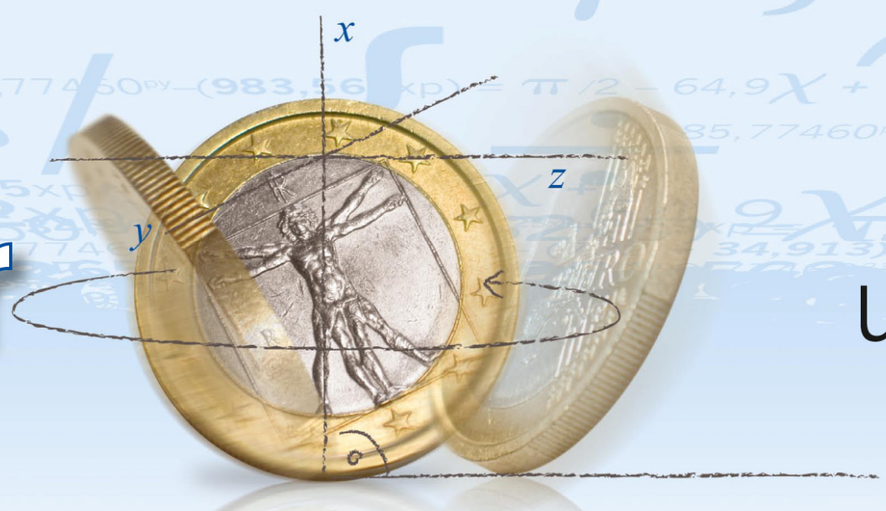
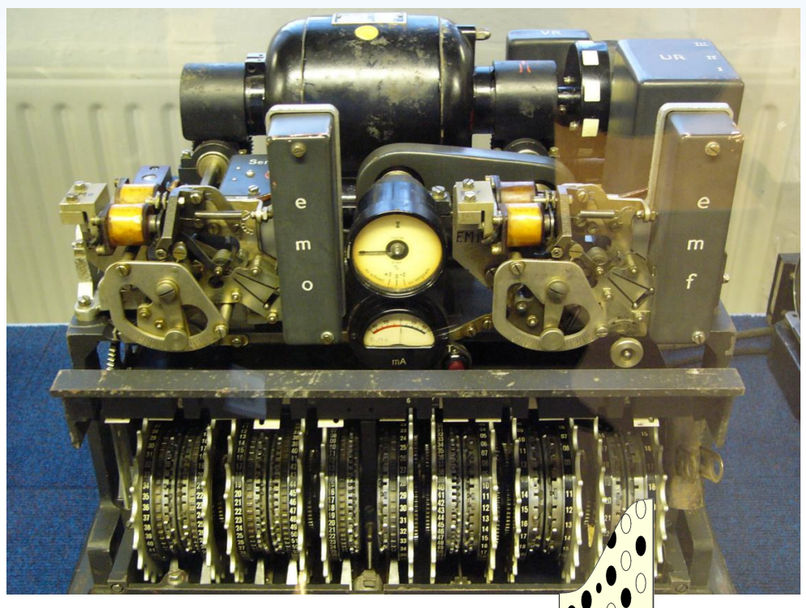
Kopf oder Zahl



universitätbonn

Bonn-Aachen
International Center for
Information Technology

computer Cosec b-it security

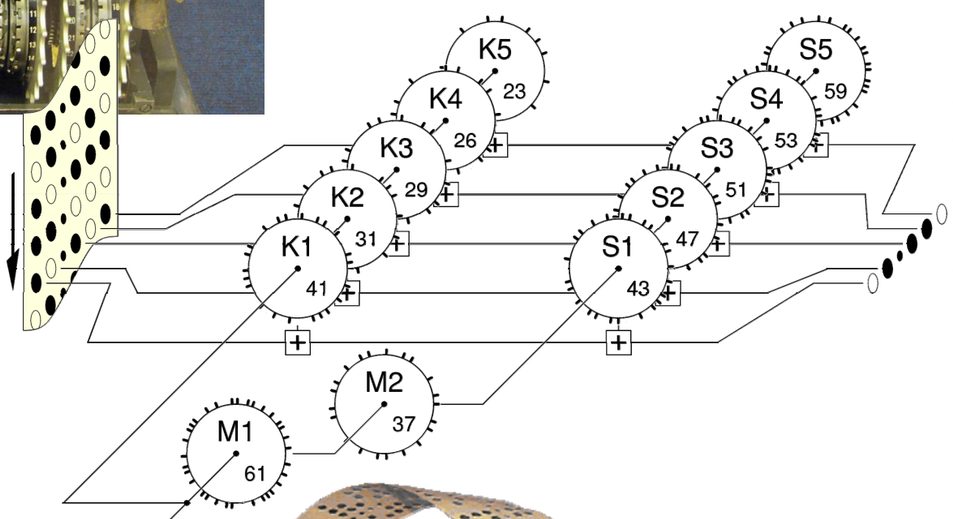


Fernschreibernachrichten werden in Baudot-Code an die SZ-42 übertragen.

Die Deutschen nutzen während des Zweiten Weltkriegs den Lorenz Schlüsselzusatz zur Verschlüsselung des Fernschreibverkehrs in der höheren Führungsebene.

Buchstaben	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Zeilenvorschub	Wagenrücklauf	Buchstaben	Zahlen	Leerzeichen	
Zahlen	-	?	:	WHO ARE YOU	3	%	@	£	8	Bell	(	)	.	,	9	0	1	4	'	5	7	=	2	/	6	+						
1	●	●	○	●	●	●	○	○	○	●	●	○	○	○	○	○	●	○	●	○	●	○	●	●	●	●	○	○	●	●	○	○
2	●	○	●	○	○	○	●	○	●	●	●	●	○	○	○	●	●	●	○	○	●	●	●	○	○	○	○	●	●	●	○	○
3	○	○	●	○	○	●	○	●	●	○	●	○	●	●	○	●	●	○	●	○	●	●	○	●	●	○	○	○	○	●	○	●
4	○	●	●	●	○	●	●	○	○	●	●	○	●	●	●	○	○	●	○	○	○	●	○	●	○	○	●	○	●	●	○	○
5	○	●	○	○	○	○	●	●	○	○	○	●	●	○	●	●	●	○	○	●	○	●	●	○	●	●	●	○	○	○	●	○

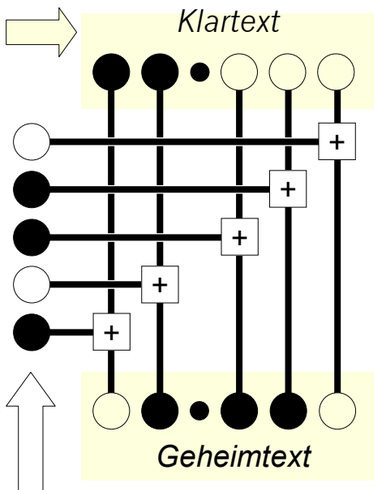
Baudot-Code (Muster aus Löchern an fünf möglichen Stellen)



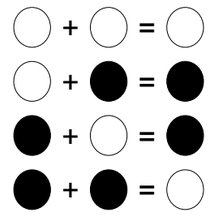
Die SZ-42 hat zwölf Walzen mit unregelmäßig verteilten Stiften. Die Walzen M1 und M2 dienen zur unregelmäßigen Weiterschaltung der Walzen K1 bis K5. Die Walzen S1 bis S5 wird bei jedem Zeichen eine Position weitergedreht. Dadurch wiederholt sich der Schlüsselstrom erst nach mehr als 16 Trillionen Schritten.
Stifte auf den Walzen geben an, ob ein Loch in ein Nicht-Loch verändert werden soll oder nicht. Für jede der fünf Stellen im Baudot-Code eines Buchstabens geschieht das zweimal, einmal durch eine K-Walze und einmal durch eine S-Walze.

Das Prinzip der Verschlüsselung

Der Schlüsselzusatz erzeugt aus einem Tagesschlüssel zunächst einen scheinbar zufälligen Strom von Zeichen. Dieser wird, wie rechts dargestellt, mit dem Klartext verknüpft und ergibt eine verschlüsselte Nachricht. Der Empfänger erhält durch erneute Verknüpfung des Zeichenstroms mit dem Geheimtext wieder den Klartext.



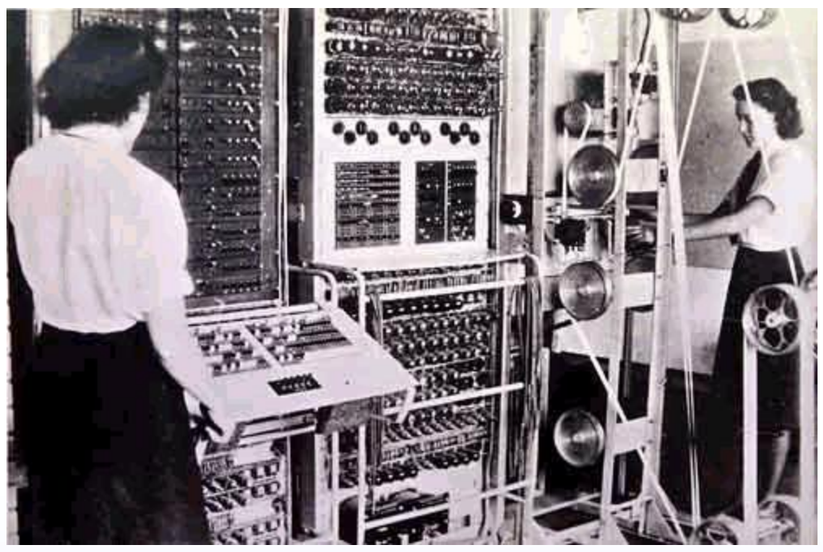
Zeichen aus dem Schlüsselstrom der SZ-42.



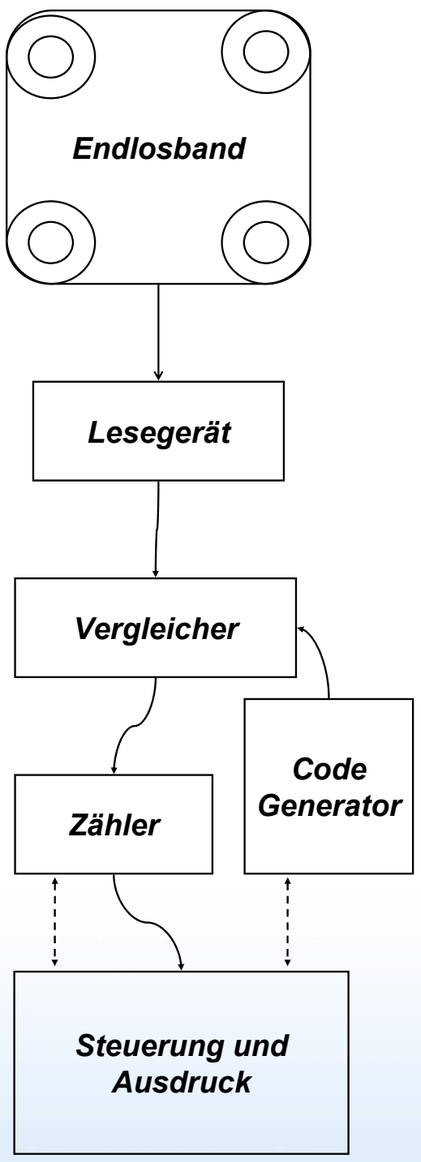
Lorenz SZ-42

Colossus

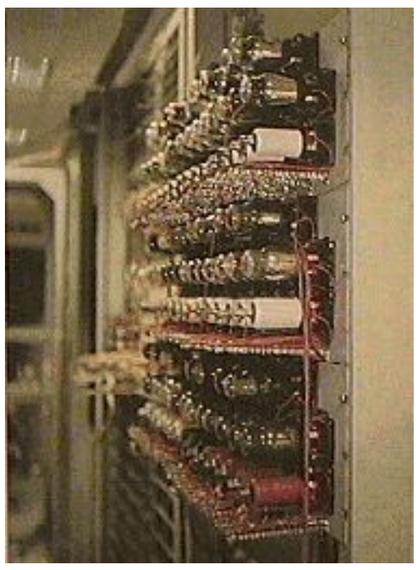
Am 30. August 1941 überträgt ein deutscher Funker eine 4000 Zeichen lange Nachricht mit leichten Änderungen zweimal mit demselben Schlüssel. Daraufhin findet *John Tiltman* in wochenlanger Kleinarbeit den Klartext und den Schlüsselstrom dieser Nachricht. Der Mathematiker *William Thomas Tutte* erschließt daraus den vollständigen Aufbau der SZ-42, ohne sie je gesehen zu haben.
Mit diesem Wissen dauert es 1943 vier Tage, um eine Nachricht von Hand zu entschlüsseln. Bis dahin sind die Meldungen unter Umständen veraltet. Ab Februar 1944 erledigt der Colossus die Entschlüsselung innerhalb weniger Stunden.



15. November 2007, *Cipher-Event*: Funker in aller Welt waren aufgerufen, den Colossus zu schlagen. *Joachim Schüth* in Bonn konnte die Funknachricht aufzeichnen. Nach erfolgreicher Beseitigung von Störungen im Funksignal brach er die Nachricht mit einem modernen Computer innerhalb von zwei Minuten, vier Stunden vor dem Colossus-Nachbau in *Bletchley Park*.

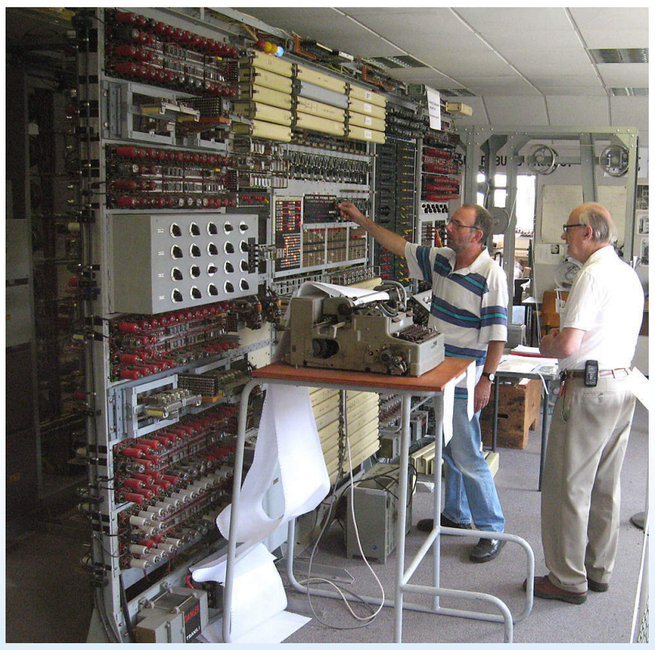


Der Colossus liest die abgefangenen Nachrichten mit 5000 Zeichen in der Sekunde, also mit etwa 50 km/h optisch ein.
Röhren speichern die Statistik für eine probierte Startposition.



Der Vergleicher leitet aus der codierten Nachricht bestimmte Werte ab und sucht in ihr nach statistischen Auffälligkeiten.
Daraus ergeben sich nach und nach mögliche Anfangs-positionen der SZ-42 Walzen.

Gute Startpositionen werden auf einem Drucker ausgegeben.



Andreas Gasper gasper@bonn.edu, Richard Tantius tantius@bonn.edu
Sinan Mece mece@cs.uni-bonn.de, Torsten Schroeder schroeder_torsten@gmx.de
Sieglinde Brunhilde Tschaki tschaki@bit.uni-bonn.de, Jérémie Detrey jdetrey@bit.uni-bonn.de, Michael Nüsken muesken@bit.uni-bonn.de
b-it (Bonn-Aachen International Center for Information Technology)

Mit Unterstützung der Deutsche Telekom Stiftung

In Kooperation mit: :wissenschaftsregion bonn

Deutsches Museum Bonn

Wissenschaftsjahr 2008 Mathematik Alles, was zählt