ZEIT PUNKT

Enigma. Der Wettlauf zwischen Ver- und Entschlüsseln

Von der deutschen Chiffriermaschine zum digitalen Computer – von Dominik Landwehr

Am Vorabend des Zweiten Weltkrieges fehlte der Schweiz vieles, was zur Verteidigung unseres kleinen Landes nötig war. Damit sind nicht nur moderne Waffen, Flugzeuge oder Panzer gemeint – auch im Bereich der Nachrichtentechnik gab es schmerzhafte Lücken. Etwa bei der Lehre der Verschlüsselung – der Kryptografie. «Man hatte dieses Gebiet nach dem Ersten Weltkrieg einschlafen lassen», erinnert sich der heute 84-jährige Paul Glur, den wir in seinem Haus im Berner Liebefeldquartier besuchen. Glur war Student der Mathematik beim Berner Mathematik-Professor Hugo Hadwiger. Sachverständige für Kryptografie gab es damals nicht viele, und so erstaunt es nicht, dass der junge Paul Glur seinen Aktivdienst bei den Kryptografie-Spezialisten leistete.

Mutter der Chiffriergeräte

Verschlüsselung war damals Handarbeit, und Glur war mit den gängigen Methoden bestens vertraut. Aber damit war kein Staat zu machen. Die Kunde, dass Deutschland ein automatisches Verschlüsselungsgerät namens Enigma (griechisch für «Rätsel») entwickelt hatte, erreichte auch die Schweiz. Bald war klar: Diese Maschine könnte der sicheren Übermittlung von heiklen Nachrichten dienlich sein. «Die ersten Maschinen wurden 1938 als Beigabe mit 14 schweren Funkstationen geliefert», erzählt uns Rudolf J.Ritter, der sich seit Jahren mit der Geschichte des Übermittlungsmaterials in der Schweizer Armee befasst. 1942 gab es in der Schweiz total 256 Enigma-Chiffriergeräte.

Und so funktionierte die Enigma: Eine Walze mit drei verschiedenen, austauschbaren Rotoren besorgte die Codierung, und zwar so, dass jeder Buchstabe nach einem anderen Schlüssel chiffriert wurde. Der ganze Mechanismus beanspruchte kaum mehr Platz als eine Reiseschreibmaschine und konnte auch unter widrigen Umständen im Feld einfach bedient werden.

Vorarbeit für Computer

Deutschland vertraute der Sicherheit der Enigma und rechnete nicht mit der Entschlossenheit der Briten. Nachdem polnische Spezialisten wichtige Hinweise geliefert hatten, entschlüsselten die Briten das Verfahren dank einer in einem deutschen U-Boot erbeuteten Enigma – allerdings mit einem beispiellosen Aufwand. Der in diesem Frühjahr angelaufene Kinofilm «Enigma» vollzieht die abenteuerliche Geschichte um den genialen Entzifferer Alan M. Turing nach.

Der Mathematiker hatte 1936 eine Rechenmaschine erfunden, die für alle «computable numbers» – alle rechenbaren Zahlen – taugte. Unter strengsten Sicherheitsvorkehrungen wurde nach Turings Anleitung auf einem Landgut namens Bletchley Park eine Abteilung mit einer riesigen Decodiermaschine und rund 10 000 Mitarbeitern aufgebaut. Das Team dechiffrierte nicht nur die Funksprüche der deutschen U-Boote und schützte so die alliierten Geleitzüge. In Bletchley Park wurde auch ein wichtiges Kapitel in der Geschichte jener Maschine geschrieben, die später Computer hiess.

In einem deutschen U-Boot erbeuteten die Briten im Zweiten Weltkrieg eine Enigma. Dass sie die Chiffriermaschine entschlüsselten, bedeutete nicht nur eine Kriegswende, sondern auch einen Schritt in die Kryptografie – die Computercodierung.

Die Urform aller Codes, ohne die eine Chiffriermaschine und später ein Computer gar nicht funktionieren konnten, wurde aber schon viel früher entdeckt. Um 1675 entwickelte der deutsche Mathematiker Gottfried Wilhelm Leibniz das binäre Zahlensystem. In ihm lässt sich jede beliebige Zahl mit den beiden Ziffern 0 und 1 ausdrücken. Diese beiden Werte liessen sich technisch leicht umsetzen – etwa als Loch/nicht Loch bei Lochkarten, als Strom/nicht Strom bei Rechnungsmaschinen oder Impuls/kein Impuls bei Computern. Heute nennt man diese Übersetzung in den 0-1-Code Digitalisierung.

Ausgehorchte Schweizer

Auch die Schweizer Enigma wurde geknackt – und zwar von allen Kriegsparteien. Das lässt sich heute anhand von britischen Dokumenten nachvollziehen. Sie beweisen die intimen Kenntnisse der britischen Chiffrierspezialisten: «The Swiss have no spare wheels for the machine which thus has only six possible wheel orders» (Die Schweizer besitzen keine zusätzlichen Rotoren, also gibt es nur sechs mögliche Stellungen). Dass auch Nazi-Deutschland die Schweizer Enigma-Botschaften lesen konnte, erstaunt nicht weiter. Einen Beweis dafür liefert ein Papier, das ein ehemaliger Mitarbeiter der deutschen Abwehr 1948 dem Schweizer Nachrichtendienst übergab.

Die Chiffriermaschine Enigma hatte ganz offensichtlich auch ihre Schwächen – etwa die bemerkenswerte Tatsache, dass ein Buchstabe bei der Verschlüsselung nie in sich selber übergehen konnte. Aus A wurde also niemals wieder A. Die Schwächen blieben auch der Schweiz nicht verborgen, und so entschied man 1942 – als die deutschen Lieferungen an die Schweiz ins Stocken geraten waren –, die Konstruktion einer eigenen Maschine an die Hand zu nehmen. Sie erhielt den Namen Nema – eine Abkürzung für den Begriff «Neue Maschine». Für die Entwicklung und den Bau dieser Maschine war die Firma Zellweger in Uster verantwortlich. «Unsere Arbeit vollzog sich unter den grössten Sicherheitsvorkehrungen», erinnert sich heute der Konstrukteur der Nema. «Ein Mitarbeiter des Schweizer Nachrichtendienstes verfolgte jeden meiner Schritte, sobald ich jeweils das Firmengelände verliess.» Mehr noch: Bis 1947 war dem Ingenieur verboten zu heiraten. Nach dem Krieg wurde in der Schweiz eine Vielzahl von Chiffriermaschinen hergestellt.

Schlüssel zum Decodieren

Die traditionellen Maschinen und ihre Chiffriermethoden mögen noch so unterschiedlich sein – in einem entscheidenden Punkt funktionieren sie alle gleich: Sender und Empfänger müssen im Besitz eines Schlüssels sein. Mit diesem Schlüssel codiert der Sender seine Botschaft, und mit dem gleichen Schlüssel kann der Empfänger die Botschaft decodieren.

Die einfachste Verschlüsselungsmethode ist die sogenannte Cäsar-Verschlüsselung: Dabei werden die Buchstaben im Alphabet zyklisch vertauscht – der Schlüssel verrät Sender und Empfänger, wo das Code-Alphabet jeweils beginnt. Weil Sender und Empfänger denselben Schlüssel benutzen, spricht man auch von der symmetrischen Methode.

Diese Methode funktioniert gut in überschaubaren Situationen. Schwieriger wird es aber, wenn eine Gruppe von Personen untereinander Botschaften tauschen will – nun braucht es für jede mögliche Kombination einen eigenen Schlüssel. Bei grossen Gruppen wird dies zur Herausforderung, und zwar aus rein mathematischen Gründen: Die Anzahl der Schlüssel steigt nämlich nicht linear, sondern quadratisch zur Anzahl der Teilnehmer.

Jedem sein Schlüssel

Neben dem symmetrischen gibt es ein asymmetrisches Verfahren, das erst in den 80er-Jahren erfunden wurde. Asymmetrisch heisst es, weil Sender und Empfänger nie mehr einen Schlüssel auszutauschen brauchen. Der Sender verschlüsselt seine Botschaft mit einem ersten Schlüssel, der dem Empfänger gehört. Dieser Schlüssel ist – und hier liegt das Paradoxe und gleichzeitig Geniale bei diesem Verfahren – öffentlich zugänglich und wird heute beispielsweise im Internet publiziert. Der Empfänger ist im Besitz eines zweiten Schlüssels, den er nie aus der Hand gibt und den also auch niemand kennen kann. Mit diesem Schlüssel entziffert er nun die für ihn bestimmte Botschaft.

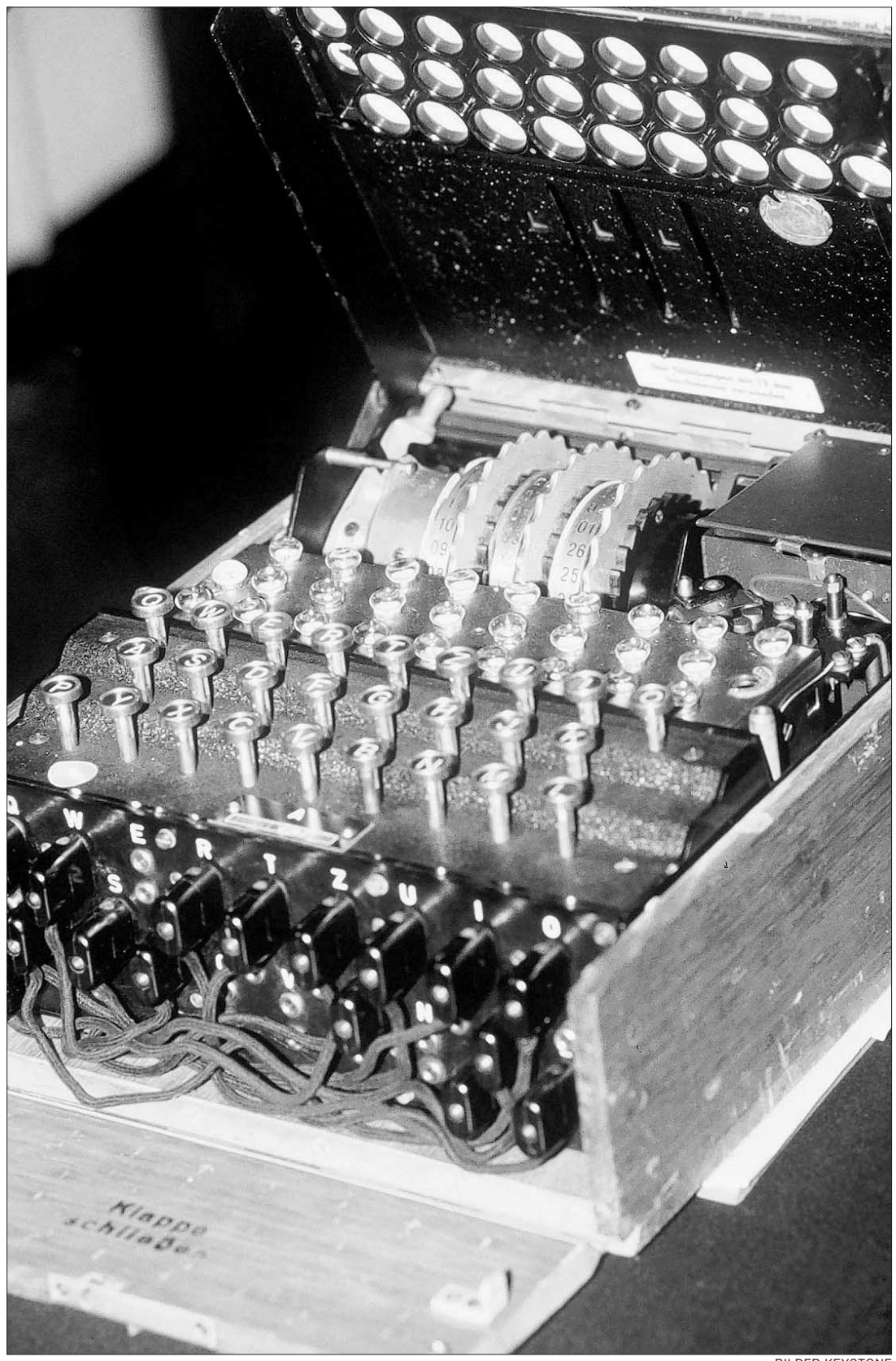
Das Prinzip des asymmetrischen Verfahrens beruht auf einer mathematischen Funktion, die sich nicht umkehren lässt. Was dieses Verfahren so revolutionär macht, ist die Tatsache, dass keine Schlüssel mehr verteilt werden müssen: Die öffentlichen Schlüssel werden publiziert, und die privaten Schlüssel bleiben bei den Teilnehmern.

Transaktionen schützen

Woher rührt das Interesse für dieses Verfahren? Es stammt weder vom Militär noch von Individuen, die ihren Mailverkehr schützen wollen, sondern vom Bedürfnis nach sicheren geschäftlichen Transaktionen: Ohne sichere Übermittlung im Internet gibt es keine sicheren Geschäftsprozesse. Die Sicherheit dieser neuen Verfahren beruht auf der simplen Tatsache, dass es heute noch keine Computer gibt, die stark genug sind, dieses Verfahren zu knacken.

Das wird sich ändern – und auch für diesen Fall ist bereits vorgesorgt: Experten träumen heute von der so genannten Quantenkryptografie. Hier würde der Empfänger eindeutig feststellen können, ob die Botschaft von einem Dritten belauscht worden ist. Dass dies möglich ist, hat eine Forschergruppe der Universität Genf 1997/98 auf einer zehn Kilometer langen Versuchsstrecke bewiesen.

Das Wettrennen zwischen Verschlüsseln und Entschlüsseln geht weiter. ◆



BILDER KEYSTONE

Tasten, Walzen, Kabel und Millionen von Kombinationsmöglichkeiten: Die mythische deutsche Chiffriermaschine Enigma, mit der die Nazi-Wehrmacht ihre Positionen tarnte.

Der Autor: Dominik Landwehr ist Leiter des Bereichs «Science and Future» des Migros Kulturprozents und publiziert regelmässig im Bereich Technologie und Gesellschaft.

Literatur: Robert Harris: Enigma, Roman, Ullstein-TB, Fr. 14.30. Andrew Hodges: Alan Turing – Enigma, Biografie, Rowohlt-TB, Fr. 23.–.