

Turingbomben

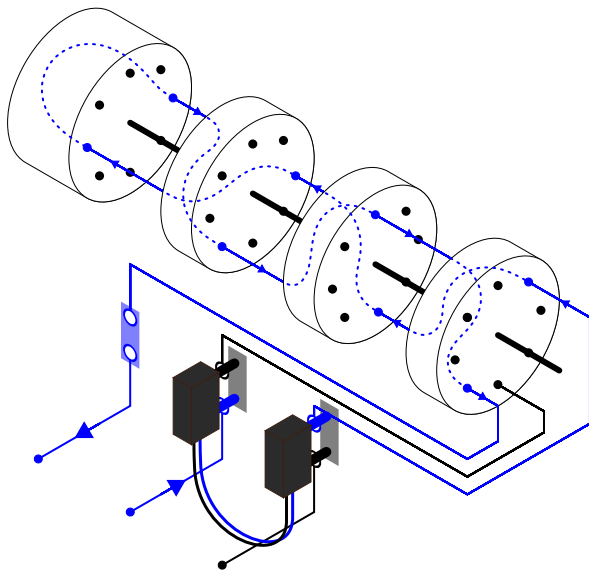
andi (Entropia)
⟨andi@entropia.de⟩

GPN 14

Schon mal gesehen?



Enigma von innen



Errata

Zur letzten Folie habe ich eine sehr wichtige Bemerkung im Vortrag vergessen: Die Umkehrwalze kann nicht anders, als je zwei Buchstaben in Paaren zu vertauschen. Kompliziertere Permutationen sind nicht möglich, weil die Walzen alle nur aus Dreht bestehen, und Hin- und Rückweg geshalb gleich sein müssen. Diese Eigenschaft überträgt sich auch auf den gesamten Walzensatz und schließlich auf die gesamte Enigma: Wenn **x** zu **y** verschlüsselt wird, dann muss **y** zu **x** verschlüsselt werden. Das bedeutet, dass Verschlüsseln und Entschlüsseln das Gleiche sind. Diese Tatsache wird später noch wichtig werden. Außerdem habe ich wild Groß- und Kleinbuchstaben durcheinandergeworfen, das ist jetzt auch korrigiert. Kleine Buchstaben stehen für Klar- oder Ciphertext, große Buchstaben stehen für Signale, die in der Enigma oder Bombe intern („hinter“ dem Steckerbrett) vorhanden sind.

Enigma von innen

Die Walzen



Einfach mal Brute-Force?

Schlüsselraum einer Enigma (ganz, ganz naiv...)

Startposition	$26^3 =$	17 576
Walzenauswahl	$\binom{5}{3} \cdot 3! =$	60
Übertrag	$26^2 =$	676
Stecker		150 738 274 937 250
Gesamt		206 651 321 783 174 268 000 000 (2^{77})

Einfach mal Brute-Force?

Schlüsselraum einer Enigma (ganz, ganz naiv...)

Startposition	$26^3 =$	17 576
Walzenauswahl	$\binom{5}{3} \cdot 3! =$	60
Übertrag	$26^2 =$	676
Stecker		150 738 274 937 250
Gesamt		206 651 321 783 174 268 000 000 (2^{77})

Moderne Brute-Force-Maschine: 119 000 000 000 AES-Keys/s

⇒ 55 066 Jahre für einen Enigma-Schlüssel.

(Das ist nach heutigen Maßstäben *sehr* wenig!)

Enigma-Funkprotokoll

Geheim!		OKH-Maschinenschlüssel A Nr. 39														Nr. 00014					
Nicht ins Flugzeug mitnehmen!																					
	Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
0	31.	V	II	IV	17	09	02	KT	AJ	IV	UR	NY	HZ	GD	XF	PB	CQ	sfy	azy	zkq	bqi
0	30.	I	III	V	22	12	10	UE	PL	AY	TB	ZH	WM	OJ	DC	KN	SI	iuu	swz	omo	myj
0	29.	V	IV	II	04	01	25	WJ	VD	PO	MQ	FX	ZR	NE	LG	UC	BK	rui	kao	fqi	rwu

- ➊ „Indikator“ und „Spruchschlüssel“ würfeln (je 3 Zeichen)
- ➋ In der Präambel senden:
 - ➊ Indikator, im Klartext
 - ➋ Spruchschlüssel, verschlüsselt mit Indikator als Startposition (alte Protokollversion: zweimal verschlüsseln und senden)
- ➌ Text senden, verschlüsselt mit Spruchschlüssel als Startposition

Enigma-Funkprotokoll

Geheim!

OKH-Maschinenschlüssel A Nr. 39

Nr. 00014

Nicht ins Flugzeug mitnehmen!

	Datum	Walzenlage			Ringstellung		Steckerverbindungen										Kenngruppen			
0	31.	V	II	IV	17	09 02	KT	AJ	IV	UR	NY	HZ	GD	XF	PB	CQ	sfy	azy	zkq	bqi
0	30.	I	III	V	22	12 10	UE	PL	AY	TB	ZH	WM	OJ	DC	KN	SI	iuy	swz	omo	myj
0	29.	V	IV	II	04	01 25	WJ	VD	PO	MQ	FX	ZR	NE	LG	UC	BK	rui	kao	fqi	rwu

Beispielfunkspruch

fo0
de
b4r
1300
2tle
1tl
250
ysf
tla
zil

Empfänger Sender Uhrzeit 2 Teile 1. Teil Länge Indikator(Nonce) Kenngruppe Spruchschlüssel

tnzsz fepzr dbtee sxapi zejwj cdpir lqoge... ← Ciphertext

Frühere Angriffe

Erste Version Indikator war im Tagesschlüssel vorgegeben. *Alle* Sprüchschlüssel wurden mit dem gleichen Keystream verschlüsselt.

Zweite Version Spruchschlüssel wurde zweimal hintereinander verschlüsselt, also war der Anfang immer $x_1x_2x_3x_1x_2x_3$.

Beide Verfahren wurden schnell von polnischen Kryptoanalysten gebrochen und an England weitergegeben.

Frühere Angriffe

Erste Version Indikator war im Tagesschlüssel vorgegeben. *Alle* Spruchschlüssel wurden mit dem gleichen Keystream verschlüsselt.

Zweite Version Spruchschlüssel wurde zweimal hintereinander verschlüsselt, also war der Anfang immer $x_1x_2x_3x_1x_2x_3$.

Beide Verfahren wurden schnell von polnischen Kryptoanalysten gebrochen und an England weitergegeben.

Änderung 1940 Spruchschlüssel wird nur noch einmal gesendet. Das hat alles kaputtgemacht.

Und jetzt?

Wie es (1940) *nicht* funktioniert:

Eine Enigma-Nachricht bekommen und bitteschön sofort entschlüsseln. (heute machbar)

Stattdessen:

- Tausende Nachrichten täglich
- An die 10 Schlüsselnetze
- Eine Nachricht pro Netz brechen

Aufgabe: einen unvorsichtigen Funker finden
→ **Trafficanalyse!**

Also dann, Trafficanalyse

Ziel: Known Plaintext für den Angriff per Turingbombe

Absender identifizieren

- Peilung, „fist“
- Rufzeichen (ändert sich ab und zu)
- Wer spricht mit wem?

Eigenarten bekannter Stationen ausnutzen

Nachricht identifizieren

- Länge (kurz = stereotyp)
- Zeit (fester Zeitpunkt = feste Nachricht)
- „Gardening“

Known Plaintext

- Zahlen müssen ausgeschrieben werden: „17.03.2013, 13:06“
einssiebenmrzzwonuleinsdreixdreieinsnulseqsuhr
- Eigennamen werden verdoppelt
xbletchleyparkxbletchleyparkx
- Ein Schiff liegt vor Helgoland, nichts ist los, Nachricht um Punkt 13:00
- Abgelegener Posten irgendwo JWD in der Sahara
- Echt deutsche Soldaten...

Known Plaintext

- Zahlen müssen ausgeschrieben werden: „17.03.2013, 13:06“
einssiebenmrzzwonuleinsdreixdreieinsnulseqsuhr
- Eigennamen werden verdoppelt
xbletchleyparkxbletchleyparkx
- Ein Schiff liegt vor Helgoland, nichts ist los, Nachricht um Punkt 13:00
wetterberichtdeutschebuchtdreieinsnulnuluhr
- Abgelegener Posten irgendwo JWD in der Sahara
- Echt deutsche Soldaten...

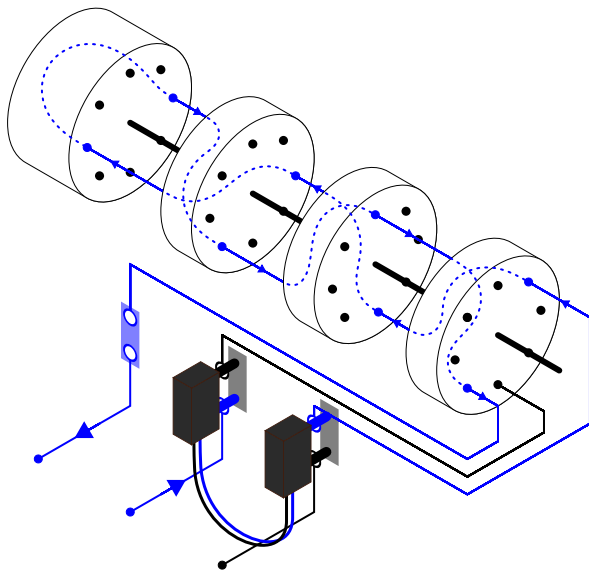
Known Plaintext

- Zahlen müssen ausgeschrieben werden: „17.03.2013, 13:06“
einssiebenmrzzwonuleinsdreixdreieinsnulseqsuhr
- Eigennamen werden verdoppelt
xbletchleyparkxbletchleyparkx
- Ein Schiff liegt vor Helgoland, nichts ist los, Nachricht um Punkt 13:00
wetterberichtdeutschebuchtdreieinsnulnuluhr
- Abgelegener Posten irgendwo JWD in der Sahara
keinebesonderenereignisse (*Jeden einzelnen Tag!*)
- Echt deutsche Soldaten...

Known Plaintext

- Zahlen müssen ausgeschrieben werden: „17.03.2013, 13:06“
einssiebenmrzzwonuleinsdreixdreieinsnulseqsuhr
- Eigennamen werden verdoppelt
xbletchleyparkxbletchleyparkx
- Ein Schiff liegt vor Helgoland, nichts ist los, Nachricht um Punkt 13:00
wetterberichtdeutschebuchtdreieinsnulnuluhr
- Abgelegener Posten irgendwo JWD in der Sahara
keinebesonderenereignisse (*Jeden einzelnen Tag!*)
- Echt deutsche Soldaten... benutzen natürlich vollständige Titel
reichsmarschallhermannngoering

Nochmal Enigma von innen



Kryptoanalyse

- Kein Buchstabe kann zu sich selbst verschlüsselt werden
→ mögliche Plaintext-Positionen finden

tnzszfepzrdbteesxapizejwjcdpirloqogearjppjooahjvothwggqbvhfjfqfmlmw
oberstleutnantmueller

oberstleutnantmueller

oberstleutnantmueller

oberstleutnantmueller

oberstleutnantmueller

oberstleutnantmueller

oberstleutnantmueller

oberstleutnantmueller

oberstleutnantmueller

oberstleutnantmueller

oberstleutnantmueller

oberstleutnantmueller

oberstleutnantmueller

oberstleutnantmueller

oberstleutnantmueller

oberstleutnantmueller

oberstleutnantmueller

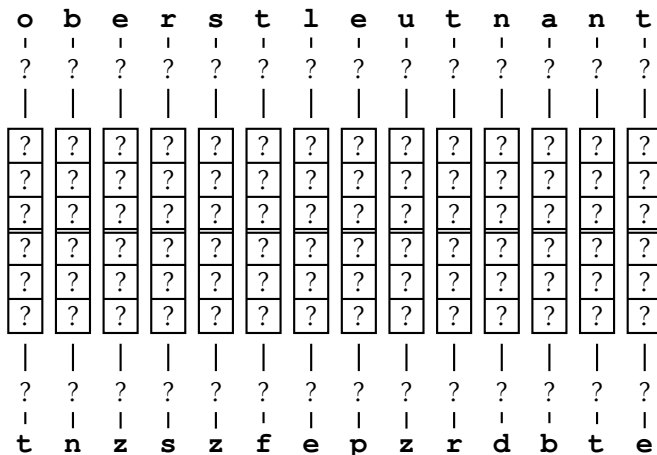
oberstleutnantmueller

- Kein Buchstabe kann zu sich selbst verschlüsselt werden
→ mögliche Plaintext-Positionen finden
- nur 1 054 560 Walzenpositionen
→ war auch 1940 bruteforcebar

- Kein Buchstabe kann zu sich selbst verschlüsselt werden
→ mögliche Plaintext-Positionen finden
- nur 1 054 560 Walzenpositionen
→ war auch 1940 bruteforcebar
- Ringstellung hat nur alle 26 Positionen Einfluss
Dazwischen: linke und mittlere Walze statisch

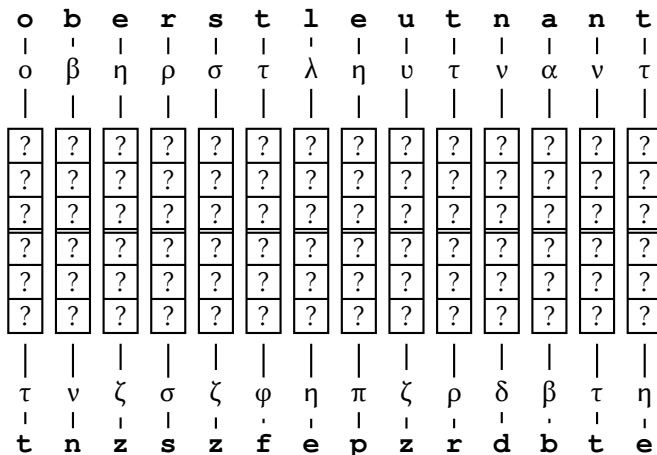
- Kein Buchstabe kann zu sich selbst verschlüsselt werden
→ mögliche Plaintext-Positionen finden
- nur 1 054 560 Walzenpositionen
→ war auch 1940 bruteforcebar
- Ringstellung hat nur alle 26 Positionen Einfluss
Dazwischen: linke und mittlere Walze statisch
- Steckerverbindungen sind statisch
→ das wird die Turingbombe ausnutzen

Die Idee hinter der Bombe



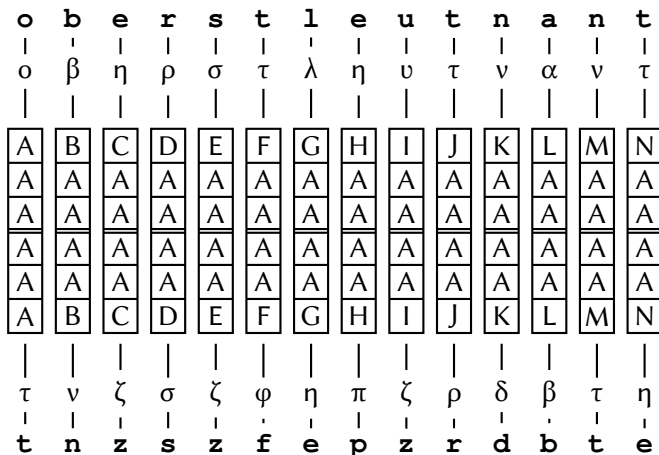
Sieht erstmal aussichtslos aus...

Die Idee hinter der Bombe



Gleiche Buchstaben, gleiche Stecker

Die Idee hinter der Bombe



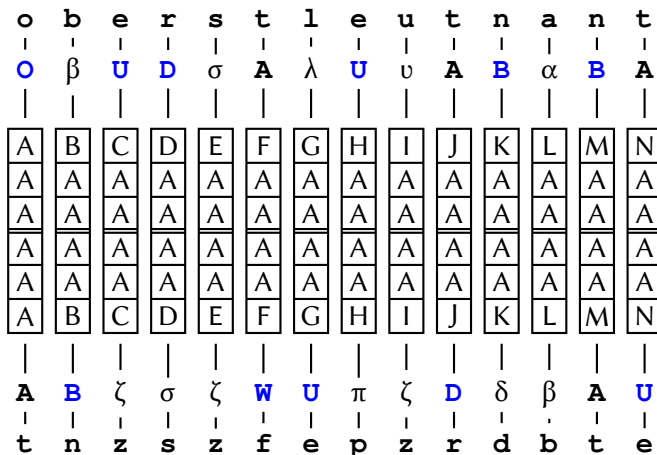
Walzenpositionen per Brute-Force \Rightarrow Erstmal vorne anfangen

Die Idee hinter der Bombe

[illegible]

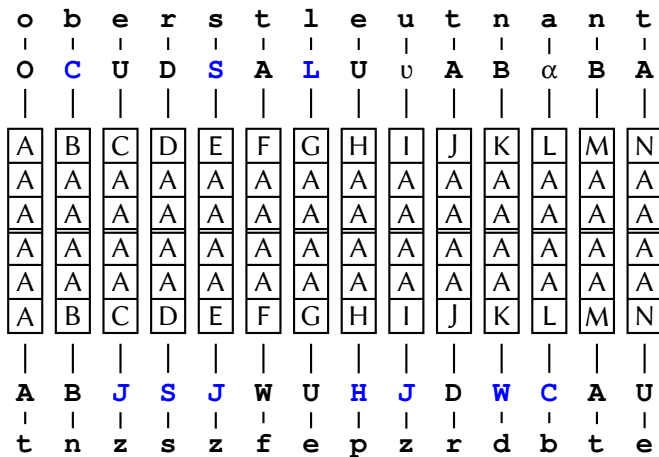
Mal angenommen, $\mathbf{t} \mapsto \mathbf{A} \dots$

Die Idee hinter der Bombe



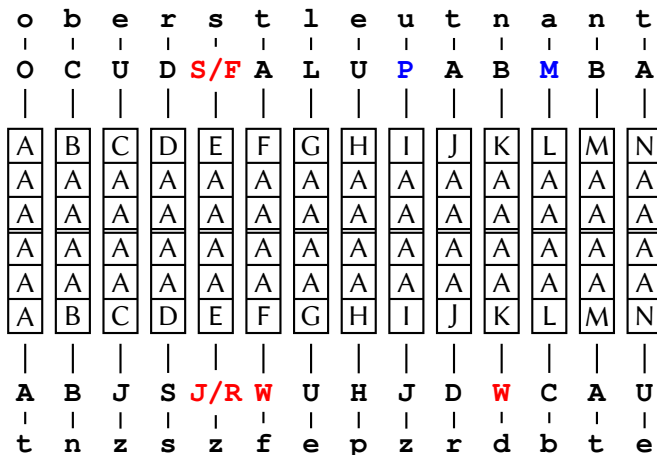
...daraus folgt...

Die Idee hinter der Bombe



...und daraus wiederum folgt...

Die Idee hinter der Bombe



...ein Widerspruch!

Was bringt uns das?

- $\mathbf{t} \mapsto \mathbf{A}$ war falsch
- $\mathbf{s} \mapsto \mathbf{S}$ war falsch
- $\mathbf{s} \mapsto \mathbf{F}$ war auch falsch

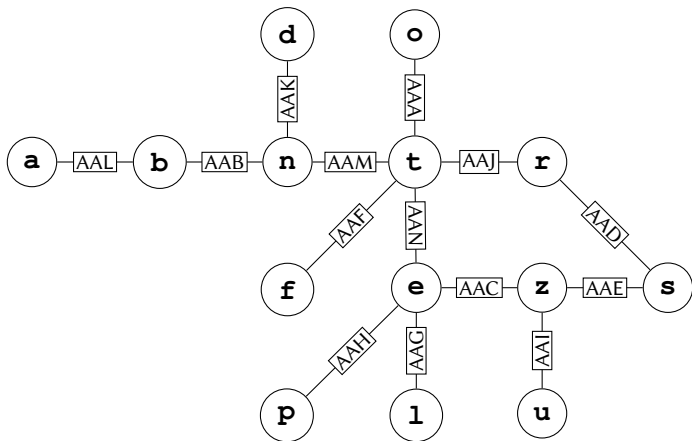
Widerspruch weiter verfolgen \Rightarrow mehr Steckerkombinationen ausschließen

Entweder, wir schließen für einen Buchstaben alle Stecker aus, dann ist die Walzenposition falsch.

Oder nicht. Das müssen wir uns genauer ansehen.

Warum hat das funktioniert?

Dieser Graph (das „Menü“) hat einen Zyklus



Errata

Hier war gerade die Eigenschaft wichtig, dass Verschlüsseln und Entschlüsseln das Gleiche sind: So müssen wir den Verbindungen im Menü keine Richtung zuweisen, womit wir doppelt so viele Knoten hätten (jeden Buchstaben einmal in Klartext und einmal im Ciphertext) und deswegen unser Menü bei gleich vielen Verbindungen wesentlich unschöner aussähe.

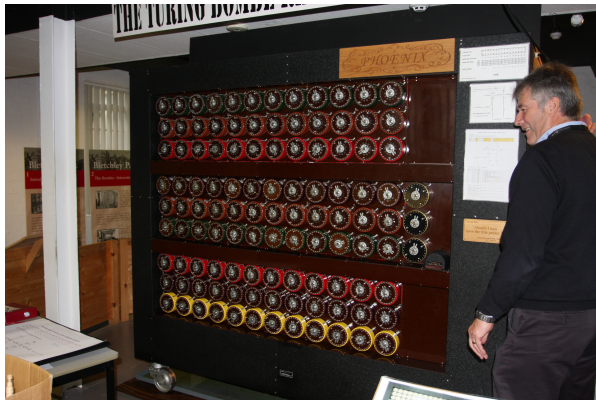
kurz zusammengefasst

```
procedure BOMBE( $p_0 \dots p_{n-1} : [\text{Char}]$ ,  $c_0 \dots c_{n-1} : [\text{Char}]$ )  
  for each  $wheels \in$  wheel orders,  $pos \in [\mathbf{AAA} \dots \mathbf{ZZZ}]$  do  
     $stecker : \text{Char} \rightarrow \{\text{Char}\}$   
     $stecker(p_0) \cup= \{\mathbf{'A'}\}$   
    while  $stecker$  changes do  
      for each  $i \in [0 \dots n - 1]$  do  
         $stecker(c_i) \cup= \bigcup_{s \in stecker(p_i)} \text{encrypt}(wheels, s, pos + i)$   
         $stecker(p_i) \cup= \bigcup_{s \in stecker(c_i)} \text{encrypt}(wheels, s, pos + i)$   
      end for  
    end while  
    if  $\forall S \in \text{cod}(stecker) : \#S < \#\text{Char}$  then  
      report( $pos, stecker$ )  
    end if  
  end for  
end procedure
```

Hausaufgabe: Implementieren. Das wars, danke für euer Interesse.

Moooment!

Es ist 1940. Worauf soll dieser Algorithmus laufen?



„Das ist kein Computer...“

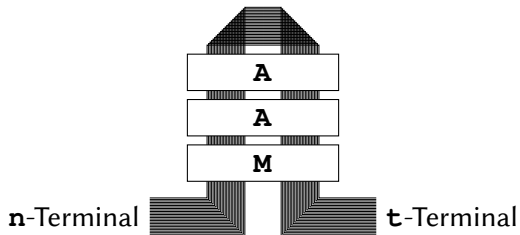
Darauf!

Und wie funktioniert das?

Menü nachbauen:



...wird zu...



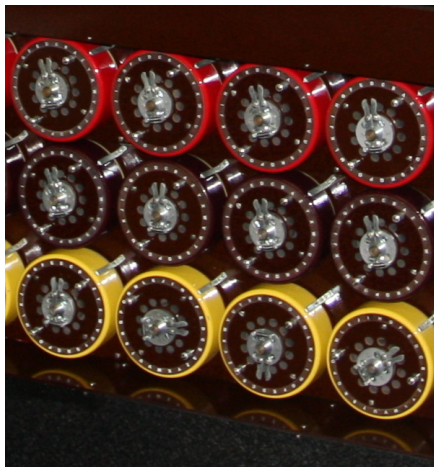
Errata

Hier habe ich mich, glaube ich, in einem fundamentalen Punkt nicht klar ausgedrückt: Die Terminals sind den Buchstaben des Klar- oder Ciphertexts zugeordnet – so weit auch im Vortrag – aber auch die einzelnen Kabel der 26-poligen Verbindungen zwischen ihnen (und durch die Enigma-Walzensätze hindurch) sind einem Buchstaben zugeordnet. Im Betrieb der Bombe bedeutet z. B. ein Signal auf der **x**-Leitung am **y**-Terminal, dass wir gerade annehmen (oder eher versuchen, auszuschließen), dass **x** und **y** miteinander gesteckert sind.

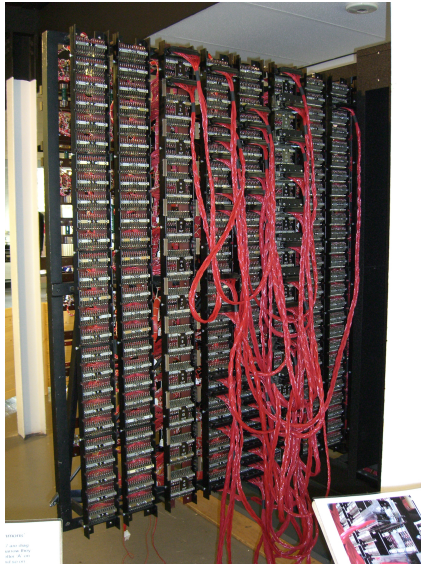
Und jetzt in Hardware



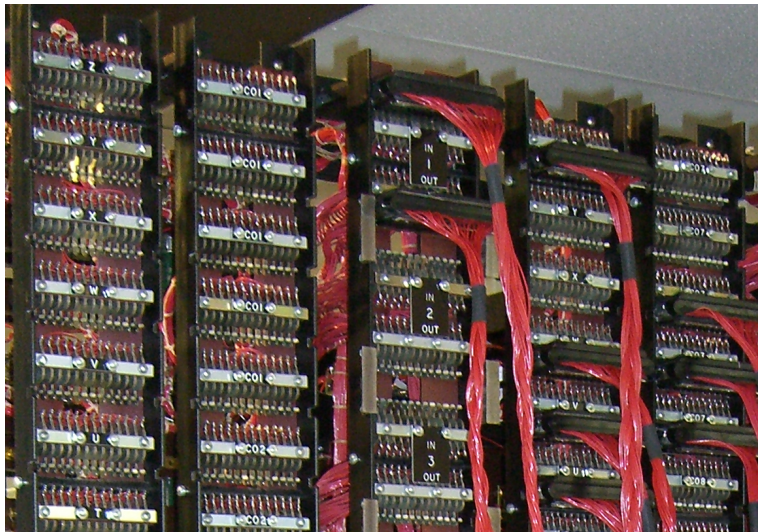
Und jetzt in Hardware



Und jetzt in Hardware



Und jetzt in Hardware



Auftritt Welchman mit Diagonal Board

Tolle Idee: Verbindet doch einfach das **A**-Kabel des **b**-Terminals mit dem **B**-Kabel des **a**-Terminals usw.

Niemand hat das beim ersten Mal verstanden.

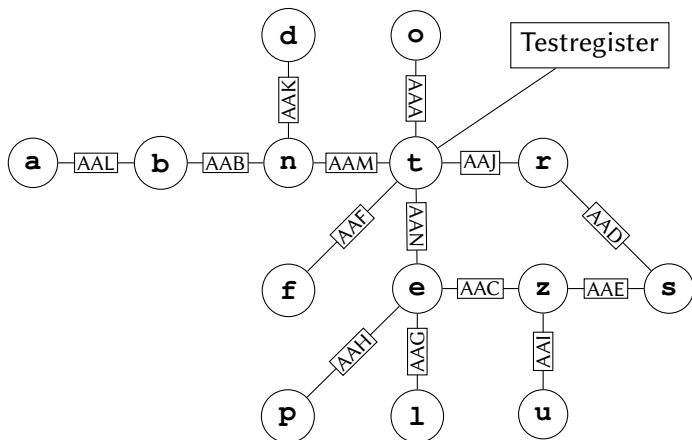
Es hat wunderbar funktioniert.

Los geht's

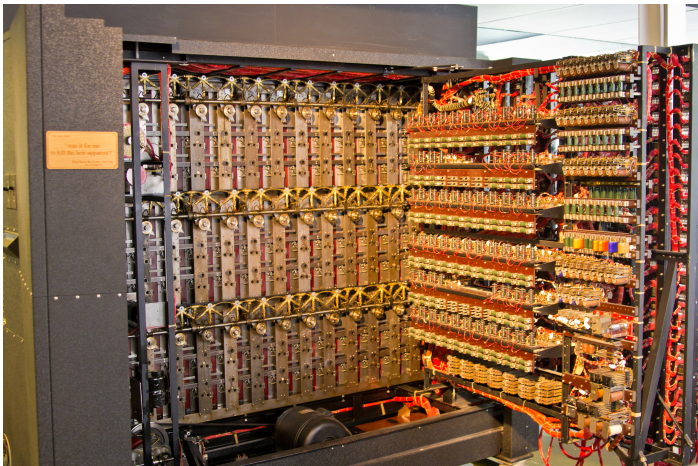
Schlüsselkandidaten erkennen

Für die Hardware müssen wir den Algorithmus vereinfachen:

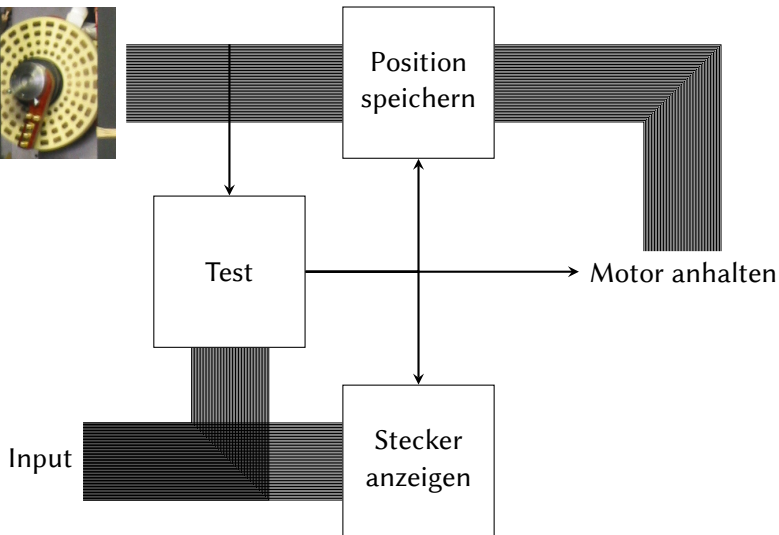
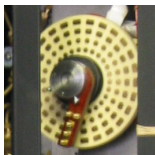
- Nur bei einem Buchstaben prüfen, ob alle Stecker ausgeschlossen werden.



Das Testregister



Das Testregister



Hat das alles etwas gebracht?

Ja! Es war ein Durchbruch

- U-Boot-Krieg
- D-Day

Winston Churchill:

Action this day! Make sure they have all they want on extreme priority and report to me that this has been done.

It was thanks to Ultra that we won the war.

Harry Hinsley:

[Ultra shortened the war] by not less than two years and probably by four years

Bildnachweis

- Enigma-Maschine (Ausschnitt)** <https://commons.wikimedia.org/wiki/File:EnigmaMachine.jpg>
Karsten Sperling, 2004. Public Domain.
- Zwei Enigma-Walzen** https://en.wikipedia.org/wiki/File:Enigma_rotors_and_spindle_showing_contacts_ratchet_and_notch.jpg
Ted Coles, 2011. Public Domain.
- Enigma-Schlüsselblatt (Ausschnitt)** <http://www.google.com/culturalinstitute/asset-viewer/enigma-setting-sheet/EAGejYOkpCao8Q?exhibitId=wRANFg9s&hl=en-GB>
UK Crown Copyright.
- Enigma-Schlüsselblatt (Ausschnitt)** <http://www.google.com/culturalinstitute/asset-viewer/enigma-setting-sheet/EAGejYOkpCao8Q?exhibitId=wRANFg9s&hl=en-GB>
UK Crown Copyright.
- Turingbombe von vorne** <https://www.flickr.com/photos/gerald-davison/10318978385>
Gerald Davison, 2013. CC-BY-NC.
- Turingbombe von vorne (Ausschnitt)** <https://www.flickr.com/photos/gerald-davison/10318978385>
Gerald Davison, 2013. CC-BY-NC.
- Trommel einer Turingbombe (von vorne)** <https://www.flickr.com/photos/djking/7755748980/>
Dave King, 2012. CC-BY-NC-SA.
- Turingbombe von vorne (Ausschnitt)** <https://www.flickr.com/photos/gerald-davison/10318978385>
Gerald Davison, 2013. CC-BY-NC.
- Trommel einer Turingbombe (von hinten)** <https://www.flickr.com/photos/djking/7755748980/>
Dave King, 2012. CC-BY-NC-SA.
- „Patchbay“ einer Turingbombe** <https://www.flickr.com/photos/ljw/790782817>
Lawrence Wilkinson, 2007. CC-BY-NC-SA.
- Turingbombe von hinten** https://commons.wikimedia.org/wiki/File:Bletchley_Park_Bombe11.jpg
Antoine Taveneaux, 2012. CC-BY-SA.