Enigma

Klaus Schmeh, GITS AG

www.gits-ag.de

schmeh@gits-ag.de

Anzeigen

Geschichte der Kryptografie

3000 v. Chr. - 1920	Zeitalter der Verschlüsselung von Hand
1920 – 1975	Zeitalter der Verschlüsselungsmaschinen
1975 - ?	Zeitalter der Computer-Verschlüsselung

Verschlüsselung von Hand

- Noch im Ersten Weltkrieg eingesetzt
- Beispiel: Vigenere-Verschlüsselung

A=0, B=1, C=2, D=3, …

Schlüssel: HITFORUM

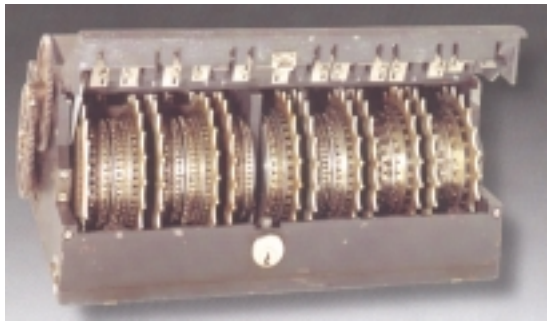
```
DER BALL IST RUND UND EIN SPIEL DAUERT NEUNZIG MINUTEN.
HIT FORU MHI TFOR UMH ITF ORUMH ITFORU MHITFOR UMHITFO.
-------------------------------------------------------
KMK GOCF UZB KZBU OZK MBS GGCQS LTZSIN ZLCGEWX GUUCMJB.
```

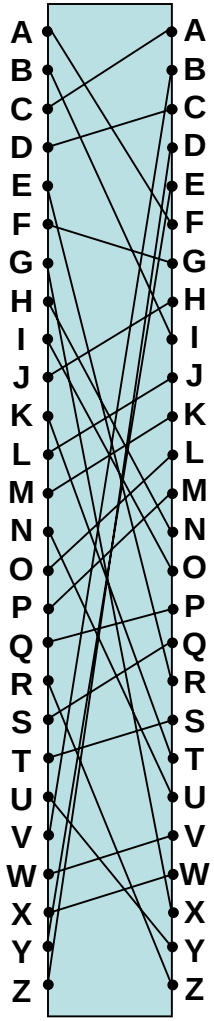
Verschlüsselung mit der Maschine

- Nahezu alle Verfahren zur Verschlüsselung von Hand wurden gebrochen
- Bessere Verfahren wurden benötigt
- Um 1920 erfanden vier Personen unabhängig voneinander das so genannte Rotor-Prinzip
- Einer davon war Arthur Scherbius
- Seine Maschine hieß Enigma

Das Rotor-Prinzip (Rotor-Chiffren)

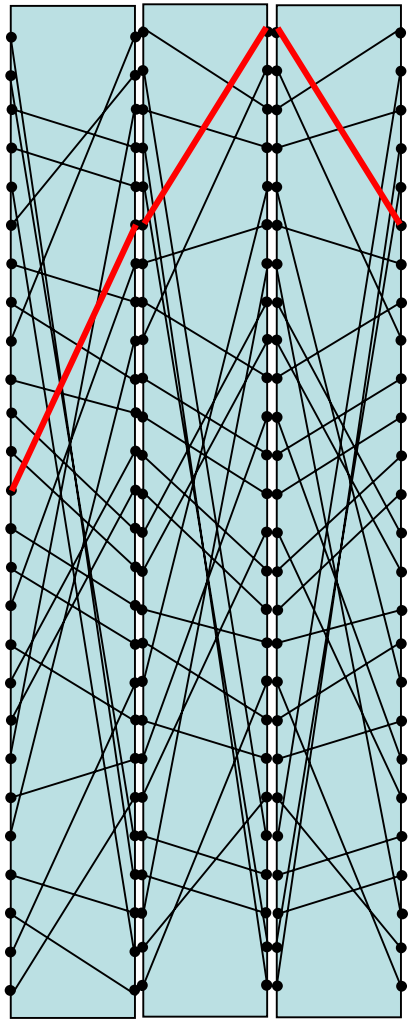
- Verschlüsselung durch verdrahtete Rotoren
- Mehrere Rotoren hintereinander geschaltet
- Rotoren bewegen sich wie Kilometer-Zähler
- Eingabe eines Buchstabens über Tastatur
- Verschlüsselter Buchstabe wird durch Lampe angezeigt





Das Rotor-Prinzip (Rotor-Chiffren)

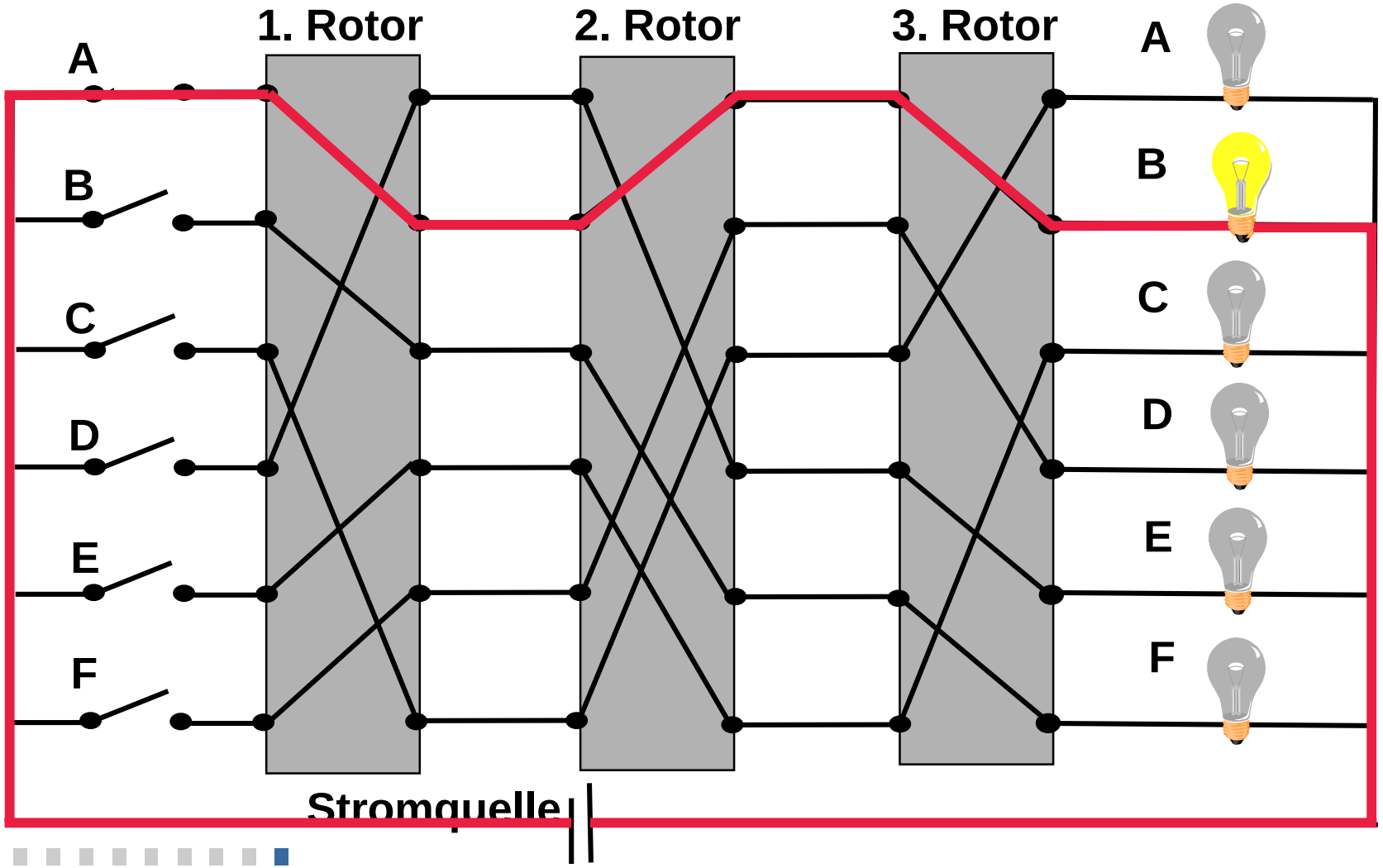
- Anfangsstellung der Rotoren als Schlüssel
- Selbst bei bekannter Verdrahtung ist die Entschlüsselung kaum möglich
- $26^3 = 17.576$ mögliche Schlüssel
- Verwendung unterschiedlicher Rotoren erhöht Sicherheit



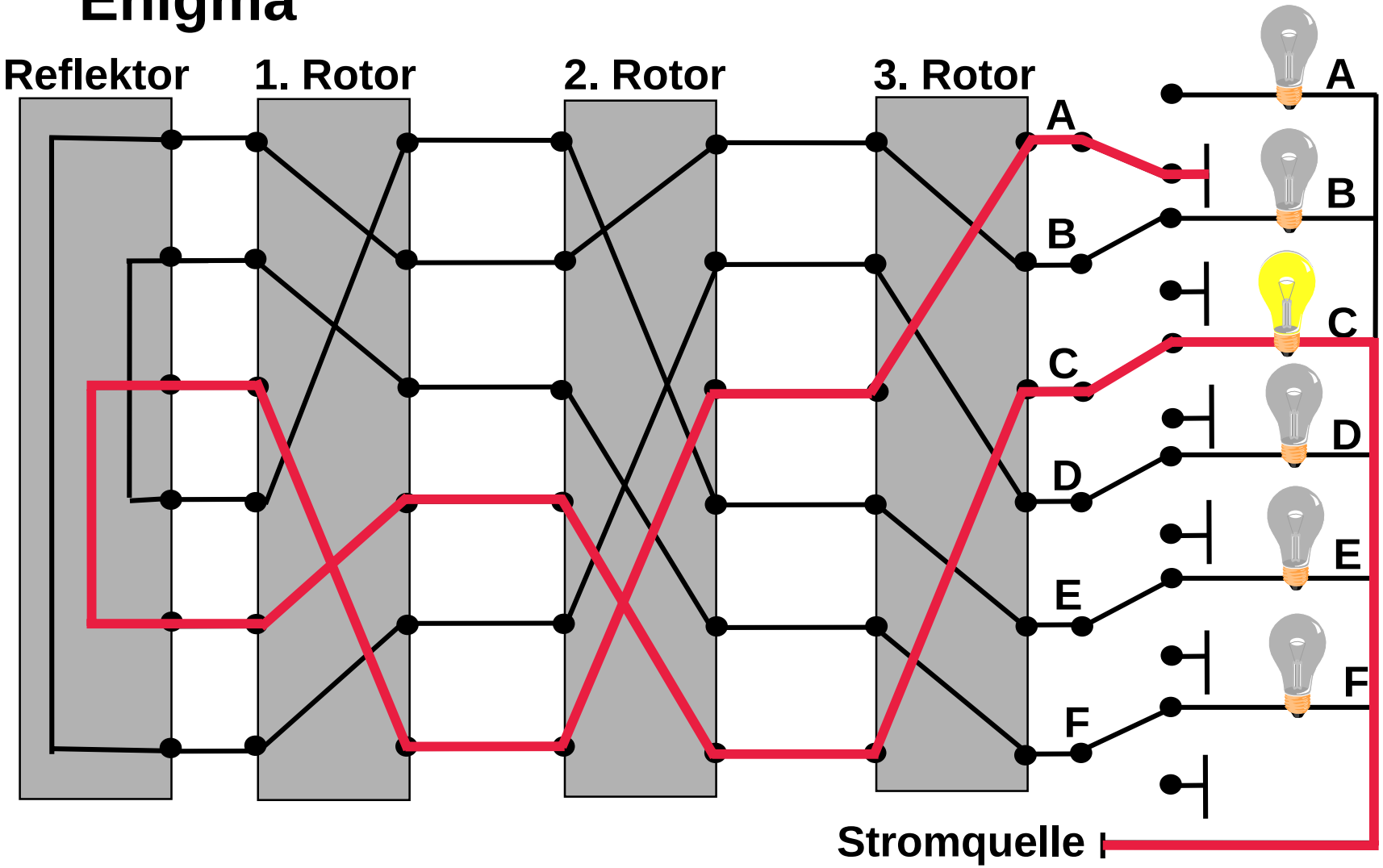
Die Enigma

- Legendäre deutsche Verschlüsselungsmaschine
- Um 1918 von Arthur Scherbius erfunden
- Verwendet Rotor-Prinzip mit Reflektor
- Einsatz durch Wehrmacht
- Über 30.000 Exemplare wurden produziert
- Entscheidende Bedeutung im Zweiten Weltkrieg
- Galt als absolut sicher, wurde aber geknackt

Einfache Rotor-Chiffre



Enigma


Reflektor
1. Rotor
2. Rotor
3. Rotor
A
B
C
D
E
F
A
B
C
D
E
F
Stromquelle

Enigma mit Schlüsselbuch

Wie die Enigma geknackt wurde

1932: Polnischer Geheimdienst knackt erstmals Wehrmacht-Enigma

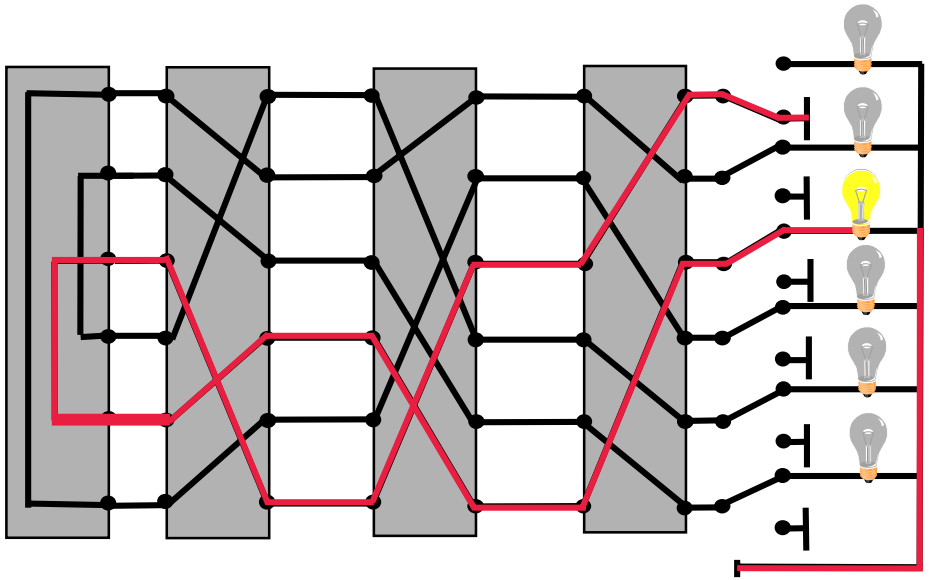
1938: Polnischer Geheimdienst baut Enigma-Knack-Maschine „Bomba“

1938: Britischer Geheimdienst wird eingeweiht

- Briten bauen „Dechiffrier-Fabrik“ in Bletchley Park
- Bomba wird weiterentwickelt („Bombe“, Vorläufer des Computers)
- Über 7.000 Mitarbeiter an Entschlüsselung beteiligt
- Zahlreiche (aber nicht alle) Nachrichten konnten entschlüsselt werden

Schwachstellen der Enigma

- Knacken der Enigma war nur mit immensem Aufwand möglich
- Reflektor erwies sich als Schwachstelle
- Aufgefundene Schlüsselbücher und Spionage half den Alliierten
- Schlampiger Umgang der Deutschen mit der Enigma war entscheidend



Der Reflektor als Schwachstelle

Durch den Reflektor wird kein Buchstabe wird in sich selbst verschlüsselt.

```
DRLMP TKOSM ECXVG WSIMN KLRTB FKOYP CRZVQ QZERN
LEUCH TBOJE
 LEUC HTBOJ E
  LEU CHTBO JE
   LE UCHTB OJE
```

Folgen der Enigma-Entschlüsselung

- Die Alliierten wussten über viele geheime Pläne der Deutschen Bescheid
- U-Boot-Krieg wurde durch dechiffrierte Enigma-Funksprüche mit entschieden
- Enigma spielte wichtige Rolle im Nordafrika-Krieg
- Ohne die Enigma-Dechiffrierung hätte der Zweite Weltkrieg länger gedauert

Die Enigma nach dem Zweiten Weltkrieg

- Enigma-Entschlüsselung blieb bis in die 70er Jahre geheim
- Die volle Wahrheit ist bis heute unbekannt
- Rotor-Chiffren wurden bis in die 70er Jahre verwendet
- Es gibt zahlreiche andere Verschlüsselungsmaschinen, die ähnlich funktionieren

Ende

Wir bedanken uns:

- beim Bundesamt für Sicherheit in der Informationstechnik (BSI) und bei Fred Fischer für die Enigma-Leihgabe
- bei der GITS Projekt GmbH und Herrn Martin Kloppenburg für die Bereitstellung der Enigma und des Raums