CRYPTO JUBILEE

EINE PUBLIKATION FÜR DIE KUNDEN UND FREUNDE DER CRYPTO AG, SCHWEIZ

2002

CRYPTO AG
50 YEARS SECURITY FOR EVER

Liebe Leserin, lieber Leser Die Crypto AG feiert dieses Jahr ein ganz besonderes Jubiläum, nämlich ihr 50-jähriges Bestehen. In diesen 50 Jahren haben wir die rasante Entwicklung auf unserem Tätigkeitsgebiet entscheidend mitgeprägt und sind zum technologisch führenden Anbieter von Systemen für Informationssicherheit geworden. Heute setzen wir mit unserem Sicherheitskonzept «Total Information Security© by Crypto AG» weltweit den Standard für den Schutz von Daten und Informationen gegen jeden unbefugten Zugriff.

Sicherheit vermitteln kann nur ein Geschäftspartner, der absolutes Vertrauen geniesst. Dass die Crypto AG in der ganzen Welt für die anspruchsvollsten Kunden dieser Partner ist, kommt nicht von ungefähr. Für viele unserer Kunden war und ist entscheidend, dass wir ein unabhängiges Schweizer Unternehmen sind. Unsere Grösse und unser Marktanteil erlauben es uns zudem, aus eigener Kraft an der Spitze der Entwicklung zu bleiben. Unsere Forschungs-, Entwicklungs- und Produktionsstätte in Zug mit 230 Mitarbeitenden bildet dazu die starke Basis.

Im Jubiläumsjahr haben wir diese Basis noch einmal gestärkt. Anfang Jahr wurde die Crypto AG in die vor einem Jahr geschaffene «The Crypto Group» integriert. Zusammen mit der Schwestergesellschaft InfoGuard AG, die vor allem den Businessmarkt bearbeitet, sind wir somit in der Lage, uns den technologischen und marktbedingten Herausforderungen der Zukunft erfolgreich zu stellen.

Vertrauen entsteht auch aus Kontinuität. Seit der Gründung im Jahr 1952 haben wir uns ausschliesslich mit Informationssicherheit beschäftigt. Und genau das werden wir auch in Zukunft tun. Unser Motto verstehen wir als Verpflichtung: «Security for ever!».

Kontinuität beinhaltet auch Wandel. Wirtschaft, Gesellschaft und Staat machen sich immer mehr die Möglichkeiten der digitalen Welt zu Nutze. Dadurch entstehen neue Märkte wie etwa im Bereich E-Business, E-Government, E-Banking etc. Mit unserer Kryptologie-Ausstellung im Schweizerischen Verkehrshaus in Luzern und mit der Jubilee-Edition dokumentieren wir diese Entwicklung sowie die Geschichte, Gegenwart und Zukunft der Kryptologie.

Walther A. Hegglin, Verwaltungsratspräsident der Crypto AG

KRYPTOGRAFIE: ALTE KUNST – TOPMODERN – MIT EINER GROSSEN ZUKUNFT

Kryptografie ist die Kunst, Nachrichten auf eine Art und Weise zu verschlüsseln, dass kein Unbefugter sie lesen kann. Bereits frühe Hochkulturen wie Ägypten, Indien, Mesopotamien oder Assyrien verwendeten sie. Berühmte Persönlichkeiten wie Caesar, der französische Diplomat Blaise de Vigenère, Päpste, die schottische Königin Maria Stuart, Thomas Jefferson, russische Zaren und Winston Churchill bedienten sich ihrer. Und sie fand unter anderem Erwähnung in der Bibel, der Ilias von Homer, dem Kamasutra und einem Werk von Edgar Allan Poe.

Michael Zimmermann

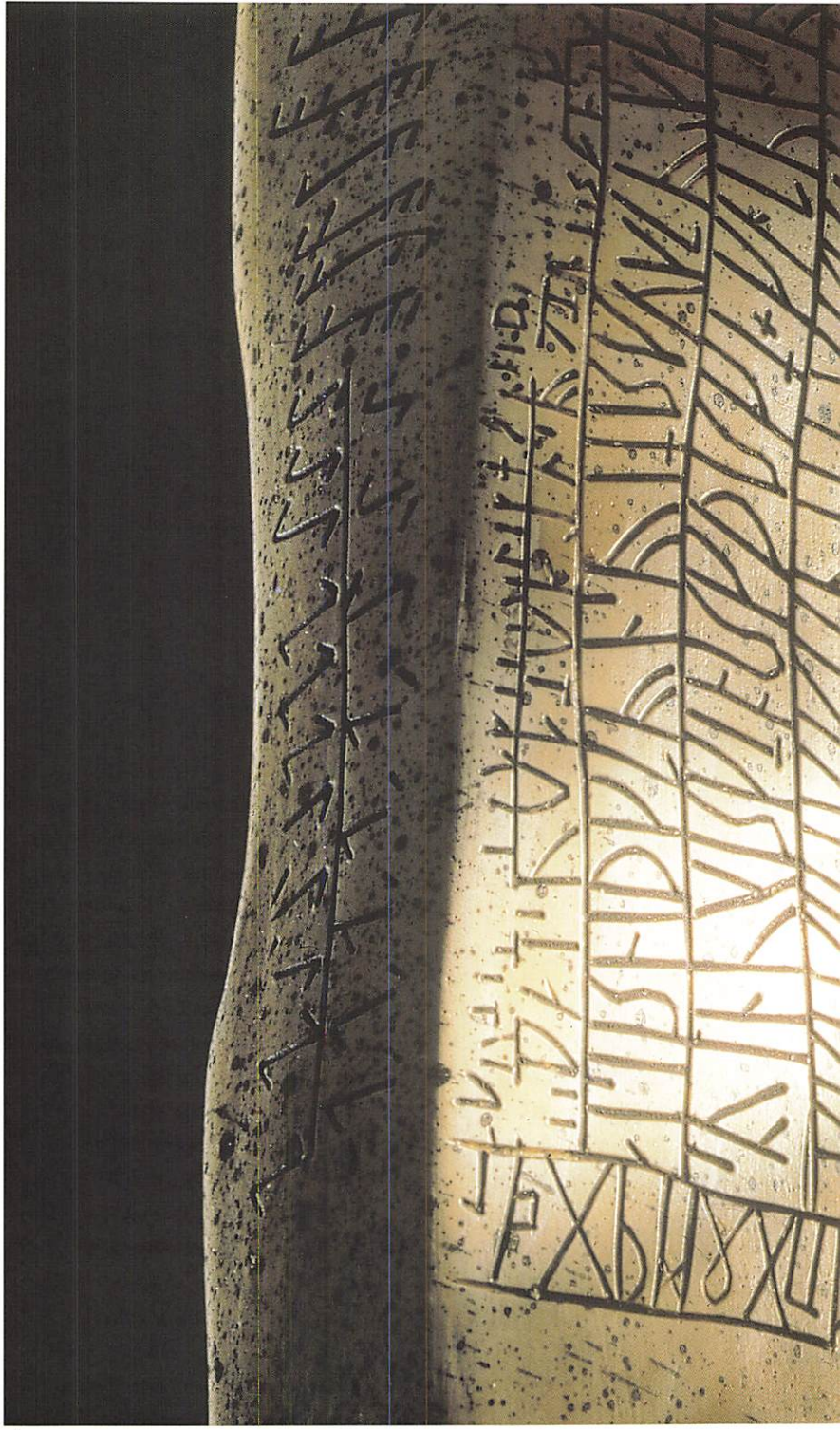
Wann der erste Mensch einem anderen eine verschlüsselte Botschaft schickte, ist sicherlich nicht erforschbar. Es gibt aber Hinweise, dass der Mensch, bald nachdem Schriften entwickelt und gebräuchlich waren, damit begonnen hat, Nachrichten auch zu verschlüsseln. Historisch belegt ist, dass die Kryptografie im antiken Sparta bereits im 5. bis 6. Jahrhundert vor Christus angewendet wurde. Plutarch schreibt darüber, wie die Regierung zur Übermittlung sensibler Informationen ein spezielles Verfahren anwendete: Skytale. Die Nachricht wurde auf einen schmalen Pergamentstreifen geschrieben, der in Form einer Wendel um die Skytale (einen Zylinder bestimmter Dicke) gewickelt war. Danach wurde nur der Streifen per Kurier übermittelt. Auf der Empfängerseite hatte man eine Skytale mit demselben Radius und konnte so die Nachricht wieder lesen. Wurde der Streifen vom Gegner abgefangen, so war er nutzlos, denn selbst wenn das Verfahren bekannt war, so konnte man den Radius der Skytale nicht kennen.

Heute mutet das Verfahren eher primitiv an, aber damals war die Lehre der Verschlüsselung erst am Anfang. Verfahren wie Skytale gehören in die Kategorie der Transpositionsverfahren. Dabei werden nur die Positionen der Buchstaben verändert, nicht aber deren Bedeutung. Dies ist eine Methode, die teilweise auch heute noch eingesetzt wird, allerdings in veränderter Form und meist nicht alleine. Wir werden ihr als Bestandteil aktueller Verfahren wiederbegegnen.

Das Caesar-Alphabet

Auch Gaius Julius Caesar (100 bis 44 v. Chr.) benützte ein Verschlüsselungsverfahren, um wichtige – auch private – Nachrichten für Unbefugte unlesbar zu machen. Es ist unter der Bezeichnung «Caesar» in die Geschichte eingegangen und funktioniert äusserst einfach. Man schreibt dazu ein Alphabet auf ein Blatt Papier und ein zweites darunter, aber um einen bestimmten Abstand verschoben. Mit den an einem der Ränder überstehenden Buchstaben füllt man auf der anderen Seite die entstandene Lücke. Caesar benutzte angeblich den Abstand «3», er ersetzte also beispielsweise A durch ein D: aus Crypto AG würde demnach «Fubswr DK». Nur wenn der Empfänger vom Schlüssel «3» wusste, konnte er die verschlüsselte Botschaft problemlos entziffern.

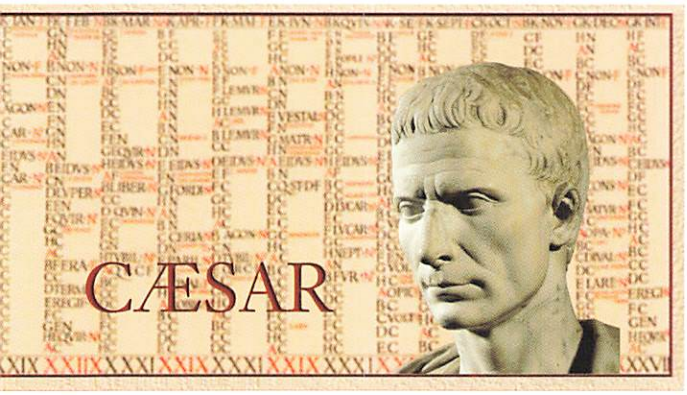
Der «Caesar» ist eine Verschiebechiffre, da die Position erhalten bleibt, nicht aber die Buchstaben selber. Deswegen werden solche Verfahren unter der Bezeichnung Substitutionsverfahren zusammengefasst. Die Schwäche dieses Verfahrens, die dem Kryptoanalytiker (Entzifferer) die Arbeit erleichtert, liegt in der Wahrscheinlichkeit der auftretenden Buchstaben im Klartext, die hier mit der im Ciphertext identisch ist, da auch der Schlüssel für jedes Zeichen des Textes identisch ist. Die einfache Verschiebechiffre ist deshalb durch statistische Mittel relativ leicht zu knacken. Jede Sprache hat nämlich ein quantitativ klares Wort- und Buchstabenprofil. Dabei spielt es keine Rolle, ob es sich um eine wissenschaftliche Abhandlung oder einen Liebesroman handelt. Im Deutschen wie auch im Englischen ist beispielsweise das «e» mit 17,4 Prozent der



RÖK STONE, RUNENSCHRIFT, SCHWEDEN, 9. JAHRHUNDERT

Die Caesar-Methode und ihre Verwandten

Das Verschlüsseln von Nachrichten hat eine lange Tradition: Schon der römische Feldherr Julius Caesar bediente sich rund hundert Jahre vor Christi Geburt eines einfachen Algorithmus, um sich bei seinen strategischen Plänen nicht über die Schulter blicken



AKG-Images/Erich Lessing

zu lassen. Statt geheime Zeichen zu verwenden, verschob Julius Caesar schlicht das Alphabet um einige Stellen: Aus A wurde D, B wurde in E umgewandelt. Er unterschied nicht zwischen Gross- und Kleinschreibung und liess die Leerzeichen weg. Caesar verdanken wir unser erstes monoalphabethisches Chiffrierverfahren: Die «Caesar-Addition» dient allen nachfolgenden Verfahren bis hin zum E-Mail-Verschlüsselungsprogramm Pretty Good Privacy (PGP) als Grundlage.

häufigste Buchstabe. Es folgt das «n» mit knapp 10 Prozent. Am dritthäufigsten wird mit 7,55 Prozent das «i» verwendet. Bedingung für eine erfolgreiche Dechiffrierung ist, dass eine ausreichend grosse Menge Geheimtext zur Verfügung steht. Das häufigste deutsche Wort heisst übrigens nicht «Geld» oder «Liebe», sondern «Zeit». Auf Platz zwei und drei: «Herr» und «Jahre». «Frau» folgt erst an vierzehnter Stelle.

Vigenère-Chiffre

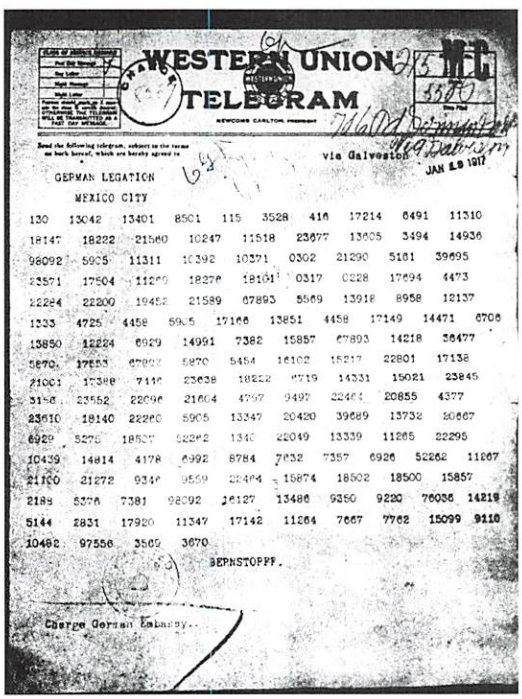
Der französische Diplomat Blaise de Vigenère (1523 bis 1596) erkannte diese Schwäche und entwickelte 1586 den so genannten Vigenère-Chiffre. Hierbei handelt es sich um eine polyalphabetische Substitution. Für die einzelnen Buchstaben des Klartextes werden zum Verschlüsseln nicht dieselbe, sondern mehrere verschiedene monoalphabetische Verschlüsselungen verwendet. Der Schlüssel kann jede beliebige

Buchstabenfolge sein. Zur Chiffrierung benötigt man das Schlüsselwort und das Vigenère-Quadrat. Die erste Zeile enthält das normale Alphabet. In der zweiten Zeile steht das um einen Buchstaben verschobene ABC. In der dritten das um zwei verschobene usw. Zuerst sucht man die Zeile, wo der Klartextbuchstabe steht, dann die Spalte, die den Schlüsselbuchstaben enthält. Im Kreuzungspunkt der beiden steht der chiffrierte Buchstabe. So arbeitet man sich bis zum Ende des Schlüsselwortes durch und beginnt dann wieder von vorne. Aber auch dieses Chiffrierverfahren ist zu knacken. Da bei langen Texten gewisse Regelmässigkeiten auftreten, sind die Schlüssellänge und dadurch das Schlüsselwort durch statistische Methoden ermittelbar.

Maria Stuart

Die schottische Königin Maria Stuart (1542 – 1587) bediente sich ebenfalls der Kryptografie. Nach

ihrer erzwungenen Absetzung suchte sie über einen raffiniert aufgebauten Spionagering Verbündete in England und im Ausland, besonders in Spanien und Frankreich. «Unablässig gehen die Boten in hundert Verkleidungen herüber und hinüber nach Paris und Madrid, Erkennungsworte werden vereinbart, ganze Chiffriersysteme ausgearbeitet und allmonatlich gewechselt, ein regelrechter überseeischer Postverkehr ist Tag für Tag im Gange. Die Briefe werden bald in die Wäsche geschmuggelt, bald in Büchern, in ausgehöhlten Stöcken oder unter dem Deckel von Schmuckkassetten verborgen, manchmal auch hinter dem Quecksilber von Spiegeln... bald Sohlen von Schuhen auseinandergeschnitten, um darin mit unsichtbarer Tinte geschriebene Botschaften einzupressen, dann wieder besondere Perücken angefertigt, in die man Papierröllchen eindreht. In den Büchern, die sich Maria Stuart aus Paris oder London schicken lässt, sind nach einem bestimmten Code einzelne Buchstaben unterstrichen, die zusammengesetzt einen Sinn ergeben.» (in: Stefan Zweig, Maria Stuart, S. 370 – 371). All dies nützte ihr aber nichts. Die Verschwörung wurde aufgedeckt und am 8. 2. 1587 fand die Enthauptung Maria Stuarts statt.


WESTERN UNION
TELEGRAM
via Galveston
JAN 19 1917
GERMAN LEGATION
MEXICO CITY
130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5181 39695
23571 17504 11299 18276 18101 0317 0228 17694 4473
22224 22200 19452 21589 07893 5569 13918 8958 12137
1335 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7110 23638 18222 0719 14331 15021 23845
3156 23552 22098 21864 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18502 98262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11867
21100 21272 9349 9559 22464 15874 18502 18500 15857
2189 5276 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670
SEPNSTOPFF.
George German Embassy.

Die Entschlüsselung des sogenannten Zimmermann-Telegramms hatte den Eintritt der USA in den Ersten Weltkrieg zur Folge.

Geheimfibeln

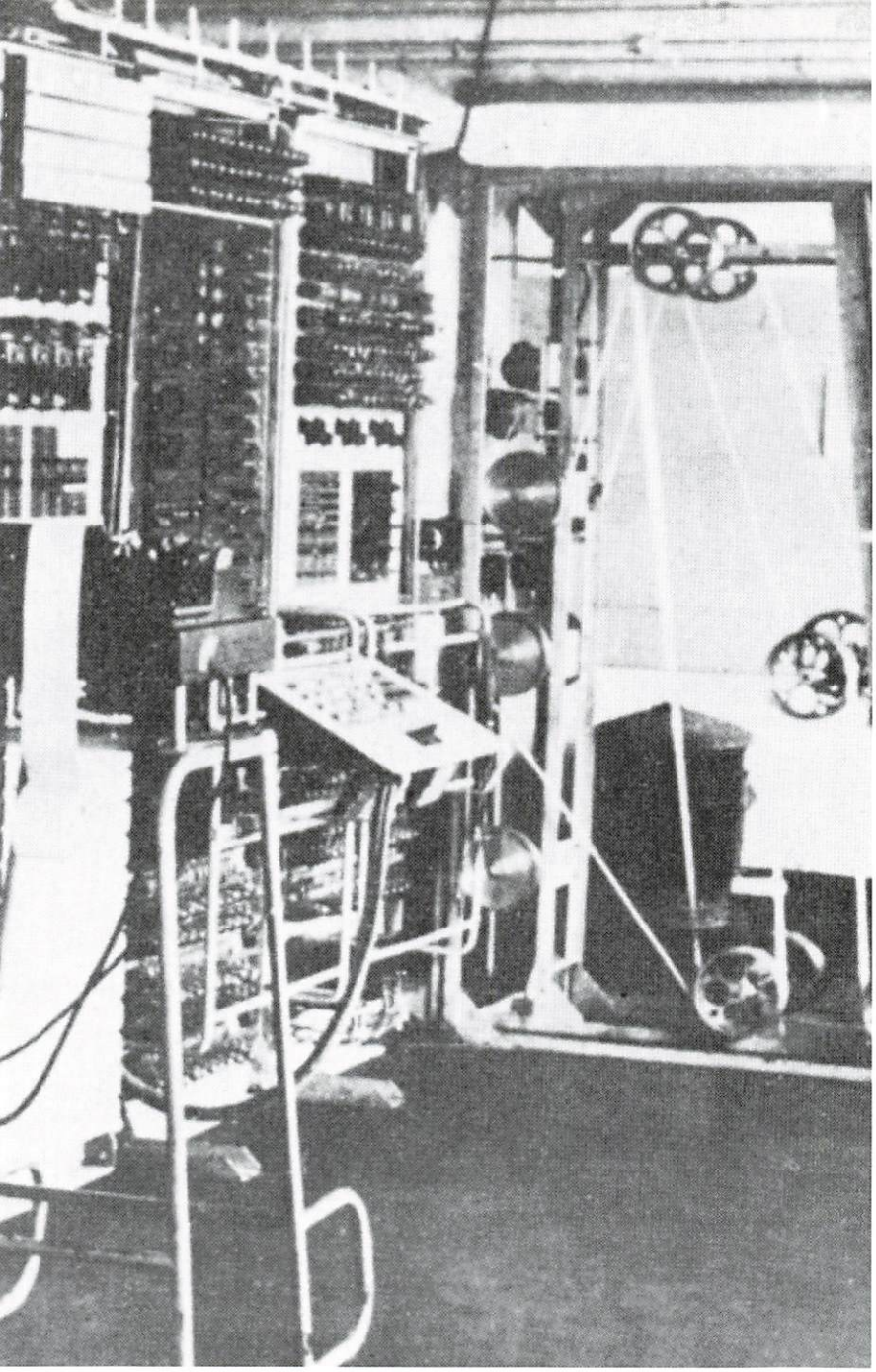
Kryptologie ist, wie das Beispiel von Caesar und Maria Stuart beweist, eng verbunden mit den Interessen der Mächtigen. In der Renaissance scharten die Päpste die besten Kryptologen um sich. Noch zu Beginn des letzten Jahrhunderts beschäftigte der Vatikan drei «cifristi», Kryptologen, um mit den Nuntiaturen in aller Welt verschlüsselt zu kommunizieren. Sie arbeiteten mit Codebüchern, in denen Begriffe und einzelne Buchstaben durch Zahlen ersetzt waren. Der Entschlüssler brauchte in seinem Codebuch nur die Zahl zu suchen, die einem Klarwort zugeordnet war. Diplomaten, Geheimlogen, Handelshäuser und Militärs, sie alle benutzten damals Codebücher, um ihre Nachrichten geheim zu halten. Das war allerdings umständlich und unsicher, denn die Codebücher mussten laufend erneuert, den Eingeweihten zugestellt und von diesen sicher verwahrt werden. Pannen gab es laufend: Entweder fiel eine der Geheimfibeln den Falschen in die Hände, oder der Code wurde geknackt.

Das Zimmermann-Telegramm

Eines der interessantesten kryptologischen Dokumente ist das so genannte Zimmermann-Telegramm. Gesendet wurde es am 16. Januar 1917. In Europa tobte der Erste Weltkrieg. Der deutsche Leiter des Auswärtigen Amtes, Arthur Zimmermann, teilte in der verschlüsselten Depesche seinem Botschafter in Mexiko mit, dass Deutschland beabsichtige, am 1. Februar den uneingeschränkten U-Boot-Krieg zu beginnen. Es werde versucht werden, die Vereinigten Staaten trotzdem neutral zu halten. Für den Fall, dass dies nicht gelingen sollte, schlage man Mexiko ein Bündnis vor mit dem Ziel, gemeinsam Krieg zu führen. Mexiko sollte mit der Rückeroberung der an die USA verlorenen Gebiete in Texas, New Mexico und Arizona geködert werden. Ein solcher Krieg hätte ein US-Engagement in Europa möglicherweise verhindert. Englische Kryptologen entzifferten jedoch den Text, die USA bekamen die Information – und schickten ihre Truppen über den Atlantik. Deutschland verlor den Ersten Weltkrieg.

Das Schicksal Europas

Das Schicksal Europas wäre wohl ein anderes ohne den deutsch-russischen Journalisten Richard Sorge. Dank der Kryptologie war es dem Tokio-Korrespondenten der «Frankfurter Zeitung» möglich, der Sowjetunion jahrelang wichtige Nachrichten weiterzugeben, ohne dass die Japaner mitlesen konnten. Im Mai 1941 warnte er Moskau vor dem bevorstehenden Überfall am 22. Juni durch Nazi-Deutschland. Das haben andere Quellen zwar auch getan. Nach dem Einmarsch aber konnte Sorge melden, dass Japan die Sowjetunion nicht angreifen werde. Dieser hochgeheime Beschluss der japanischen Führung gestattete dem UdSSR-General Shukow,



«Operation Bletchley Park» beschleunigt den Zweiten Weltkrieg

Der britische Mathematiker Alan Turing und seine Dechiffrierexperten arbeiteten in grösster Abgeschiedenheit im legendären Herrschaftshaus in Bletchley Park unweit von London. Sie brachten es fertig, in jahrelanger mühseliger Kleinarbeit die Signale der Enigma mittels einer «bomb», einer Vorform des heutigen Computers, zu entschlüsseln. Dank dieser Operation «Ultra» gelang es den Alliierten, ab 1942 monatlich 84000 deutsche Funksprüche zu entziffern. Ebenfalls hilfreich war das Wissen um die genauen deutschen Truppenaufstellungen entlang der französischen Küste im Vorfeld der Invasion in der Normandie.

Kampfverbände aus Sibirien abzuziehen und gegen die deutschen Aggressoren im Westen einzusetzen. Ohne Sorges Nachricht wären Hitlers Armeen vermutlich in der Lage gewesen, in Moskau einzumarschieren.

Die Enigma und Bletchley Park

Im Zweiten Weltkrieg spielte die Kryptologie nicht nur in diesem Fall eine entscheidende Rolle. Begriffe wie «Enigma» oder «Turing» dürften auch bei Nichtmathematikern nicht ganz unbekannt sein. Um ihre Kommunikation vor dem Feind geheim zu halten, benutzten sowohl die Alliierten wie auch die Achsenmächte unterschiedlichste Verfahren und trieben einen erheblichen Aufwand. In England machten sich die Kryptologen ab 1939 in Bletchley Park, einem Anwesen 50 Kilometer nordwestlich von London, an die Arbeit. Ihr Ziel war es, die mit der deutschen Chiffriermaschine Enigma (griechisch: Rätsel) verschlüsselten Feindmeldungen zu entziffern. Bekannt wurde dabei vor allem Alan Turing, ein genialer Mathematiker, dem mit seinen rund 200 Kollegen das von den Deutschen für unmöglich Gehaltene gelang. Entscheidend waren dabei unter anderem von deutschen Wetterbeobachtungsschiffen erbeutete Listen, denen die entsprechenden Einstellungen der Enigmas zu

entnehmen waren. Viele Historiker meinen, dass die Kryptografie im 2. Weltkrieg den Menschen ein Jahr Krieg erspart hat.

Die Enigma arbeitete mit mechanischen Mitteln. Sie bestand aus einer Reihe von Walzen, die komplex verdrahtet waren und sich nach jedem Buchstaben zudem wie ein Kilometerzähler weiterdrehten. Darüber hinaus wurden die Walzen in ihrer Reihenfolge ständig vertauscht. Damals erschien das Knacken einer Enigma-chiffrierten Botschaft als ein fast unlösbares Problem. Heute jedoch gelten Enigmas oder Rotormaschinen als nicht mehr hinreichend sicher.

Enigma, die genialste Schreibmaschine der Welt

Der legendären Enigma sind unzählige Artikel und Bücher gewidmet. Die erste elektromechanische Verschlüsselungsmaschine war ein Produkt gründlicher deutscher Ingenieurstechnik zur Zeit des Zweiten Weltkrieges. Die Enigma ähnelte äusserlich einer Schreibmaschine, ohne dass mit ihr jedoch Papier beschriftet werden konnte. Sie basierte auf dem Rotor-Chiffrierprinzip: Im Innern der Maschine waren 5 Walzen am Werk, welche sich nach jeder Eingabe um ein kleines Stück weiterdrehten. Dieses Prinzip war nicht durchschaubar. Aufgrund des täglich geänderten Tagescodes zur Einstellung der Walzen galten Enigma-Chiffren lange Zeit als unknackbar.

Die Navajos und Boris Hagelin

Während die deutsche Seite die Enigma und die Japaner die «Purple» (die bald von den Amerikanern geknackt wurde) einsetzten, benutzten die USA unter anderem eine Ressource, die nur ihnen zur Verfügung stand: die Sprachen der nordamerikanischen Ureinwohner. Nach einigen Versuchen mit Comanchen und anderen Stämmen wurden schliesslich vor allem im pazifischen Raum Navajos eingesetzt, die den USA einen enormen Vorteil gegenüber den Japanern einräumten. Navajos eigneten sich besonders für diesen Zweck: Der Stamm war genügend gross (damit war die Sprache noch lebendig), keiner der wenigen weissen und asiatischen Experten, die Navajo sprachen, war Japaner oder Deutscher, und die Sprache selbst ist hochkomplex und für Erwachsene schwierig zu lernen. Am Ende arbeiteten mehr als vierhundert Navajos als «Relais» in der amerikanischen Militärkommunikation.

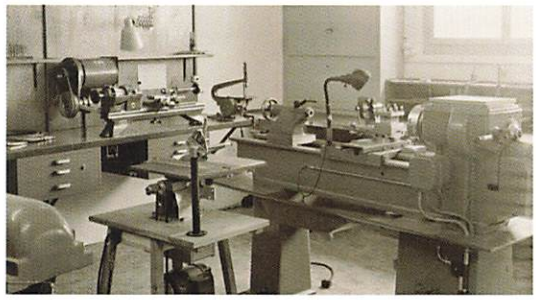
Daneben benutzten die Amerikaner aber natürlich auch andere Chiffriergeräte, und zwar solche, die von Boris Hagelin entwickelt wurden – dem Gründer der Crypto AG. Im Jahr 1939, praktisch in letzter Minute vor Kriegsbeginn, reiste der gebürtige Schwede über Genua in die USA. In seinem Gepäck hatte er zwei Exemplare seiner neuesten Entwicklung, der C-36-Maschine, dabei. Und diese Maschine sollte zur entscheidenden Basis für seinen endgültigen Durchbruch werden.

Sein Glück war, dass die USA bei Kriegsbeginn sofort eine grosse Anzahl Chiffriergeräte benötigten. Boris Hagelin war genau zur richtigen Zeit am richtigen Ort: Er konnte seine Prototypen vorführen und erhielt den Auftrag, so schnell als möglich eine Grossserienproduktion aufzuziehen. Dies geschah innerhalb von wenigen Monaten bei der Schreibmaschinenfirma Smith-Corona. Bis Kriegsende wurden nicht weniger als 140'000 Stück produziert! Die M-209, wie sie als Lizenzmodell hiess, war z.B. in grosser Stückzahl während der Invasion in der Normandie im Einsatz. Ihr Übername bei den GIs – «The Hag» – war nicht nur als Abkürzung von Hag-elin zu verstehen, sondern auch als Ausdruck der Bewunderung im Sinne des englische Wortes «The Hag», was soviel wie «Hexe» heisst...

Von den USA in die Schweiz

Den 2. Weltkrieg musste Boris Hagelin notgedrungen im Exil in den USA verbringen. Seine Firma in Schweden hatte in dieser Zeit weiter produziert und nach seinen Anweisungen neue Maschinen entwickelt. Nach Kriegsende wollte Boris Hagelin deshalb sofort von Schweden aus den Know-how-Vorsprung ausnützen und in den Export einsteigen. Die restriktive Exportgesetzgebung in Schweden behinderte jedoch seine ehrgeizigen Pläne. Es blieb ihm nichts anderes übrig, als nach einem anderen Standort zu suchen. Er fand ihn durch die Vermittlung eines Schweizer Industriellen in Zug in der Schweiz. Hier richtete er – im Jahr 1948 – zuerst ein Entwicklungslabor ein, das die Basis für seine weitere industrielle Tätigkeit werden sollte. Die Schweiz wurde in der Folge zu seiner zweiten Heimat. Hier starb er auch im Jahre 1983.

Die Pionierleistungen von Boris Hagelin basierten auf dem Prinzip der elektromechanischen Kryptografie. Mit solchen Geräten konnte man Buchstaben oder Zahlen mit mechanisch gesteuerten Schaltkreisen fortlaufend vertauschen und so für Unbefugte unlesbar machen. Die Hauptbestandteile dabei waren Zahnräder, Zahlenscheiben und elektrische Kontakte. Das Vertauschen erfolgte nach einem wählbaren Prozedere: Dem Chiffrierschlüssel. Die Schweiz als Land der Uhrmacher konnte hier Höchstleistungen an mechanischer Präzision und Zuverlässigkeit liefern.



Start der Crypto AG 1952 im Herzen der Schweiz

Die Gründung der Crypto AG geht auf den 15. Mai 1952 zurück. Zu diesem Zeitpunkt hatte der schwedische Kryptologe und Industrielle Boris Hagelin bereits eine erfolgreiche Karriere als Erfinder und Unternehmer hinter sich. Er übersiedelte 1948 in die Schweiz und verlegte Teile seines Unternehmens A.B. Cryptoteknik von Stockholm nach Zug.

Neue Technologie

Aber diese Ära der Elektromechanik ging im Laufe der Siebzigerjahre zu Ende. Eine neue Technologie, die Elektronik, begann immer mehr die Elektromechanik zu verdrängen. Das grundlegend Neue bestand in der Möglichkeit, Zahlen und Buchstaben zu digitalisieren. Damit wurde es möglich, Informationen in Computern und mit Hilfe von mathematischen Algorithmen beliebig rechnerisch zu verändern – statt bloss zu vertauschen. Sicherheit und Geschwindigkeit der Chiffrierung erreichten damit ganz neue Dimensionen. Bei der Crypto AG erkannte man rasch das ungeheure Potenzial der Digitalisierung und investierte bereits zu einem sehr frühen Zeitpunkt grosse Summen in diese neue Technologie. So wurde sie einmal mehr zum Pio-

nier, denn sie war in den Siebzigerjahren das erste Unternehmen in Europa, das integrierte Schaltungen in grossem Stil industriell einsetzte. Die Elektronik schuf auch ganz neue Möglichkeiten zur Automatisierung der Sicherheitsprozesse. Boris Hagelins Ziel, Sicherheit zu schaffen, möglichst ohne dass der Benutzer etwas damit zu tun hat, wurde immer realistischer.

Start in Zug

Ursprünglich in einem kleinen Schweizer Chalet an der Weinbergstrasse in Zug angesiedelt, entwickelte sich die Crypto AG sehr rasch und litt zusehends unter Platznot. 1966 erfolgte dann die Übersiedelung nach Steinhausen ZG, dem heutigen Standort. Die Crypto AG ist auf den Einsatz von Sicherheitslösungen in allen Arten von Kommunikationsnetzen spezialisiert, sei es IT, Telekom, Multimedia oder Funk. Weltweit vertrauen militärische wie auch zivile Behörden und Privatunternehmen den höchsten Sicherheitsansprüchen genügenden Crypto-Systemlösungen.

Von der Garagenfirma zum Global Player

Boris Hagelin begann seine Tätigkeit 1948 mit einem sozusagen «privaten» Konstruktionslabor in seinem Wohnhaus in Zug. Wenig später richtete er die erste Werkstatt in einer Doppelgarage auf dem Nachbargrundstück ein. Man kann also sagen, dass auch die Crypto AG als «Garagenfirma» begann – wie z.B. der Weltkonzern Hewlett-Packard. Bei der Garage blieb es allerdings nicht lange. Boris Hagelin sorgte mit seiner Dynamik rasch für Expansion. Obwohl er bei der Gründung der Crypto AG bereits 60 Jahre alt war.

In den folgenden 18 Jahren blieb das Unternehmen zwar in Zug, aber es musste immer wieder zusätzlichen Raum an verschiedenen Standorten beschaffen. Natürlich kam bald eine Produktionsabteilung hinzu, welche ihrerseits rasch grösser wurde. Die Folge: Zwei Standorte zu unterhalten – in Schweden und in der Schweiz – war nicht mehr sinnvoll. Seine Firma A. B. Cryptoteknik in Schweden – wie sie zuletzt hiess – wurde 1958 geschlossen und das ganze Unternehmen in Zug konzentriert.

Anfang der Sechzigerjahre wurde es allerdings immer schwieriger, in der Stadt geeigneten Raum für die Expansion zu finden. Man suchte deshalb ein Gelände für einen Neubau und fand es im Vorort Steinhausen. Die Eröffnung erfolgte 1966 mit einer Gebäudefläche von 6200 m² und mit 180 Angestellten. Damit erreichte die Crypto AG eindeutig industrielle Dimensionen. Aber auch hier musste der Betrieb bald vergrössert werden. Der Ausbau erfolgte in Steinhausen in mehreren Schritten, bis im Jahr 1986 mit einer Verdreifachung der Gebäudefläche auf fast 18000 m² und mit einer Belegschaft von 380 Angestellten der Höhepunkt der Expansion erreicht war.

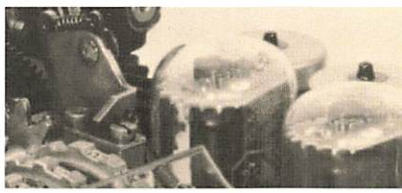
Die Trendwende

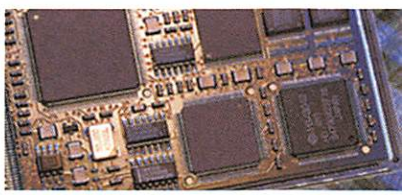
Die Trendwende in der äusserlich sichtbaren Enwicklung kam mit dem vollständigen Übergang zur integrierten Elektronik. Sie ermöglichte es, auf kleinstem Raum sehr viele technische Funktionen unterzubringen. Und dies veränderte zwangsläufig auch die Anforderungen an die Produktionsstrukturen und an das Personal: Mit weniger Beschäftigten konnte immer mehr produziert werden. Komplexe Produktionsprozesse, wie etwa die Bestückung von Leiterplatten, liefen nun vollautomatisch ab. Heute wird nur noch wenig mechanische Arbeit geleistet, z. B. in der Gehäuseherstellung. Demgegenüber nimmt der Einsatz von «Brain Power» laufend zu. So beschäftigt die Crypto AG heute Softwarespezialisten, Kryptologen, Mathematiker, Wissenschafter und

Schaltungstechniker. Aktuell sind es rund 230 Angestellte.

Kryptologie und die neuen Medien

Computer haben seit ihrer Erfindung in den Dreissigerjahren des letzten Jahrhunderts eine rasante Entwicklung genommen. Immer schneller und leistungsfähiger werdend, haben sie es geschafft, mehr und mehr in unser Leben Einzug zu halten und es grundlegend zu verändern. Der enorme Boom des Internets, ausgelöst durch die Entwicklung des World Wide Web zu Beginn der Neunzigerjahre, hat dazu geführt, dass unsere Welt immer vernetzter wird. Es gibt heute nur noch wenige Bereiche unserer Gesellschaft, die davon nicht betroffen sind. Innerhalb weniger Jahre sind wir dazu übergegangen, den Computer nicht mehr nur als nützliche Rechenhilfe oder Spielkonsole zu benutzen, sondern auch als neues Medium der Kommunikation. Eine eigene E-Mail-Adresse zu besitzen, war vor wenigen Jahren noch ausschliesslich Firmen- oder Universitätsangehörigen vorbehalten. Heute wird man oft schon verwundert angesehen, wenn man keine vorweisen kann.





Auch die Geschäftswelt hat das Internet für sich entdeckt. Es werden Videokonferenzen über das Internet abgehalten, Zweigstellen und Betriebe miteinander verbunden. Die Zahl der Online-Shops nimmt täglich zu. Banken bieten ihren Kunden längst die Möglichkeit, ihre Bankgeschäfte über das Internet zu erledigen. Der Computer in Verbindung mit dem Internet hat sich also zu dem Kommunikationsmedium des neuen Jahrtausends schlechthin entwickelt. Kommunikation, die über das Internet abgewickelt wird, ist allerdings potenziell unsicher. Sicherheit in der Informationstechnik – auch im Internet – ist deshalb untrennbar mit kryptografischen Techniken verbunden. Sie sind wichtige

Symmetrische Chiffrierung

Bei symmetrischen Verfahren wird zum Chiffrieren und Dechiffrieren derselbe Schlüssel verwendet. Dieser muss also sowohl dem Sender als auch dem Empfänger bekannt sein. Die Sicherheit ist aber nur gewährleistet, wenn der Schlüssel vor Dritten geheim gehalten werden kann. Zu den symmetrischen Verfahren gehören unter anderem Triple-DES und AES.

Instrumente zur Unterstützung der Vertraulichkeit, Integrität und Authentizität der elektronischen Kommunikation, aber auch bei der Speicherung bzw. Archivierung von Informationen. Diese grundlegenden IT-Sicherheitsziele sind nur auf der Basis starker kryptografischer Verfahren sicherzustellen.

Public-Key-Kryptografie

Für solche Verfahren sind heute nicht nur die technologisch-mathematischen Grundlagen vorhanden, sondern es gibt auch erprobte Lösungen für alle Sicherheitsbedürfnisse. Dabei wird heute insbesondere zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren unterschieden. Bis zum Beginn des 20. Jahrhunderts hatten nicht die Mathematiker, sondern die Sprachwissenschaftler in der Kryptografie die erste Geige gespielt. «Bisher hat noch niemand einen Nutzen der Zahlentheorie entdeckt», hatte der englische Mathematiker G. H. Hardy 1940 noch über denjenigen Zweig der Mathematik behauptet, der sich mit den besonderen Eigenschaften ganzer Zahlen beschäftigt. Heute hat sich das grundlegend verändert. Ebendiese Zahlentheorie verhalf der Kryptografie zum grössten Durchbruch seit über 2000 Jahren. Sie führte zur so genannten Kryptografie mit öffentlichen Schlüsseln (Public-Key-Kryptografie). Die gebräuchlichste Variante der Public-Key-Kryptografie, das nach den drei Entwicklern Ronald Rivest, Adi Shamir und Leonard Adleman benannte RSA-Verfahren, nutzt die Schwierigkeit aus, grosse Zahlen in ihre Primfaktoren zu zerlegen.

Besonders interessant ist hier die Geschichte von Phil Zimmermann. Er hat sich zum Ziel gesetzt, die hochgradig sichere Verschlüsselung einem breiten Publikum zugänglich zu machen, und versetzte damit die amerikanischen Sicherheitsexperten in Panik, meinen Experten in verschiedenen Publikationen. Denn ein hohes Mass an Sicherheit im Internet schützt zwar die Privatsphäre der Nutzer – schliesslich sind E-Mails unglaublich leicht abzufangen – ist aber ein zweischneidiges Schwert. Denn auch Kriminelle, Terroristen, Waffen- und Drogenhändler können ihre Machenschaften mit starken Chiffrierverfahren vor der Strafverfolgung schützen. So hat die

COMPUTERGRAFIK DES GLOBALEN INTERNETVERKEHRS: JEDE LINIE REPRÄSENTIERT DEN WEG VON DATEN, DIE AN EINE VON 20 000 AUSGEWÄHLTEN STATIONEN GESCHICKT WURDEN. DIE EINGEFÄRBTEN LINIEN ZEIGEN AUF, WELCHEN ANTEIL AUSGEWÄHLTE NATIONEN AM GESAMTEN INTERNETVERKEHR AUSMACHEN: PINK STEHT FÜR USA, DUNKELBLAU FÜR GROSSBRITANNIEN, HELLBLAU FÜR ITALIEN, HELLGRÜN FÜR SCHWEDEN UND WEISS FÜR UNBEKANNT.

Asymmetrische Chiffrierung

Bei asymmetrischen Verfahren werden zwei verschiedene Schlüssel verwendet, ein öffentlicher Schlüssel (Public Key) zum Chiffrieren und ein privater Schlüssel (Private Key) zum Dechiffrieren. Die beiden Schlüssel werden vom Empfänger als Paar erzeugt, wobei der öffentliche Schlüssel bekannt gemacht und der private Schlüssel geheim gehalten wird. Mit dem öffentlichen Schlüssel kann nun jedermann Nachrichten so chiffrieren, dass sie nur noch vom Besitzer des dazugehörenden privaten Schlüssels dechiffriert werden können. Der Vorteil gegenüber symmetrischen Verfahren liegt darin, dass keine geheimen Schlüssel verteilt werden müssen. Typische Vertreter von asymmetrischen Verfahren sind Diffie-Hellman und RSA.

Chancen und Gefahren der Informationstechnologie

Im Bereich der Informations- und Kommunikationstechnologie erleben wir seit Jahren eine geradezu atemberaubende Entwicklung, die durch grossartige Leistungssteigerungen der informationstechnischen Systeme und immer kürzere Innovationszeitspannen gekennzeichnet ist. Sie stellt uns politisch, wirtschaftlich, rechtlich, organisatorisch, kultur- und sozialpolitisch sowie auf dem Gebiet der Sicherheit der Informationstechnik vor schwierige Aufgaben. Verschlüsselung, elektronische Signaturen und fehlerfreie Softwaretechnologie sind einige der wichtigsten Themenbereiche in der aktuellen Diskussion über Sicherheitsstrategien auf dem Weg in die Informationsgesellschaft.

Die treibende Kraft und der Motor der Entwicklung ist die Internet-Technologie. Sie verändert bereits heute fast alle gesellschaftlichen Bereiche. Diese Entwicklung bietet grosse Chancen. Wissen wird als Produktionsfaktor und als Faktor für die menschliche Entwicklung durch die Zugangsmöglichkeiten der Informationstechnik breit verfügbar. Mehr Wissen und mehr Bildung bedeuten mehr Lebensqualität. Den Chancen stehen allerdings auch Risiken gegenüber. Zu den Problemen gehören der wachsende Missbrauch der neuen technischen Möglichkeiten durch Kriminelle und Extremisten. Dies gilt vor allem für das Internet. Die Bandbreite der kriminellen Machenschaften ist inzwischen erschreckend und Delikte der Wirtschaftskriminalität, wie Betrug und Geldwäsche, aber auch Wirtschaftsspionage und Sabotage, werden weiter zunehmen.

Aum-Sekte, die 1995 den Giftgasanschlag in einer Tokioter U-Bahn verübte, einen Teil ihrer Kommunikation mit einer Methode der Public-Key-Kryptografie verschlüsselt. Experten diskutieren daher wiederholt die Frage, inwieweit kryptografische Methoden öffentlich zugänglich gemacht werden sollten.

Zimmermann hat seine Version der Public-Key-Kryptografie, die er «Pretty Good Privacy» (PGP) nennt, allen Widerständen zum Trotz im Internet zur Verfügung gestellt. Weil die amerikanische Regierung Verschlüsselungssoftware zu den Rüstungsgütern zählt, sah sich Zimmermann beschuldigt, ein Waffenhändler zu sein. Erst nach dreijähriger Ermittlung stellte die amerikanische Bundesanwaltschaft 1996 das Verfahren gegen Zimmermann ein, denn PGP war längst durchs Internet entwischt.

Quantenkryptografie

Die Entwicklung eines so genannten Quanten-

Biometrie: wo das Auge nicht Spiegel der Seele, sondern Beweis der Identität ist.

Biometrie – die Lehre der Vermessung körpereigener Merkmale: Wo PIN und Passwörter keine ausreichende Sicherheit mehr gewährleisten, setzen die biometrischen Verfahren an. Zeitlose physische Eigenschaften wie Iris oder Fingerabdruck lassen nicht nur die Identität, sondern gerade auch die Authentizität einer Person beweisen. Ein Augen-Scan wird beispielsweise mittels eines Sensors erfasst und auf bestimmte Charakteristika reduziert. Diese Eigenschaften, auf Zahlenwerte reduziert, werden mit den gespeicherten Datensätzen verglichen. Der geschützte Zugang zu einem Gebäude oder einem Computer ist jedoch nur ein Anwendungsgebiet biometrischer Verfahren. Bald schon sollen Schnittstellen zwischen Mensch und Computer möglich sein, welche sich an der menschlichen Sprache und Mimik orientieren.

computers, eines Rechners, der heutige Supercomputer zu Rechenschiebern degradieren könnte und gängige Verschlüsselungen in Sekundenschnelle knacken soll, ist für Experten eine Schreckensvision. Ein Quantencomputer würde «unsere Privatsphäre gefährden, den elektronischen Handel untergraben und sämtliche Vorstellungen von nationaler Stabilität gefährden», meinen diese.

So dramatisch wird es wahrscheinlich nicht kommen, eher wird die Kryptografie vor der Verbreitung leistungsfähiger Quantencomputer an das nötige Sicherheitsniveau angepasst. Gegenüber der Quantenkryptografie, einer absolut abhörsicheren Methode der Verschlüsselung, die spezielle Eigenschaften von Photonen ausnutzt, ist selbst der stärkste Quantencomputer machtlos.

«UNSER ZIEL IST ES, FÜR UNSERE KUNDEN SYSTEME DER INFORMATIONSSICHERHEIT HÖCHSTER GÜTE ZU ENTWICKELN UND ZUR VERFÜGUNG ZU STELLEN.»

GIULIANO OTTH, GESCHÄFTSFÜHRENDER DIREKTOR:

«DIE ZUKUNFT GEHÖRT DER INFORMATIONSSICHERHEIT UND DAMIT AUCH DER CRYPTO AG»

Die Crypto AG feiert in diesem Jahr ihr 50-jähriges Bestehen. Im folgenden Interview hält der geschäftsführende Direktor Giuliano Otth einen kurzen Rückblick auf die Geschichte der Crypto AG, die Entwicklung auf dem Gebiet der Informationssicherheit in den letzten 50 Jahren und nimmt Stellung zu den heutigen und künftigen Anforderungen an Systeme der Informationssicherheit.

Interview: Michael Zimmermann

Herr Otth, für die Firma Crypto AG ist das Jahr 2002 ein ganz besonderes: Sie feiert nämlich ihr 50-jähriges Bestehen. Und die Firma ist heute der technologisch führende Anbieter von Systemen für Informationssicherheit. Was die Firma heute ist, verdankt sie natürlich auch ihrer Vergangenheit. Können Sie uns etwas über die Anfänge der bewegten Firmengeschichte erzählen?

Giuliano Otth: Wir sind bei der Crypto AG in der glücklichen Lage, uns auf einen absoluten Pionier der Chiffriertechnik als Firmengründer

berufen zu dürfen: Auf den 1882 geborenen Schweden Boris Hagelin. Die Familie Hagelin war mit der Familie Nobel befreundet, also mit jener Familie, aus der auch der Stifter der Nobelpreise stammte. Die Familie Nobel war es, die Boris Hagelin den Einstieg in die Kryptografie ermöglichte. Sie half ihm und seinem Vater 1921 bei der Finanzierung des Kaufs einer Firma, die sich mit der Konstruktion von Chiffriergeräten befasste.

Aber wieso haben die Firmen Nobel und Hagelin damals ausgerechnet in die Kryptografie investiert?

Giuliano Otth: Wie Boris Hagelin in seinen Lebenserinnerungen erzählt, war er bereits zu diesem Zeitpunkt überzeugt, dass der zunehmende diplomatische Verkehr zwischen den Staaten es nötig machen würde, Geheimschrift maschinell zu erzeugen. Eine wahrhaft visionäre Einsicht! Seine Zielsetzung hiess immer: Perfektionismus. Aber mit der Absicht, den Menschen als das schwächste Glied zu entlasten. Es ging ihm also darum, den Betrieb der Chiffriermaschinen so zu vereinfachen, dass Fehler möglichst ausgeschlossen wurden. Damit formulierte er ein Sicherheitsprinzip, das bis heute nichts von seiner Bedeutung eingebüsst hat.

Boris Hagelin konnte zu Beginn des 2. Weltkrieges seine neuste Erfindung in Lizenz verkaufen und hat damit den finanziellen Grundstein für seine spätere, zweite Unternehmerphase gelegt. Warum hat ihn der Weg dazu in die Schweiz geführt?

Giuliano Otth: Nach Kriegsende wurde in Schweden eine sehr restriktive Exportgesetzgebung auch in Bezug auf Chiffriergeräte erlassen und behinderte seine ehrgeizigen Pläne, weshalb er sich nach einem anderen Standort umsah. Auch im Rückblick darf man sagen, dass Boris Hagelin sehr genau wusste, warum er gerade die Schweiz wählte. Vieles von dem, was ihn in die Schweiz brachte, gilt auch heute noch: Neben den landschaftlichen Schönheiten der Schweiz gibt es natürlich auch eine ganze Reihe von harten Facts, die für einen Standort Schweiz sprechen, wenn man auf dem Gebiet der Informationstechnologie und Informationssicherheit tätig ist. Man findet in der Schweiz zum Beispiel viele hoch qualifizierte Arbeitskräfte in praktisch allen Technologie- und Wissenschaftsbereichen. Die Gesetzgebung in Bezug auf den Export ist freiheitlich und die Schweiz ist politisch neutral. Ferner ist die politische Stabilität sprichwörtlich und es herrscht ein vorteilhaftes Investitionsklima für Unternehmen.

In den vergangenen 50 Jahren hat sich nicht nur die Crypto AG stark entwickelt, sondern es gab auf dem Gebiet der Informationstechnologie und der Chiffrierung von Information generell grosse technische Fortschritte.

Giuliano Otth: Es gab in den letzten 50 Jahren enorm viele Entwicklungen in diesen beiden Bereichen, und zwar in verschiedenen Sparten. Ich will nur einige davon nennen. Technologisch fand der Übergang von der Mechanik über elektromechanische Produkte zur elektronischen Hardware und vor allem heute auch Software statt. Die Rechner- und Speicherleistungen der Computer nehmen rasend schnell zu. Gängige Übertragungsgeschwindigkeiten waren vor fünfzig Jahren höchstens ein paar hundert Zeichen pro Sekunde. Sofern überhaupt digital gearbeitet wurde. Viel verbreiteter waren Analogsysteme. Heute reden wir von Gigabits pro Sekunde, Entwicklungen gehen zu Übertragungsgeschwindigkeiten von Terabits pro Sekunde. Die Applikationen, vor 50 Jahren primär Telex, Telefon und Kurzwelle, entwickelten sich über Fax zu Datenübermittlung, Richtstrahl- und Satellitenverbindungen bis zum heute sehr verbreiteten Internet. Auf der Anwenderseite waren vor 50 Jahren ausschliesslich Regierungskunden, und dabei vor allem das Militär und die Aussenministerien, an Informationssicherheit interessiert. Im Laufe der Jahre kamen weitere Regierungsstellen dazu. In den letzten Jahren, mit der unheimlich schnellen Verbreitung vor allem des Internets und der Einführung des E-Commerce, auch Banken, Industrieunternehmen, Versicherungen usw.

Was sind die heutigen Anforderungen im Bereich Informationssicherheit und was bringt uns die nahe Zukunft in dieser Hinsicht?

Giuliano Otth: Ein nächster Schub, der dann alle Bürgerinnen und Bürger eines Landes betrifft, kommt mit der Einführung des so genannten E-Governments. Auf der Seite der Informationssicherheit erlaubt die technologische Entwicklung die Implementierung immer leistungsfähigerer und komplexerer Chiffrieralgorithmen. Dies ist auch notwendig, da der Kryptoanalyse auch immer leistungsfähigere Systeme zur Verfügung stehen. Ein Meilenstein war sicher die Entwicklung der asymmetrischen Chiffrierverfahren (auch Public-Key-Systeme genannt). Die dabei zur Anwendung gelangenden mathematischen Verfahren erlauben, die Integrität und Authentizität einer Nachricht, sowie die Identität von Sender und Empfänger zu überprüfen. Auch auf dem Gebiet der vor allem von Regierungsstellen genutzten proprietären Algorithmen wurden grosse Fortschritte erzielt. Ich denke dabei an die Sicherheitsmanagementsysteme und vor allem auch an die immer grösser werdenden Möglichkeiten der kundenspezifischen Wahl der Struktur der Algorithmen. Insgesamt bin ich davon überzeugt, dass der Informationssicherheit und damit auch Firmen wie der Crypto AG die Zukunft gehört.

Was bedeutet dies in Bezug auf die Systeme und Produkte der Crypto AG?

Giuliano Otth: Natürlich müssen wir mit der Entwicklung in der Informationstechnologie Schritt halten. Das ist eine sehr grosse Herausforderung. Unsere Systeme und Produkte sind ja in der Regel nur ein Teil des Gesamtsystems. Daneben müssen wir natürlich auch neue Bedrohungsformen, gerade bei der Einführung neuer Technologien, sorgfältig analysieren. Von Viren hat man vor fünfzig Jahren sicher noch nicht gesprochen. Bei der Vielfalt der heutigen Anwendungen ist es aber für ein kommerzielles Unternehmen wie die Crypto AG äusserst wichtig, zusammen mit unseren Kunden eine Analyse durchzuführen, welche Systeme bei ihnen tatsächlich zum Einsatz kommen werden. Sie finden bei uns eine breite Palette von Lösungen und dazugehörigen Produkten. Unser Ziel ist es, für die bei unseren Kunden eingesetzten IT- und Kommunikationssysteme optimal abgestimmte Sicherheit höchster Güte zu entwickeln und zur Verfügung zu stellen.

Wie stellt sich die Crypto AG heute und in Zukunft diesen Herausforderungen?

Giuliano Otth: Technisch gesehen haben wir ein umfassendes Sicherheitskonzept erarbeitet: «TIS© by Crypto AG». Die Diskussion um IT-Security wird fälschlicherweise oft auf Schlüssellängen reduziert. Sicherheit auf höchstem Niveau hat aber ganz andere Dimensionen. Sie besteht bei Systemen mit der Qualifikation «TIS© by Crypto AG» aus einer ausgeklügelten Sicherheitsarchitektur, die in Hard- und Software implementiert ist. Selbstverständlich kommt den eingesetzten Algorithmen zentrale Bedeutung zu. Die Qualität der von uns entwickelten Algorithmen und des automatisierbaren Key-Managements gilt in Expertenkreisen als konkurrenzlos. Jeder Kunde unserer proprietären Verfahren erhält Customer Specific Algorithms (CSA) und operiert somit kryptologisch auf gleichem Niveau, wie wenn er sie selbst entwickelt hätte. Einzigartig sind wir auch in Bezug auf System-Transparenz, dank unserem exklusiven «Acceptance Cipher Check» ACC. TIS© (Total Information Security) heisst: Der gesamte Systemaufbau wird von A bis Z der Zielsetzung «integrale, automatisierte Sicherheit» unterworfen. Alle gewünschten Sicherheitsdienste sind anwendbar. Logische, physikalische und organisatorische Massnahmen können mit unserem umfassenden Sicherheitskonzept anwenderspezifisch eingeplant werden.

Und was braucht es sonst noch dazu?

Giuliano Otth: Erfolgreich zu sein, steht und fällt mit den Mitarbeiterinnen und Mitarbeitern. Sie sind es, die die Impulse von aussen aufnehmen, evaluieren und wiederum in Systeme und Produkte umsetzen. Um Impulse zu bekommen, sind natürlich enge Kontakte zu unseren wichtigsten Partnern, nämlich den Kunden, notwendig. Sie ent-

scheiden, was für Systeme beschafft und zum Einsatz kommen werden. Unsere Sicherheitslösungen müssen dazu passen. Auch mit den Herstellern von Gesamtsystemen in der Informationsbranche ist ein enger Kontakt notwendig. Sie sind es, die die technologischen Impulse geben und umsetzen. Und in ihren Systemen müssen unsere Lösungen funktionieren. Daneben muss das Unternehmen natürlich bereit sein, den notwendigen F&E-Aufwand bereitzustellen. Die Crypto AG hat das stets getan und war deshalb mit ihrem Produktsortiment immer «up to date». Wir werden das auch in Zukunft tun. Und wir können es tun, weil immer mehr Organisationen die Sicherheit ihrer Informationen unseren Lösungen und Produkten anvertrauen. Und dafür möchte ich allen unseren Kunden an dieser Stelle herzlich danken.

Die Crypto AG hat vor etwas mehr als einem Jahr eine Schwestergesellschaft gegründet – die InfoGuard AG, die sich vor allem um den Businessmarkt kümmert. Was sind die Gründe dafür?

Giuliano Otth: Im Jahr 2000 haben wir uns entschieden, den Businessmarkt intensiv und professionell anzugehen. Wir wollen die Kunden im Businessmarkt mit optimal für ihre Bedürfnisse entwickelten Produkten und Dienstleistungen für uns gewinnen. Mit den fünf Kompetenzzentren Awareness Establishing, Consulting Services, Education Services, Technology Implementation und Security Preservation Services verfügt InfoGuard AG über das umfassende Know-how, um ihren Kunden eine durchgehend gesicherte Information für den Geschäftsprozess zu gewährleisten. Das Spektrum beinhaltet die Schulung in der Problemerkennung und dem Umgang mit Risiken, welche mit der Anwendung von modernen Informationstechnologien verbunden sind, sowie die unternehmensspezifische Beratung und Schulungsleistungen, die es dem Kunden ermöglichen, eine individuelle Sicherheitslösung zu definieren und umzusetzen. Weiter bietet InfoGuard AG eigene, konkrete IT-Sicherheitslösungen an und hilft bei deren Implementation. Mit diesen auf AES-Standard-Algorithmen basierenden Lösungen kann der Kunde seine Aktivitäten uneingeschränkt und risikolos abwickeln. Schliesslich garantiert InfoGuard AG seinen Kunden jederzeit die Sicherheit und Verfügbarkeit der eingesetzten Systeme.

Nun wird in diesem Jahr ja auch kräftig gefeiert: Nicht nur mit den Mitarbeitenden, den Kunden und Behörden, sondern auch in Form einer Jubiläumsausstellung. Worum handelt es sich dabei?

Giuliano Otth: Die Crypto AG ist dabei, aus Anlass ihres 50-Jahr-Jubiläums im Verkehrshaus der Schweiz in Luzern auf einer Fläche von 100 bis 120 Quadratmetern eine Kryptologie-Ausstellung zu realisieren. Diese einzigartige Ausstellung soll die Bereiche Geschichte, Gegenwart und Zukunft der Kryptologie umfassen. Die Crypto AG will mit der Ausstellung einerseits ein technisch hochkomplexes Thema auf populärwissenschaftliche Art und Weise einer breiten Öffentlichkeit zugänglich machen. Andererseits soll das Bewusstsein geweckt werden, dass IT- und Informationssicherheit heute und in Zukunft für jeden Einzelnen ein immer wichtigeres Thema wird.

DER ERFOLG EINER FIRMA STEHT UND FÄLLT MIT DEN MITARBEITERINNEN UND MITARBEITERN.

Crypto AG
P.O. Box 460, CH-6301 Zug/Switzerland, Phone +41 41/749 77 22, Fax +41 41/741 22 72, crypto@crypto.ch, www.crypto.ch
Regionale Büros: Abidjan • Abu Dhabi • Buenos Aires • Kuala Lumpur • Riyadh • Sultanate of Oman