Die ENIGMA

Vorlesungsvertretung Elliptische Kurven und Kryptographie

Franziska Jahnke

WWU Münster

17.06.15

Geschichte der Enigma – Entwicklung

Die Enigma ist eine mechanische Verschlüsselungsmaschine, die im zweiten Weltkrieg eingesetzt wurde.

- erste mechanische Verschlüsselungsmaschinen werden nach dem ersten Weltkrieg entwickelt
  - $\rightsquigarrow$ werden fortlaufend verbessert
- als Erfinder der Enigma gilt Arthur Scherbius (1878–1929, Enigma-Patent 1918)
- Herstellung ab 1934 im großen Stil
- Verwendung: Verschlüsselung des Nachrichtenverkehrs des deutschen Militärs und anderer Dienste (SS, Polizei, Reichsbahn, . . .)
- Einsatz insgesamt ca. 100.000 Stück

Geschichte der Enigma – Entschlüsselung

- Enigma galt als kryptographisch sicher
- Alliierten gelang es, die deutschen Funksprüche zu entziffern und vollständig abzuhören (Codename Ultra)
- ohne Kenntnis der Deutschen $\rightsquigarrow$ großer strategischer Vorteil!
- Schätzung: "Knacken" der Enigma verkürzt den zweiten Weltkrieg um 2–4 Jahre

  $\rightsquigarrow$ Rettung vieler Menschenleben auf allen Seiten des Krieges

Aufbau und Prinzip

Enigma Verschlüsselungsmaschine mit Beschriftung

Foto: Karsten Sperling

Beispiel - Papier Enigma

Verwenden Sie die Papier Enigma mit den folgenden Einstellungen:

- linke Walze = I, mittlere Walze = II, rechte Walze = III
- Startposition der Walzen ist `FMJ`

Beispiel - Papier Enigma

Verwenden Sie die Papier Enigma mit den folgenden Einstellungen:

- linke Walze = I, mittlere Walze = II, rechte Walze = III
- Startposition der Walzen ist `FMJ`

Was ist die decodierte Nachricht zum Geheimtext `JWNBUN`?

Beispiel - Papier Enigma

Verwenden Sie die Papier Enigma mit den folgenden Einstellungen:

- linke Walze = I, mittlere Walze = II, rechte Walze = III
- Startposition der Walzen ist `FMJ`

Was ist die decodierte Nachricht zum Geheimtext `JWNBUN`?

1. Rechte Walze bewegt sich einen Schritt.

Beispiel - Papier Enigma

Verwenden Sie die Papier Enigma mit den folgenden Einstellungen:

- linke Walze = I, mittlere Walze = II, rechte Walze = III
- Startposition der Walzen ist `FMJ`

Was ist die decodierte Nachricht zum Geheimtext `JWNBUN`?

1. Rechte Walze bewegt sich einen Schritt.
2. `J` geht auf `A` beim Übergang zur rechten Walze,

Beispiel - Papier Enigma

Verwenden Sie die Papier Enigma mit den folgenden Einstellungen:

- linke Walze = I, mittlere Walze = II, rechte Walze = III
- Startposition der Walzen ist `FMJ`

Was ist die decodierte Nachricht zum Geheimtext `JWNBUN`?

1. Rechte Walze bewegt sich einen Schritt.
2. `J` geht auf `A` beim Übergang zur rechten Walze, `A` geht auf `D` beim Übergang zur mittleren Walze,

Beispiel - Papier Enigma

Verwenden Sie die Papier Enigma mit den folgenden Einstellungen:

- linke Walze = I, mittlere Walze = II, rechte Walze = III
- Startposition der Walzen ist `FMJ`

Was ist die decodierte Nachricht zum Geheimtext `JWNBUN`?

1. Rechte Walze bewegt sich einen Schritt.
2. `J` geht auf `A` beim Übergang zur rechten Walze, `A` geht auf `D` beim Übergang zur mittleren Walze, `D` geht auf `B` beim Übergang zur linken Walze.

Beispiel - Papier Enigma

Verwenden Sie die Papier Enigma mit den folgenden Einstellungen:

- linke Walze = I, mittlere Walze = II, rechte Walze = III
- Startposition der Walzen ist `FMJ`

Was ist die decodierte Nachricht zum Geheimtext `JWNBUN`?

1. Rechte Walze bewegt sich einen Schritt.
2. `J` geht auf `A` beim Übergang zur rechten Walze, `A` geht auf `D` beim Übergang zur mittleren Walze, `D` geht auf `B` beim Übergang zur linken Walze.
3. `B` geht auf `V` und wird auf der Umkehrwalze gespiegelt.

Beispiel - Papier Enigma

Verwenden Sie die Papier Enigma mit den folgenden Einstellungen:

- linke Walze = I, mittlere Walze = II, rechte Walze = III
- Startposition der Walzen ist `FMJ`

Was ist die decodierte Nachricht zum Geheimtext `JWNBUN`?

1. Rechte Walze bewegt sich einen Schritt.
2. `J` geht auf `A` beim Übergang zur rechten Walze, `A` geht auf `D` beim Übergang zur mittleren Walze, `D` geht auf `B` beim Übergang zur linken Walze.
3. `B` geht auf `V` und wird auf der Umkehrwalze gespiegelt.
4. `V` $\rightsquigarrow$ `A`

Beispiel - Papier Enigma

Verwenden Sie die Papier Enigma mit den folgenden Einstellungen:

- linke Walze = I, mittlere Walze = II, rechte Walze = III
- Startposition der Walzen ist `FMJ`

Was ist die decodierte Nachricht zum Geheimtext `JWNBUN`?

1. Rechte Walze bewegt sich einen Schritt.
2. `J` geht auf `A` beim Übergang zur rechten Walze, `A` geht auf `D` beim Übergang zur mittleren Walze, `D` geht auf `B` beim Übergang zur linken Walze.
3. `B` geht auf `V` und wird auf der Umkehrwalze gespiegelt.
4. `V` $\rightsquigarrow$ `A` $\rightsquigarrow$ `B`

Beispiel - Papier Enigma

Verwenden Sie die Papier Enigma mit den folgenden Einstellungen:

- linke Walze = I, mittlere Walze = II, rechte Walze = III
- Startposition der Walzen ist `FMJ`

Was ist die decodierte Nachricht zum Geheimtext `JWNBUN`?

1. Rechte Walze bewegt sich einen Schritt.
2. `J` geht auf `A` beim Übergang zur rechten Walze, `A` geht auf `D` beim Übergang zur mittleren Walze, `D` geht auf `B` beim Übergang zur linken Walze.
3. `B` geht auf `V` und wird auf der Umkehrwalze gespiegelt.
4. `V` $\rightsquigarrow$ `A` $\rightsquigarrow$ `B` $\rightsquigarrow$ `H`

Beispiel - Papier Enigma

Verwenden Sie die Papier Enigma mit den folgenden Einstellungen:

- linke Walze = I, mittlere Walze = II, rechte Walze = III
- Startposition der Walzen ist `FMJ`

Was ist die decodierte Nachricht zum Geheimtext `JWNBUN`?

1. Rechte Walze bewegt sich einen Schritt.
2. `J` geht auf `A` beim Übergang zur rechten Walze, `A` geht auf `D` beim Übergang zur mittleren Walze, `D` geht auf `B` beim Übergang zur linken Walze.
3. `B` geht auf `V` und wird auf der Umkehrwalze gespiegelt.
4. `V` $\rightsquigarrow$ `A` $\rightsquigarrow$ `B` $\rightsquigarrow$ `H` $\rightsquigarrow$ `T`

Beispiel - Papier Enigma

Verwenden Sie die Papier Enigma mit den folgenden Einstellungen:

- linke Walze = I, mittlere Walze = II, rechte Walze = III
- Startposition der Walzen ist `FMJ`

Was ist die decodierte Nachricht zum Geheimtext `JWNBUN`?

1. Rechte Walze bewegt sich einen Schritt.
2. `J` geht auf `A` beim Übergang zur rechten Walze, `A` geht auf `D` beim Übergang zur mittleren Walze, `D` geht auf `B` beim Übergang zur linken Walze.
3. `B` geht auf `V` und wird auf der Umkehrwalze gespiegelt.
4. `V` $\rightsquigarrow$ `A` $\rightsquigarrow$ `B` $\rightsquigarrow$ `H` $\rightsquigarrow$ `T`
5. Also: `J` $\rightsquigarrow$ `T`.

Schwierigkeiten beim Entschlüsseln

- Innere Verdrahtung

Schwierigkeiten beim Entschlüsseln

- Innere Verdrahtung
  $\rightsquigarrow$ weitgehend gelöst durch die Arbeiten der polnischen Kryptographen um Marian Rejewski

Foto: Privatarchiv von M. Rejewskis Tochter

Schwierigkeiten beim Entschlüsseln

- Innere Verdrahtung
  $\rightsquigarrow$ weitgehend gelöst durch die Arbeiten der polnischen Kryptographen um Marian Rejewski
- Täglich wechselnde Walzeneinstellungen

Foto: Matt Crypto

Schwierigkeiten beim Entschlüsseln

- Innere Verdrahtung
  $\rightsquigarrow$ weitgehend gelöst durch die Arbeiten der polnischen Kryptographen um Marian Rejewski
- Täglich wechselnde Walzeneinstellungen
  Auch wenn eine Nachricht mit Verschlüsselung bekannt ist, kann man noch nicht alle anderen Nachrichten des Tages entschlüsseln.

Foto: Matt Crypto

Ansätze zur Entschüsselung

- Einsatz immensen Personals und immenser Mittel in GC&CS (fast 10.000 Beschäftigte in Bletchley Park)

Ansätze zur Entschüsselung

- Einsatz immensen Personals und immenser Mittel in GC&CS (fast 10.000 Beschäftigte in Bletchley Park)
- Verwendung von wahrscheinlichen Wörtern (Cribs)

Ansätze zur Entschüsselung

- Einsatz immensen Personals und immenser Mittel in GC&CS (fast 10.000 Beschäftigte in Bletchley Park)
- Verwendung von wahrscheinlichen Wörtern (Cribs) etwa ‘Wettervorhersage’ oder ‘Oberkommando der Wehrmacht’

Ansätze zur Entschüsselung

- Einsatz immensen Personals und immenser Mittel in GC&CS (fast 10.000 Beschäftigte in Bletchley Park)
- Verwendung von wahrscheinlichen Wörtern (Cribs) etwa ‘Wettervorhersage’ oder ‘Oberkommando der Wehrmacht’
- Verschlüsselung ist fixpunktfrei

Ansätze zur Entschüsselung

- Einsatz immensen Personals und immenser Mittel in GC&CS (fast 10.000 Beschäftigte in Bletchley Park)
- Verwendung von wahrscheinlichen Wörtern (Cribs)
  etwa ‘Wettervorhersage’ oder ‘Oberkommando der Wehrmacht’
- Verschlüsselung ist fixpunktfrei
  Bauweise der Enigma $\rightsquigarrow$ kein Buchstabe kann als er selbst kodiert werden

Ansätze zur Entschüsselung

- Einsatz immensen Personals und immenser Mittel in GC&CS (fast 10.000 Beschäftigte in Bletchley Park)
- Verwendung von wahrscheinlichen Wörtern (Cribs)
  etwa ‘Wettervorhersage’ oder ‘Oberkommando der Wehrmacht’
- Verschlüsselung ist fixpunktfrei
  Bauweise der Enigma $\rightsquigarrow$ kein Buchstabe kann als er selbst kodiert werden
- Verschlüsselung ist involutorisch

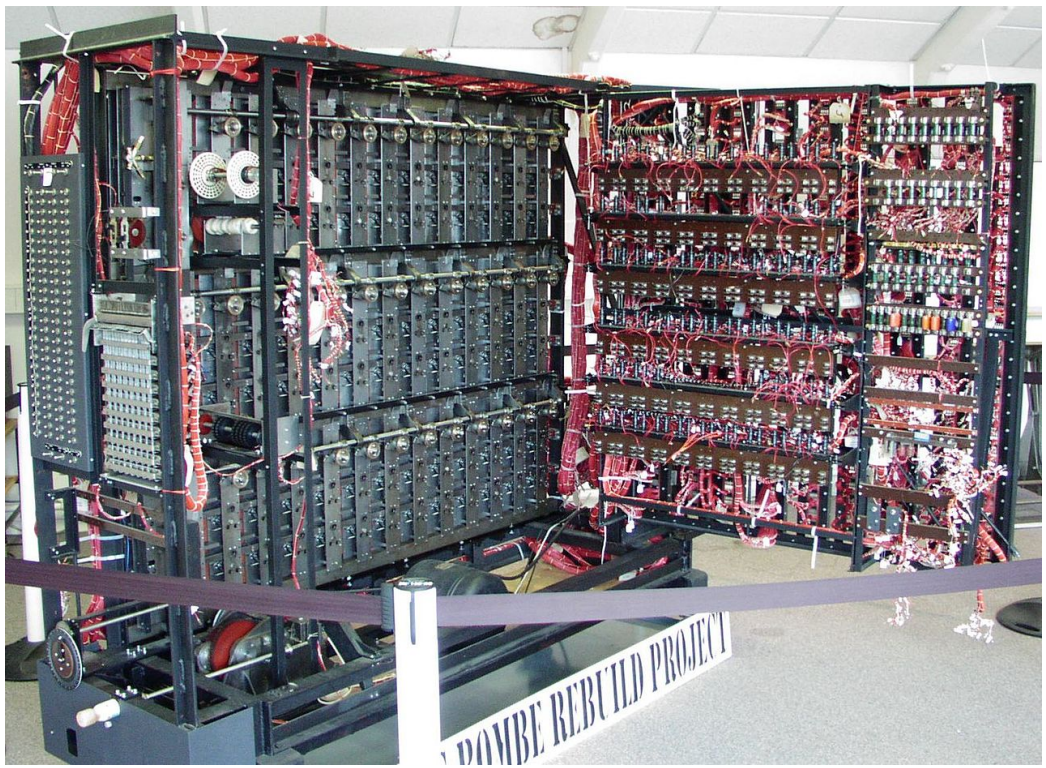
Ansätze zur Entschüsselung

- Einsatz immensen Personals und immenser Mittel in GC&CS (fast 10.000 Beschäftigte in Bletchley Park)
- Verwendung von wahrscheinlichen Wörtern (Cribs)
  etwa ‘Wettervorhersage’ oder ‘Oberkommando der Wehrmacht’
- Verschlüsselung ist fixpunktfrei
  Bauweise der Enigma $\rightsquigarrow$ kein Buchstabe kann als er selbst kodiert werden
- Verschlüsselung ist involutorisch
  Verschlüsseln $=$ Entschlüsseln

Maschinen entwickelt zum Decodieren von Enigma

Bomba $\rightsquigarrow$ Turing-Bombe (ab 1940)

braucht nur etwa 10 Stunden zum Testen sämtlicher Möglichkeiten



Fotos: Jon Callas (links) und Tom Yates (rechts)

Übungsaufgabe

Gegeben ist eine ‘Mini-Enigma’ mit dem Alphabet $\Sigma = \{\texttt{A},\texttt{E},\texttt{H},\texttt{N}\}$ mit zwei Walzen und einer Umkehrwalze. Bekannt ist, dass der Klartext `AHNE HANN AHNA HEAN NE` verschlüsselt wurde zu `HAEN AHEE HAEH ANHE EN`.

1. Mit welcher inneren Verdrahtung arbeitet die Enigma?
2. Welcher Geheimtext wird (bei gleicher Anfangsstellung) dem Klartext `NAEH EANN A` zugeordnet?