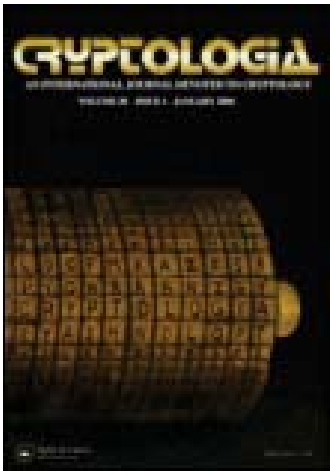


Cryptologia

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ucry20

Konrad Zuse's Proposal for a Cipher Machine

Raul Rojas

Published online: 30 Aug 2014.

To cite this article: Raul Rojas (2014) Konrad Zuse's Proposal for a Cipher Machine, Cryptologia, 38:4, 362-369, DOI: 10.1080/01611194.2014.915265

To link to this article: http://dx.doi.org/10.1080/01611194.2014.915265

Cryptologia, 38:362–369, 2014

ISSN: 0161-1194 print
DOI: 10.1080/01611194.2014.915265

Konrad Zuse's Proposal for a Cipher Machine

RAUL ROJAS

Abstract The German inventor Konrad Zuse wrote a proposal for a cipher machine during the winter of 1939–1940. The document was prepared at the Eastern front during WWII and reached the German military authorities, possibly with the help of Kurt Pannke, a manufacturer of calculating equipment. Zuse's scheme was recently found in his *Nachlass.* It is documented here for the first time. Zuse's offer was rejected by the military, so the software-based cipher machine described in the letter never materialized.

Keywords Konrad Zuse, mechanical computer, Z1

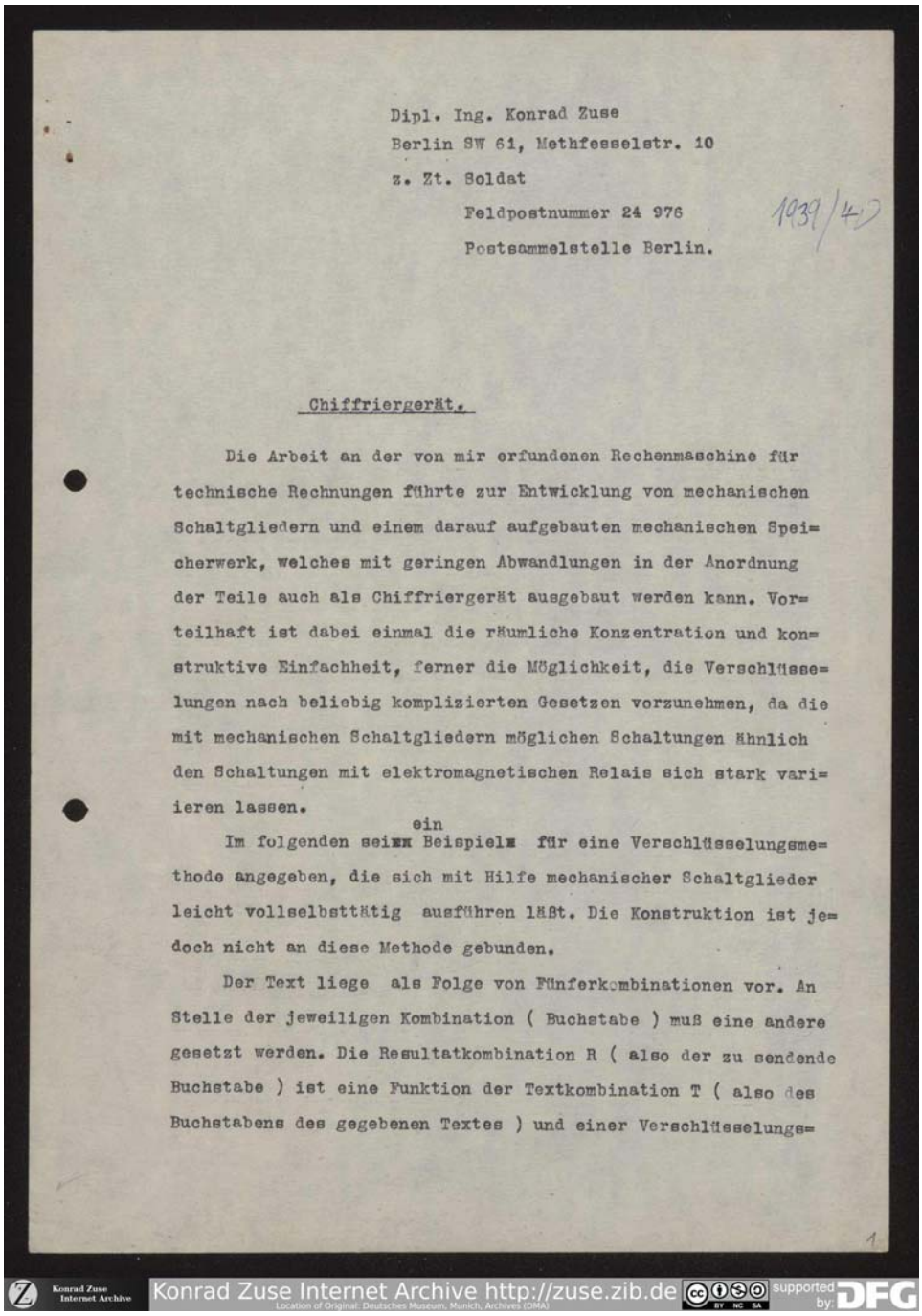
The Context of the Invention

It has been know for years that Konrad Zuse, the German inventor and entrepreneur, designed a cipher machine around 1939–1940 (one page of a handwritten description is reproduced in [6]), but until now no further details have been available. This article provides the first overview of Zuse's idea, the context of the invention, and its eventual rejection by the German military. Konrad Zuse is highly regarded in Germany, since the series of machines he built from 1936 to 1945 were the first programmable calculators (and one could say computers) in Europe.

Konrad Zuse was called to the Eastern front in 1939. He was 29 years old, and WWII proved to be a critical interruption of his work on computer machinery. He had started to tinker with mechanical binary elements as early as 1934, so that in February 1936 he was confident that he could build a complete calculating machine composed of such mechanical components (he later wrote an overview of the elementary circuits used [7]). It was a total departure from orthodoxy, since at the time all calculating machines contained gears and were based on decimal arithmetic (a gear being able to encode the ten necessary decimal digits). He built the Z1, a mechanical programmable calculator, from 1936 to 1938 in his parent's living room. The machine consisted of a mechanical storage for 16 floating-point binary numbers and a floating-point processor capable of adding, subtracting, multiplying, and dividing the arguments contained in two registers [2]. The program was stored on a punched tape. The Z1 was, in fact, one of the first computers in the world, although it was not reliable enough. Therefore, Zuse discarded the mechanical components in 1940 and built a relay computer in 1941 (the so-called Z3) [3].

Address correspondence to Raul Rojas, Freie Universität Berlin, CS, Arnimallee 7, Berlin 14195, Germany. E-mail: rojas@inf.fu-berlin.de

Color versions of one or more of the figures in the article can be found online at www.tandfonline.com/ucry.



Dipl. Ing. Konrad Zuse
Berlin SW 61, Methfesselstr. 10
z. Zt. Soldat
Feldpostnummer 24 976
Postsammelstelle Berlin.

1939/41

Chiffriergerät.

Die Arbeit an der von mir erfundenen Rechenmaschine für technische Rechnungen führte zur Entwicklung von mechanischen Schaltgliedern und einem darauf aufgebauten mechanischen Speicherwerk, welches mit geringen Abwandlungen in der Anordnung der Teile auch als Chiffriergerät ausgebaut werden kann. Vorteilhaft ist dabei einmal die räumliche Konzentration und konstruktive Einfachheit, ferner die Möglichkeit, die Verschlüsselungen nach beliebig komplizierten Gesetzen vorzunehmen, da die mit mechanischen Schaltgliedern möglichen Schaltungen ähnlich den Schaltungen mit elektromagnetischen Relais sich stark variieren lassen.

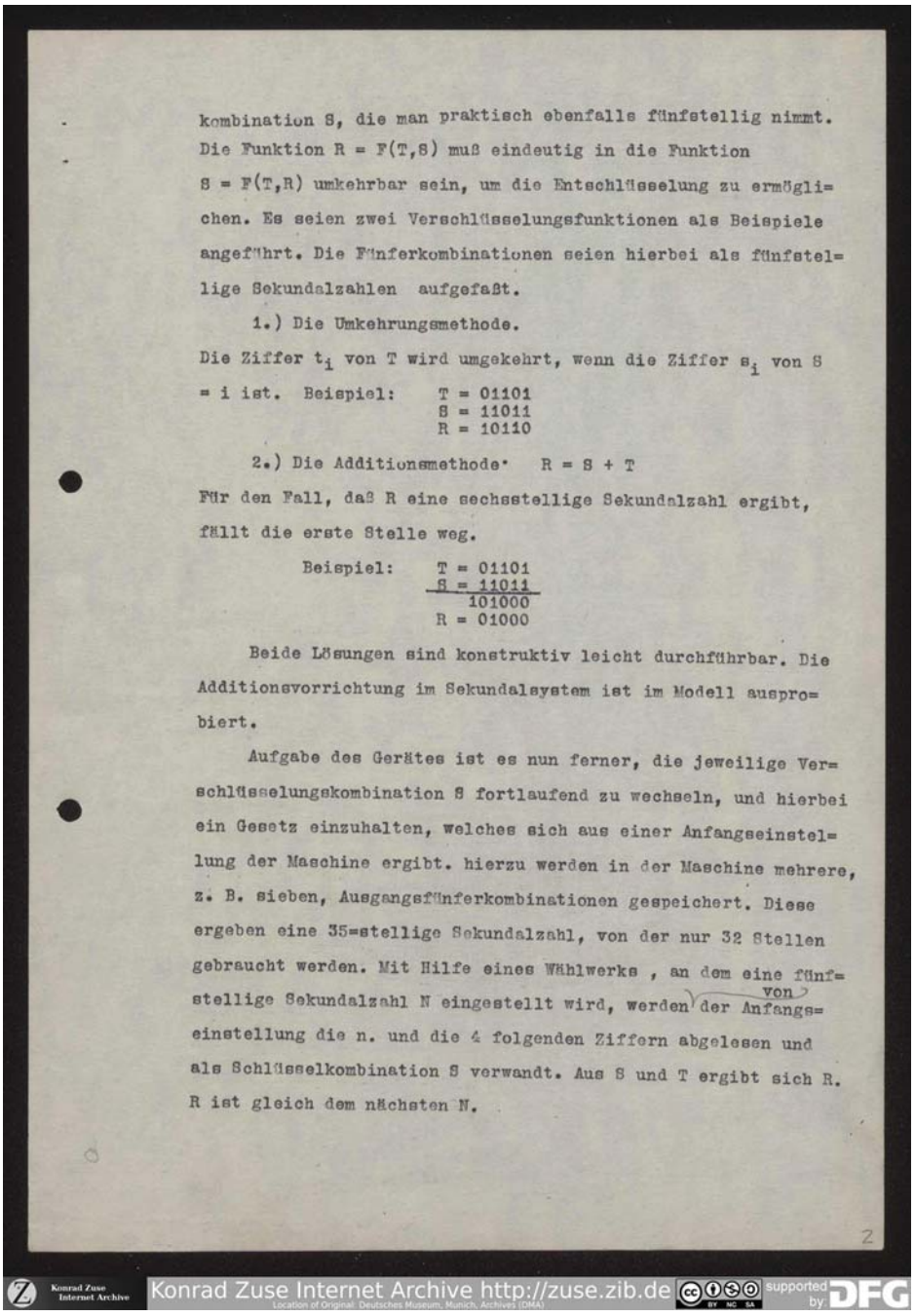
Im folgenden sein ein Beispiel für eine Verschlüsselungsmethode angegeben, die sich mit Hilfe mechanischer Schaltglieder leicht vollselbsttätig ausführen läßt. Die Konstruktion ist jedoch nicht an diese Methode gebunden.

Der Text liege als Folge von Fünferkombinationen vor. An Stelle der jeweiligen Kombination (Buchstabe) muß eine andere gesetzt werden. Die Resultatkombination R (also der zu sendende Buchstabe) ist eine Funktion der Textkombination T (also des Buchstabens des gegebenen Textes) und einer Verschlüsselungs-

1

Figure 1. Scan of the original of Zuse's letter with his proposal for a cipher machine.

Between the construction of the Z1 and the Z3, he served six months in the military, a setback to his intention of starting an engineering company for marketing his invention (he could later register the company in 1941).



kombination S, die man praktisch ebenfalls fünfstellig nimmt. Die Funktion R = F(T,S) muß eindeutig in die Funktion S = F(T,R) umkehrbar sein, um die Entschlüsselung zu ermöglichen. Es seien zwei Verschlüsselungsfunktionen als Beispiele angeführt. Die Fünferkombinationen seien hierbei als fünfstellige Sekundalzahlen aufgefaßt.

1.) Die Umkehrungsmethode.

Die Ziffer t_i von T wird umgekehrt, wenn die Ziffer s_i von S = i ist. Beispiel:

T = 01101
S = 11011
R = 10110

2.) Die Additionsmethode. R = S + T

Für den Fall, daß R eine sechsstellige Sekundalzahl ergibt, fällt die erste Stelle weg.

Beispiel:

T = 01101
S = 11011
101000
R = 01000

Beide Lösungen sind konstruktiv leicht durchführbar. Die Additionsvorrichtung im Sekundalsystem ist im Modell ausprobiert.

Aufgabe des Gerätes ist es nun ferner, die jeweilige Verschlüsselungskombination S fortlaufend zu wechseln, und hierbei ein Gesetz einzuhalten, welches sich aus einer Anfangseinstellung der Maschine ergibt. hierzu werden in der Maschine mehrere, z. B. sieben, Ausgangsfünferkombinationen gespeichert. Diese ergeben eine 35=stellige Sekundalzahl, von der nur 32 Stellen gebraucht werden. Mit Hilfe eines Wählwerks , an dem eine fünfstellige Sekundalzahl N eingestellt wird, werden von der Anfangseinstellung die n. und die 4 folgenden Ziffern abgelesen und als Schlüsselkombination S verwandt. Aus S und T ergibt sich R. R ist gleich dem nächsten N.

2

Figure 1. Continued.

Zuse was forced to adapt his creation to the needs of the military. He had to "sell" his idea in order to be sent back to Berlin from the front, so he could continue working on his machines. Previously, in 1937, Zuse had made contact with Kurt

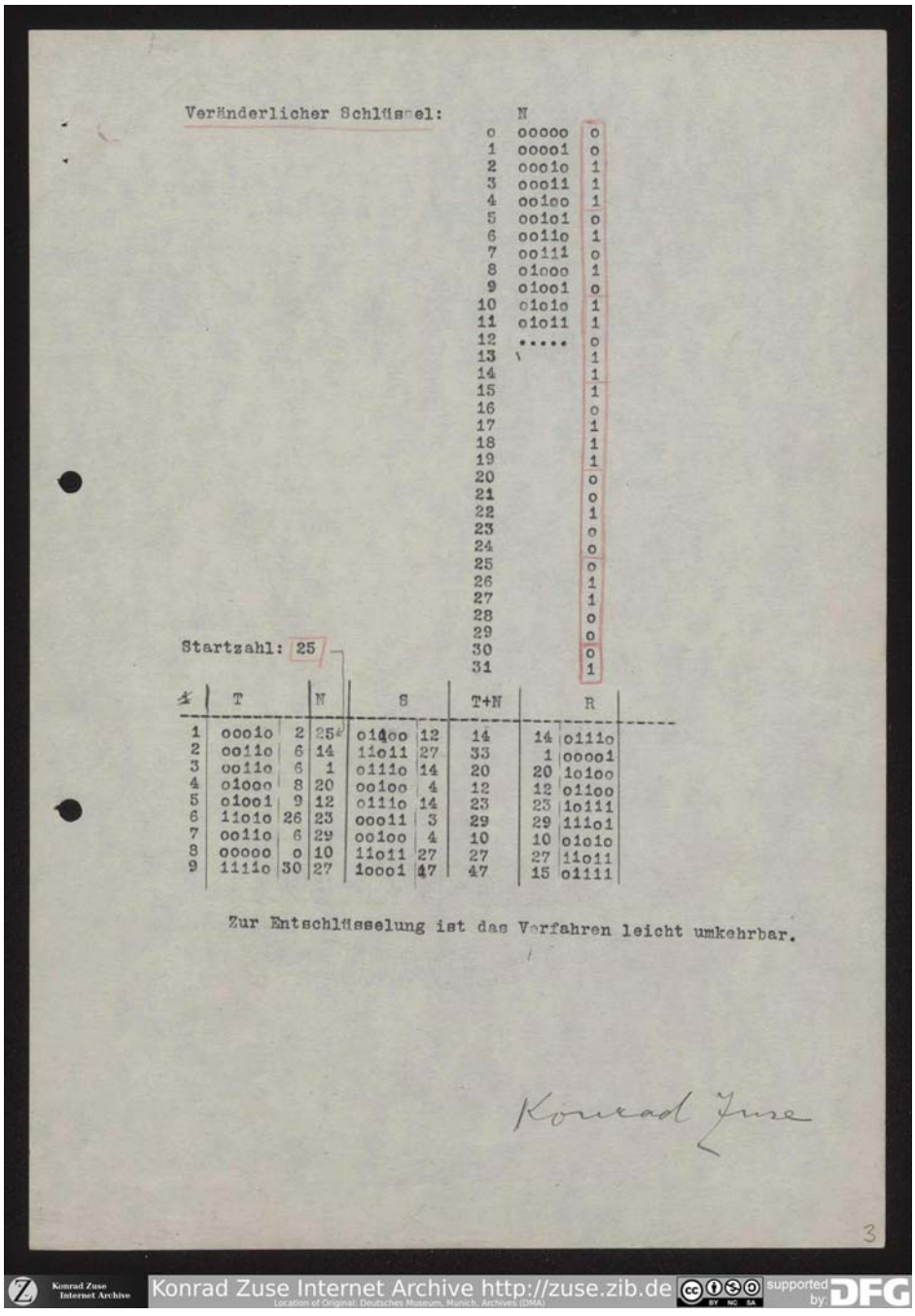


Figure 1. Continued.

Pannke, who marketed calculators in Germany and became interested in the Z1. Pannke partially financed the construction of the machine with 7,000 Reichsmark [6]. Pannke had worked in the past on machines for artillery calculations and even

had a patent for such a device [1]. It was probably Pannke's idea to modify the Z1, so letters were exchanged between him and Zuse, discussing the possible adaptation of the machine to cryptography [5]. The result was the document I present here, in which the young soldier Konrad Zuse proposes the German military to build a binary programmable mechanical device for cryptography [4] (Figure 1). Potentially any encoding algorithm could be implemented in the machine. In the document, Zuse gives an example of one possible encoding, making clear that the machine itself was not constrained by this choice.

As is evident from Zuse's pitch, he was not an expert cryptographer. He might have learned the basics before submitting his letter. It was written at the front (where Zuse was not involved in direct fighting) and was mailed to Berlin. The document reached the authorities. A second proposal, with a more complex recipe for mixing bits, was prepared later by Zuse and was also sent to the authorities. That second "algorithm" is currently being analyzed, and I will report on it elsewhere. It is the handwritten text whose first page was reproduced by Zuse in his autobiography [6]. Nevertheless, the core of Zuse's argument was that the concrete ciphering algorithm is, in principle, just a matter of choice, once a computing machine is available that can carry out any desired encryption and decryption. Random addressing of a chain of random bits was the main new computational feature that Zuse could offer to cryptographers.

Konrad Zuse's Letter

The following is a translation of Konrad Zuse's proposal for a cipher machine [4]. The original of the letter (in German) is kept at *Deutsches Museum* in Munich, being part of the documents provided by Zuse's family to the museum after his death. The letter was typed. We find the date 1939/40 handwritten on the first page (probably by Zuse).

> Dipl. Ing. Konrad Zuse
> Berlin SW 61, Methfesselstr. 10
> Soldier
> Field Postal Number 24 976
> Post Office Berlin
>
> Cipher Machine
>
> My work on the machine I invented for technical computations has led to the development of mechanical switches, and also of a mechanical storage composed of such elements. It is possible to redesign the disposition of the parts so that the machine can be adapted for cryptographic use. The advantage is, firstly, the spatial concentration and the simplicity of the construction, secondly, the cipher can be built using functional laws as complex as desired. This is so, because the circuits can be totally modified with ease, as can be done with circuits made out of relays.
>
> In the following, we illustrate an encoding method that can be executed completely automatically by the mechanical elements. The construction is independent of this specific method.

The text to be encoded consists of a sequence of groups of five binary symbols. Each combination (a letter) must be substituted by another one. The result R (the letter to be sent) is a function of the text T (the letters in the given text), and of an encoding combination S, that we assume to consist of five binary symbols.

The function $R = F(T,S)$ must be invertible in the function $S = F(T,R)$, in order to make decoding possible. Let us consider two encoding functions as examples. The groups of five symbols are binary numbers with five digits each.

(1) The inversion method.

The digit t_i of T is inverted when the digit s_i of S is one.

Example: T = 01101
S = 11011
R = 10110

(2) The addition method $R = S + T$.

In the case that R becomes a binary number of six digits, we suppress the sixth digit.

Example:
$$\begin{array}{rr} T = & 01101 \\ S = & 11011 \\ \hline & 101000 \\ R = & 01000 \end{array}$$

Both solutions are straightforward to implement. The binary adder has been tested in a prototype. The machine can also change the encoding combination S continuously, following certain rules and maintaining the calculation laws determined by the initial configuration. We can store in the machine several, for example seven, initial configurations of five binary digits. They produce a binary number of 35 digits, from which we only need to use 32 positions. Using a decoder, we can select from the binary sequence the n-th and as many binary digits as needed for the key S. From S and T we determine R. R is equal to the next N.

Variable key:

N		
0	00000	0
1	00001	0
2	00010	1
3	00011	1
4	00100	$\underline{1}$
5	00101	$\underline{0}$
6	00110	1
7	00111	0
8	01000	1
9	01001	$\underline{0}$

	10	01010 1
	11	01011 1
	12	... 0
	13	... 1
	14	$\overline{1}$
	15	$\overline{1}$
	16	0
	17	1
	18	1
	19	$\overline{1}$
	20	$\overline{0}$
	21	0
	22	1
	23	0
	24	$\overline{0}$
	25	$\overline{0}$
	26	1
	27	1
	28	0
	29	$\overline{0}$
	30	$\overline{0}$
Start number: 25	31	1

	T	N	S	T+N	R
1	00010 2	25	01000 12	14	14 01110
2	00110 6	14	11011 27	33	1 00001
3	00110 6	1	01110 14	20	20 10100
4	01000 8	20	00100 4	12	12 01100
5	01001 9	12	01110 14	23	23 10111
6	11010 26	23	00011 3	29	29 11101
7	00110 6	29	00100 4	10	10 01010
8	00000 0	10	11011 27	27	27 11011
9	11110 30	27	10001 47	47	15 01110

In order to decode, the process can be inverted easily.

Discussion

There are several interesting aspects in Zuse's proposal. First, he advises to use a purely binary approach. Machines such as the Enigma and later the Lorenz SZ40 were mechanical devices based on rotors and some wiring. They were provided to the users and were black boxes for them. The user could only adjust the start position of the rotors but not completely reprogram the machine. In Zuse's proposal, the pseudorandom stream of binary digits is provided in advance (it can be generated by any means), can be kept in memory, and the "scrambling," that is the selection of the bits needed for a substitution, could be done with any good algorithm. Zuse does not compare his machine to those already known, simply because he was unaware of the cryptographic methods they implemented.

Zuse's method consists of taking 35 random bits and then generating a random pointer to any position between 0 and 31. The five bits starting at the pointer would be taken and used for the encoding (the last position, 31, can use the additional bits at positions 32 to 34). A random pointer to a random position would seem to be a good way of scrambling text. However, the reuse of the random bits would be significant in an encoded text of any useful length, so the cipher could be broken easily.

For the combination of a letter with five random bits, Zuse proposes to use XOR (the "inversion method") or addition. The expressions $R = F(T,S)$ and $S = F(T,R)$ are only valid for the XOR case (since $S = T$ XOR (T XOR S)). For the addition case, a subtraction would be needed to recover S.

For recovering the plain text from the cipher, the key and the starting position are needed. Given S and R, T can be recovered for the first line of the table in Zuse's letter. R provides the next pointer into the key, for recovering five bits of the key and for proceeding to the next line of decoding.

Zuse's letter has only a historical value today. It shows that very early during the development of the computer, he was aware of the full range of applications that a fast calculating machine could have.

Although his bid was rejected, Zuse was well connected within the military-technical complex, so he could arrange for a discharge for working on computing corrections to the shape of flying bombs at the Henschel Flugzeugwerke in Berlin. He returned to that city in March 1940, continued working on his computers until 1945, and never again returned to the subject of cryptography.

About the Author

Raul Rojas is a Professor of Computer Science at Freie Universitaet Berlin, Germany. He is the Director of the Konrad Zuse Internet Archive.

References

1. Pannke, K. "Rechenvorrichtung," German Patent DE 447780, 5.8.1927.
2. Rojas, R. 1997. Konrad Zuse's Legacy: The Architecture of the Z1 and Z3, *Annals of the History of Computing*, 19(2): 5–16.
3. Rojas, R. (Ed.). 1998. *Die Rechenmaschinen von Konrad Zuse*, Berlin: Springer-Verlag.
4. Zuse, K. 1939/40. "Chiffriermaschine", Zuse Archive at Deutsches Museum, Germany: Munich. Images 202_4–01, 202_4–02, 202_4–03.
5. Zuse, K. Draft of a letter to Kurt Pannke, Zuse Archive at Deutsches Museum, Germany: Munich.
6. Zuse, K. 1993. *The Computer: My Life*. Berlin: Springer-Verlag.
7. Zuse, K. Undated. "Rechenvorrichtung aus mechanischen Schaltglieder," Zuse Papers, GMD 019/003. http://zuse.zib.de/ (accesssed July 21, 2013).