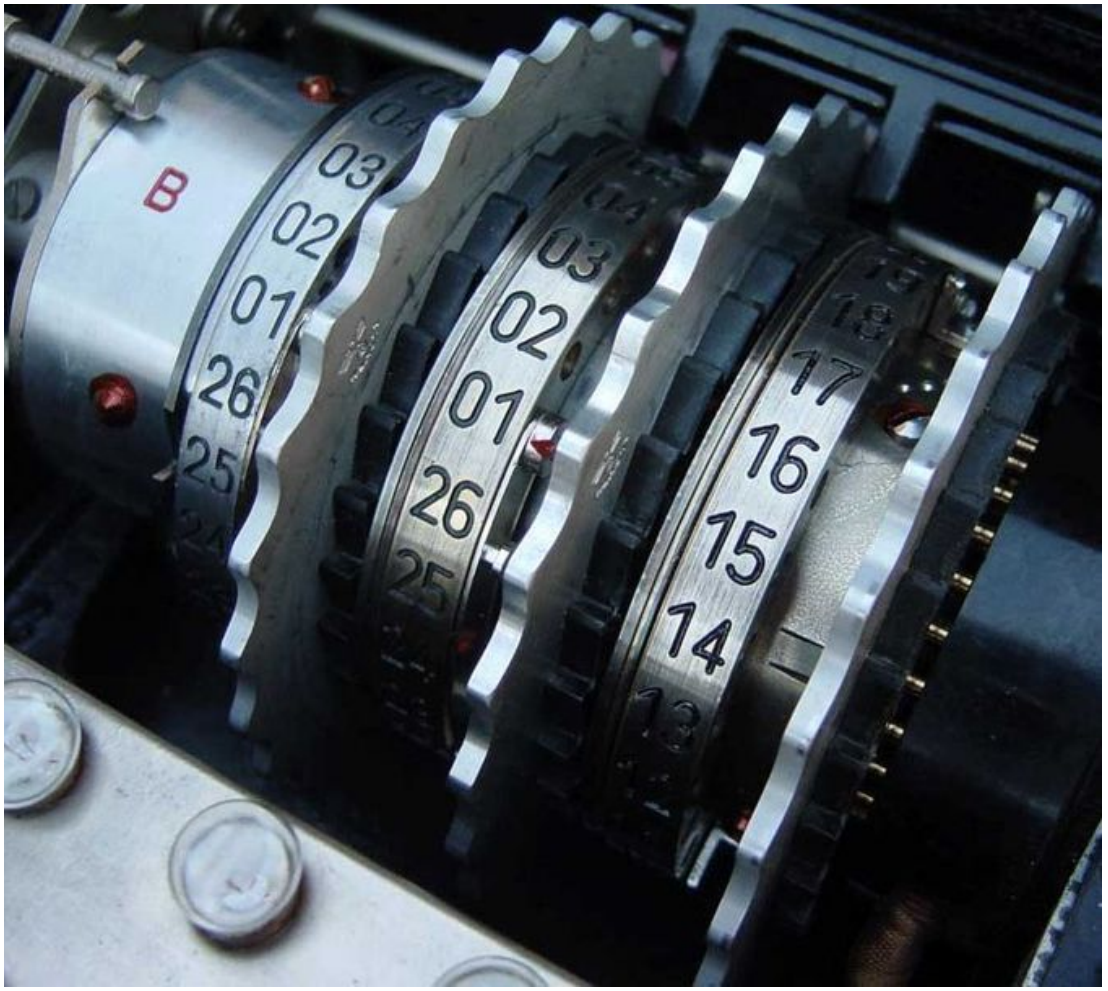
https://de.wikipedia.org/w/index.php?title=Datei:Enigma-rotor-pin-contacts.jpg&filetimestamp=20050808012315

Enigma

Die Umkehrwalze

Die Umkehrwalze (oder Reflektor) hatte ebenfalls 26 elektrische Kontakte, doch diese waren nur auf einer Seite. Die Kontakte waren intern auch verdrahtet.

https://de.wikipedia.org/w/index.php?title=Datei:EnigmaReflector.jpg&filetimestamp=20070209095019

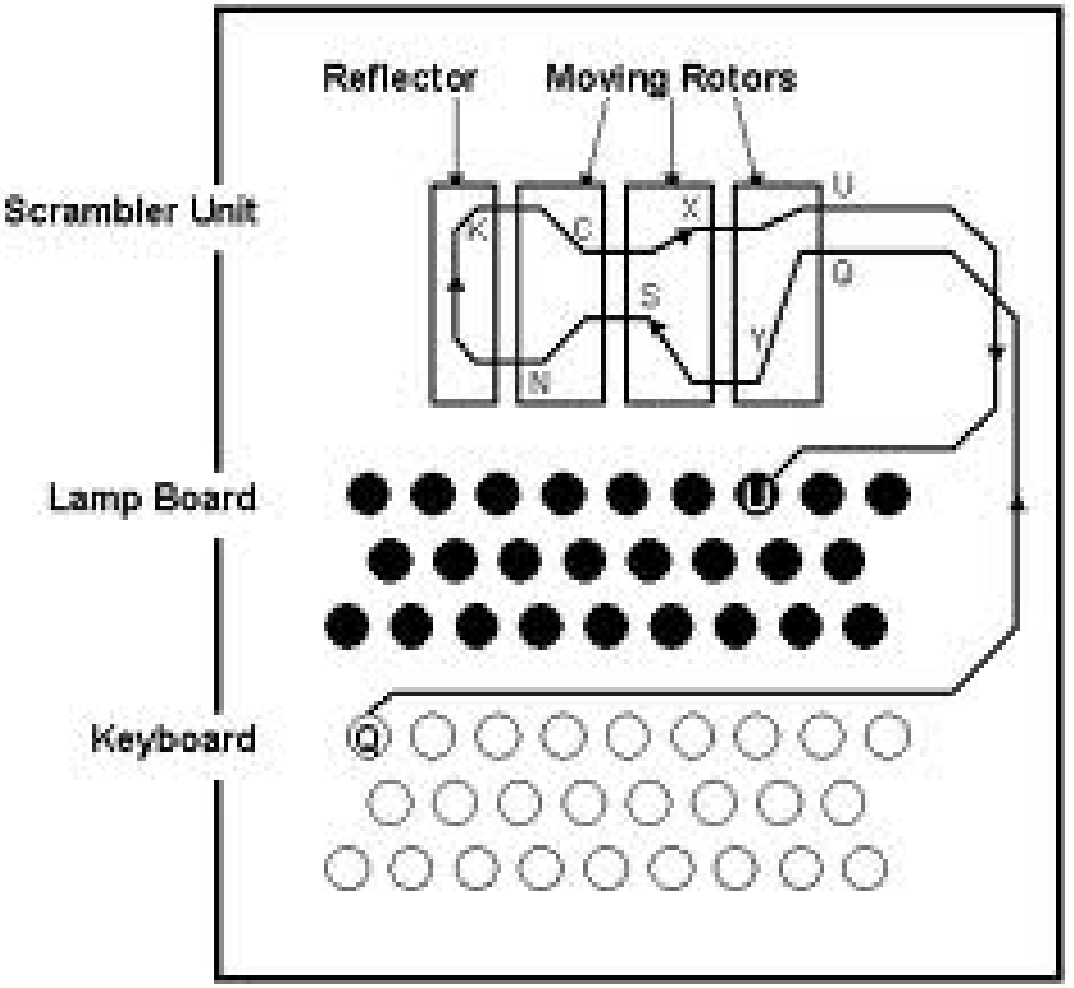


https://de.wikipedia.org/w/index.php?title=Datei:Enigma-rotor-stack-cropped.jpg&filetimestamp=20060215205523

Enigma

Elektrik

Mit jedem Tastenanschlag wurde ein elektrischer Kreis geschlossen. Der Strom ging durch die drei Walzen, wurde durch den Reflektor nochmals durch die drei Walzen geschickt und ließ am Ende eine Lampe aufleuchten.



http://www.sebastianlueth.de/index.php?page=Projekte%2FEnigma

Enigma

Bedienung

Die Handhabung der Enigma unterlag strengen Vorschriften. Damit der Geheimtext auch wieder entschlüsselt werden konnte, mußten gemeinsame Schlüssel, definiert durch Walzenauswahl, Walzenlage, Ringstellung, Grundstellung und Steckerverbindungen, vereinbart werden. Diese Vereinbarung erfolgte über die Schlüsseltafeln. Anfänglich waren monatliche Schlüssel vorgesehen, zum Ende des Krieges wurde der Schlüssel alle acht Stunden gewechselt. Gebräuchlich waren aber Tagesschlüssel.

Tag	UKW	Walzenlage	Ringstellung	---- Steckerverbindungen ----
31	B	I IV III	16 26 08	AD CN ET FL GI JV KZ PU QY WX
30	B	II V I	18 24 11	BN DZ EP FX GT HW IY OU QV RS
29	B	III I IV	01 17 22	AH BL CX DI ER FK GU NP OQ TY

http://krypto.mufuku.de/2006-10-18/wie-funktioniert-verschluesselung/

Enigma
Der Schlüssel

Walzenauswahl, -lage
Gemäß der Walzenlage mußten die auszuwählenden Walzen in dieser Reihenfolge in die Maschine eingesetzt werden.
Ringstellung
Der Mitnehmer jeder Walze konnte verstellt werden. Somit verschob sich der Moment der Mitnahme der jeweils linksseitigen Walze.
Grundstellung
Es ist die Ausgangsstellung für die Verschlüsselung.
Steckerverbindungen
Mit der Steckerverbindung konnten Buchstabenpaare vertauscht werden. Es stellt zwar nur eine einfache monoalphabetische Substitution dar, hat die Komplexität der Maschine aber erheblich erhöht.

Enigma

Schlüsselraum

Walzenlage
Drei aus fünf Walzen macht 60 Kombinationen
Ringstellung
Nur die Verschiebung der ersten beiden Walzen spielen eine Rolle, also 26 x 26 = 676 Kombinationen
Grundstellung
Jede Walze konnte eine andere Grundstellung einnehmen:
26 x 26 x 26 = 17576
Steckerverbindungen
Mittels 10 Kabeln konnten 150.738.274.937.250 verschiedene Kombinationen erstellt werden.

$$\frac{n!}{(n-2\mathrm{m})!\cdot m!\cdot 2^m}$$

107.458.687.327.250.619.360.000 mögliche Schlüssel

also rund 107 Trilliarden Schlüssel (~10^{24})

Enigma

Verschlüsseln

Nachdem die Vorgaben für den jeweiligen Tag aus der gültigen Schlüsseltafel eingestellt wurden, mußte sich der Schlüssler einen Spruchschlüssel ausdenken. Dieser sollte aus drei quasi zufälligen Buchstaben bestehen, z.B. LUG.
Diese Buchstabenfolge wurde nun **zweimal** in die Maschine eingegeben und der zu jedem getippten Buchstaben aufleuchtene Buchstabe notiert.
Nun wurde dieser 'zufällige' Schlüssel als Grundeinstellung eingestellt.
Damit wurde der Klartext in den Geheimtext übersetzt.
Sowohl die sechs verschlüsselten Buchstaben für den Spruchschlüssel als auch der Geheimtext konnten jetzt per Funk oder Boten übertragen werden.

Enigma

Entschlüsseln

Die eigentlich geniale Idee hinter der Funktionsweise der Enigma liegt in der einfachen Entschlüsselung eines Geheimtextes.

Die Maschine wurde gemäß Schlüsseltafel eingestellt, die ersten sechs Buchstaben wurden eingetippt. Das Ergebnis war zweimal der einzustellende Spruchschlüssel. Dieser wurde eingestellt und der Rest des Geheimtextes konnte nun übersetzte werden.
Diese einfache Handhabung verdankt die Maschine der Umkehrwalze (oder auch Reflektor genannt).

Somit war die Enigma eine **involutorische*** Rotor-Chiffriermaschine.

* selbstinverse Abbildung

Enigma

Online-

http://www.ostfalia.de/cms/de/pws/seutter/kryptologie/enigma/Simulation/Simulator/simulation.html

Enigma

Scheitern

Systematische Fehler

- Umkehrwalze
- Cribs
- Schlüsselverteilung
- Spruchschlüssel
- Walzenauswahl, -lage, Steckverbindungen

Handhabungsfehler

- Quasi zufällige Spruchschlüssel
- Wetterberichte
- 'gardening'

Enigma

Umkehrwalze

Der vermeintliche Vorteil der Involutorik führte kryptologisch zu einer Einschränkung des Schlüsselraumes.

1. Kein Buchstabe wurde mit sich selbst verschlüsselt.

2. Buchstaben wurden immer paarweise verschlüsselt:
   - aus A wurde E,
   - mit der gleichen Einstellung wurde aus E aber auch A.

Enigma

Beispiel

Als Beispiel dient ein viel zitiertes Alphabet aus vier Buchstaben.
Zuerst streichen wir alle Alphabete mit sogenannten Fixpunkten (**fett**).
Als nächstes werden auch noch alle nichtinvolutorischen Alphabete (*kursiv*) gestrichen.
Übrig bleiben drei verwendbare Alphabete.

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

Für die Enigma bedeutete diese Tatsache, daß der verfügbare Schlüsselraum von 10^{24} auf ungefähr 10^{13} schrumpfte.

Enigma

Cribs

Als Cribs bezeichnet der Kryptoanalytiker Wortphrasen, z.B. Oberkommando Wehrmacht.

Wenn nun vermutet wird, daß so eine Phrase in einem Geheimtext verschlüsselt sein könnte, kann man anfangen nach der passenden Stelle zu suchen.

Mit dem Wissen, daß ein Buchstabe niemals mit sich selber verschlüsselt werden kann, lassen sich Rückschlüsse auf die Position innerhalb des Textes ziehen. Und somit auch einzelne Schlüssel ausschließen.

Enigma

Beispiel

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

https://de.wikipedia.org/wiki/Enigma_%28Maschine%29

Enigma

Schlüsselverteilung

Das größte Problem stellte die Verteilung und Wahrung der Schlüsseltafeln dar.
Aus Sicherheitsgründen waren die Schlüsseltafeln nur für einen Monat gültig.

Nicht selten konnten Schlüsseltafel und andere als geheim eingestufte Dokumente erbeutet werden..

Das Aktualisieren der Schlüssel war besonders bei weit operierenden Einheit, z.B. U-Booten, ein erhebliches Problem.

Enigma

Spruchschlüssel

Der Spruchschlüssel mußte gemäß Dienstanweisung doppelt eingegeben werden.

Dieses Vorgehen erleichterte die statistische Suche nach dem passenden Schlüssel.

Enigma

Walzenauswahl, -lage

Die Walzenauswahl, wie auch die Walzenlage, wurde nach einem genau beschriebenen Verfahren erstellt.

So durfte z.B. keine Walze an zwei aufeinander folgenden Tagen an der gleichen Stelle eingesetzt werde.

Mit dieser Erkenntnis ließ sich so durchaus eine Walze für einen folgenden Tag ausschließen.

Enigma

Quasi zufällige Spruchschlüssel

Aus Bequemlichkeit wurde von den Schlüsslern gerne mal der gleich Schlüssel für mehrere Nachrichten an unterschiedliche Empfänger verwendet.

Auch wurden gerne sinnvolle, zusammenhängende oder gar gleiche Buchstabenfolgen verwendet.

Enigma

Wetterberichte

Wetterberichte wurden häufig zweimal gesendet. Das erste Mal unverschlüsselt, das zweite Mal verschlüsselt.

Damit wurde ein Angriff auf den Schlüssel vereinfacht.

Enigma

'gardening'

'Gardening' ist eigentlich kein richtiger Handhabungsfehler, sondern viel mehr der alliierte Versuch das deutsche Militär zu konkreten vorher bekannten Daten zu zwingen.

Beispielsweise wurden gezielt in einem Seegebiet Minen abgeworfen, um eine Nachricht, aus der mindestens die Koordinaten bekannt sind, zu erzwingen.

Enigma

Bedeutung für den Gebrauch der Kryptographie

1.Der Schlüsselraum alleine bietet noch keine Gewährleistung, daß eine Nachricht nicht gebrochen werden kann. Gegen systembedingte Schwächen kann der Nutzer nichts unternehmen.
Umso wichtiger ist es, daß verwendete und/oder erzeugte Sitzungsschlüssel lang und vielleicht wirklich annähernd zufällig sein sollten.

2.Der eigentliche Klartext sollte auch auf dem eigenen System nicht existieren, sondern nur in verschlüsselter Form abgespeichert sein.

3.Mehrere Nachrichten sollten nicht mit dem Sitzungsschlüssel einer vorherigen Nachricht verschlüsselt werden.

Ende
und
Vielen Dank