

Vertraulich.



Moderne Kryptologie.

«Wissen ist Macht», heisst es bei Francis Bacon. Darum ist es besser, manches Wissen dem Zugriff derer zu entziehen, die es manipulieren oder die Wissensmacht missbrauchen könnten.

Seit das Zeitalter der Geheimeure vom Zeitalter elektronischer Medien abgelöst wurde, zirkuliert vertrauliches Wissen in Kommunikationskanälen, die mit wenig Aufwand angezapft werden können:



Funkstrecken, Telefon- und Telexverbindungen, Datenfernübertragungs- und Computernetze. Da diese Wege der Kommunikation vom Benutzer meist weder kontrolliert noch lückenlos abgedichtet werden können, muss die Absicherung bei den Inhalten ansetzen. Die Lösung heisst Informationssicherheit. Und die kommt von Crypto.

In dieser Broschüre
lesen Sie

von sicherheitsbewussten
Polizisten und
Grenzwächtern
Seite 4

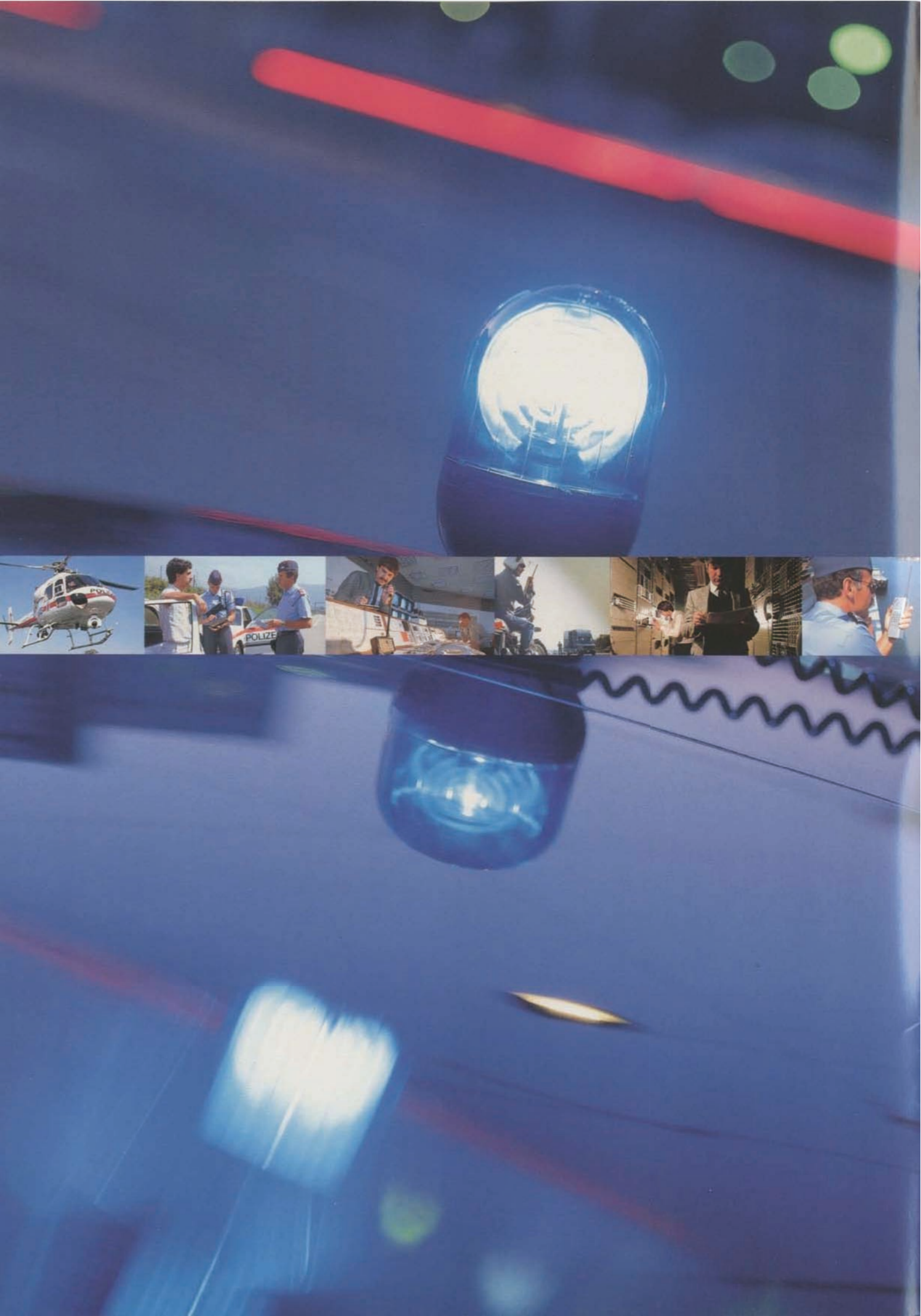
von verschwiegenen
Diplomaten und Attachés
Seite 6

von geheimnisvollen
Militärs Seite 8

über die Forschung
bei Crypto
Seite 10

über die Logistik
von Crypto
Seite 12

über Ägypter, Sumerer,
Spartaner, Römer
und den Crypto-Gründer
Boris Hagelin
Seite 14



Öffentliche Sicherheit ist nichts für fremde Ohren.

Die Sicherheitskräfte von Polizei und Grenzschutz sind Teil der zivilen Staatsmacht. Sie sorgen für die Aufrechterhaltung von Sicherheit und Ordnung im Land, und sie bekämpfen die Kriminalität, indem sie Rechtsbrecher verfolgen und überführen.

Es versteht sich von selbst, dass Polizisten und Grenzbeamte Aussenstehenden keinen Einblick in ihre Absichten und in ihre Einsatzplanung geben wollen,



untereinander jedoch intensiven Kontakt pflegen müssen, um erfolgreich zu sein. Das Problem ist, dass der Grossteil ihrer internen Kommunikation über Funknetze abgewickelt wird, die abgehört werden können. Crypto hat dafür die Lösung.

Beamte der Sicherheitsdienste werden heute zunehmend mit mobilen Datengeräten ausgerüstet, über die sie während des Einsatzes sicherheitsrelevante Kenndaten von Personen und Fahrzeugen über Funk bei zentralen Fahndungscomputern abfragen können. Diesen Datenverkehr und zugleich den gesamten Sprechfunk sichern intelligente Chiffriersysteme von Crypto.



Verhandlungskünstler brauchen vertrauliche Sphären.

Die Diplomaten und Attachés vertreten ihr Land in anderen Staaten und bei internationalen Organisationen. Als offizielle Gesandte beobachten sie die politischen, wirtschaftlichen und kulturellen Beziehungen zu ihrem Land und wachen über dessen Interessen.

Mit dem Aussenministerium ihres Heimatlands stehen die Diplomaten in regelmässigem Kontakt,



vor allem über Telekommunikationsnetze, die jedermann zugänglich sind. Und hier liegt das Problem. Die Meldungen, die über die öffentlichen Telefon-, Telefax-, Telex-, Daten- und Funkverbindungen ausgetauscht werden, müssen gegen unerwünschte Mitleser und -hörer abgesichert sein. Die Lösung kommt von Crypto.

Die Chiffriertechnik von Crypto macht jeden diplomatischen Kommunikationskanal abhörsicher, denn sie verschlüsselt gesprochene, geschriebene oder digitalisierte Kommunikationsinhalte. Vollautomatische integrierte Systeme chiffrieren Telex-, Telefaxmeldungen oder Computerdaten, wählen die geeignete internationale Übermittlungsrouten und versenden den chiffrierten Inhalt an den richtigen Empfänger – alles völlig selbständig, zuverlässig und vor allem sicher.



Strategen lassen sich nicht in die Karten gucken.

Das Militär – Armee, Luftwaffe, Marine – sorgt für die Verteidigung eines Staates. Seine Einsatzbereitschaft, in Friedenszeiten eingeübt, muss jederzeit für den Ernstfall verfügbar sein.

Der Erfolg militärischer Operationen steht und fällt mit dem Funktionieren der Kommunikation. Truppenverbände müssen während der Vorbereitung und des Ablaufs von Operationen rechtzeitig ihre Befehle



erhalten, zugleich haben jedoch die Absichten dem Gegner verborgen zu bleiben. Das ist das Problem. Den Militärs stehen heute modernste elektronische Kommunikationsmittel zur Verfügung – doch der Gegenseite ebenfalls. Weil aber kein Funknetz und keine Richtstrahlverbindung abhörsicher ist, müssen es die übermittelten Inhalte sein. Crypto hat die Lösung.

Die militärischen Ansprüche an eine sichere und abgesicherte Kommunikation sind besonders hoch. Funkempfangs- und -sendegeräte zum Beispiel müssen vielfältigen Störquellen und harten Einsatzbedingungen gewachsen sein (Störsender, Frequenzschwankungen, elektromagnetischer Impuls, Kälte, Hitze, Nässe u.a.m.).

Crypto entwickelt und produziert Geräte für die gesicherte Kommunikation in komplexen integrierten Führungssystemen, die höchste militärische Normen erfüllen, von der einfachen Telefonverbindung bis zu C³I-Systemen (Command, Control, Communication, Intelligence).



Das Chiffrieren haben wir nicht erfunden. Aber wir perfektionieren es laufend.

Die Entwicklung von Kommunikationstechnik und Mikroelektronik ist in vollem Gang. Die Übermittlung und Verarbeitung der Information wird noch schneller, besser und flexibler werden. Für uns ist selbstverständlich, dass die Verschlüsselungstechnik damit Schritt halten muss.

Rund 20 Prozent aller Crypto-Mitarbeiterinnen und -Mitarbeiter arbeiten in Forschung und Entwicklung:



Mathematiker setzen neueste Erkenntnisse in Chiffrier-Algorithmen um; Entwicklungsingenieure entwerfen Geräte aus modernsten Komponenten und konzipieren damit vollständige, gesicherte Kommunikationssysteme; Testingenieure prüfen Geräte nach neusten Kriterien und Standards. Wichtige Anregungen kommen auch aus der täglichen Kommunikationspraxis unserer Kunden. Ihre Ansprüche zu erfüllen, ist für Crypto die wichtigste Aufgabe.

Für gleichbleibend hohe Fertigungs- und Funktionsqualität der Crypto-Chiffriergeräte bürgt das SQS-Zertifikat, das Crypto als einem der ersten schweizerischen Unternehmen schon 1985 zugesprochen worden ist. Das periodisch überprüfte SQS-Zertifikat entspricht den internationalen Normen ISO 9001/EN 29001 bzw. dem NATO-Standard AQAP-1. Gerätetests bei Crypto folgen den strengsten internationalen Prüfprozeduren (MIL-STD-810, IEC 529, IEC 68-2-XX u.a.).



Den Umgang mit Geheimnissen kann man lernen. Von uns.

Das bestgebaute Chiffriersystem ist nur so gut wie die Menschen, von denen es eingerichtet, bedient und gewartet wird. Crypto bietet ihren Kunden in aller Welt umfassende technische und logistische Unterstützung für das einwandfreie Funktionieren der Geräte und Anlagen.

Damit die ausgeklügelte Technik ihre Aufgabe erfüllen kann, legt Crypto grossen Wert auf gründliche



Ausbildung und Schulung der Benutzer und der Techniker. Im unternehmenseigenen Ausbildungszentrum vermitteln mehrsprachige Instrukturen nebst praxisgerechtem Umgang mit den Kommunikationssystemen auch Grundlagenkurse in Kryptologie, Schlüsselverwaltung (Key Management) und moderner Elektronik.

Zur Dienstleistungspalette von Crypto gehören: sorgfältiges Abklären der Sicherheitsbedürfnisse beim Kunden, kompetente Beratung in allen technischen und verschlüsselungstechnischen Fragen, Planen und Installieren schlüsselfertiger Systeme, Bereitstellen durchdachter mehrstufiger Wartungskonzepte, schnelles Liefern von Ersatzteilen, Instruieren und Schulen von Wartungspersonal sowie Durchführen von Reparaturen und Unterhaltsarbeiten durch Crypto-Spezialisten vor Ort.

Früher war manches anders. Auch die Kryptologie.

Die Ägypter und die Sumerer taten es, später die Spartaner und die Römer: Nachrichten so verschleiern, dass unbefugte Leser im dunkeln tappten. Im 16. Jahrhundert wurde in Italien eine Verschlüsselungsscheibe erfunden und im 18. Jahrhundert in Schweden eine raffinierte Chiffriertrommel.

Mit den modernen Kommunikationsmitteln im 20. Jahrhundert wuchsen jedoch die Ansprüche an



die Chiffriertechnik sprunghaft. 1920 entwickelte Boris Hagelin ein elektromechanisches Chiffriergesät, später eine Verschlüsselungsmaschine, von der im Krieg über 140 000 Exemplare durch die USA eingesetzt wurden. 1952 gründete Hagelin in Zug die Crypto AG. Und damit begann die Neuzeit der Kryptologie.

Chiffrieren heisst, eine Botschaft (verständlicher Klartext) mit Hilfe eines Chiffrierschlüssels in ein Chiffrat (unverständliche Zeichenfolge) umzuwandeln.

Im cryptoeigenen Museum in Zug sind die technischen Meilensteine historischer und neuzeitlicher Chiffrierverfahren einträchtig versammelt.



HAGELIN-CRYPTOS

CRYPTO AG

Postfach 474
CH-6301 Zug/Schweiz
Telefon +41 42/44 77 22
Telefax +41 42/41 22 72
Telex 868 702 cry ch

Crypto Update.

Crypto Update.



CRYPTO AG

Postfach 474
CH-6301 Zug/Schweiz
Telefon +41 42/44 77 22
Telefax +41 42/41 22 72
Telex 868 702 cry ch

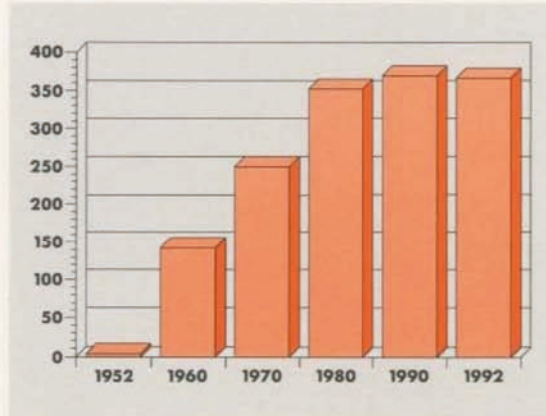


CRYPTO AG

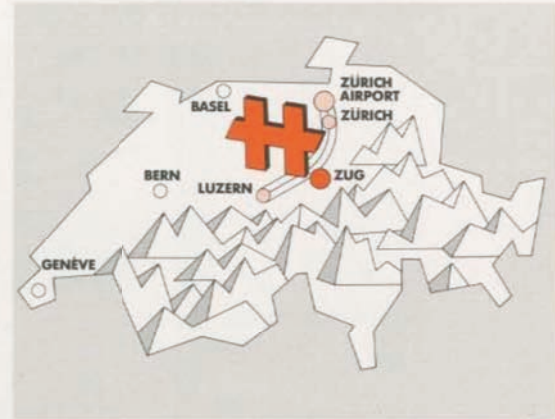
Ein Fünftel von Crypto arbeitet schon für morgen.

Crypto ist ihren Kunden weltweit nahe.

Die Mitarbeiterzahl von Crypto.

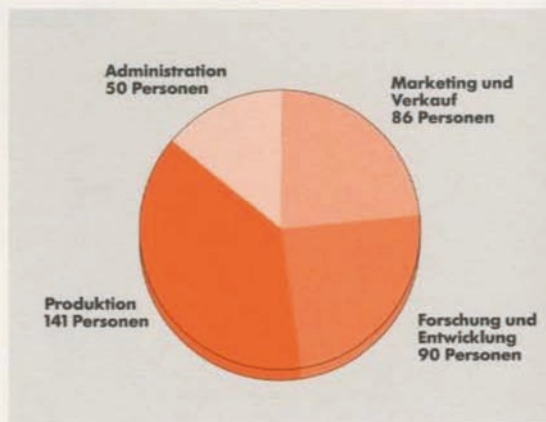


Crypto ist in der Mitte der Schweiz.



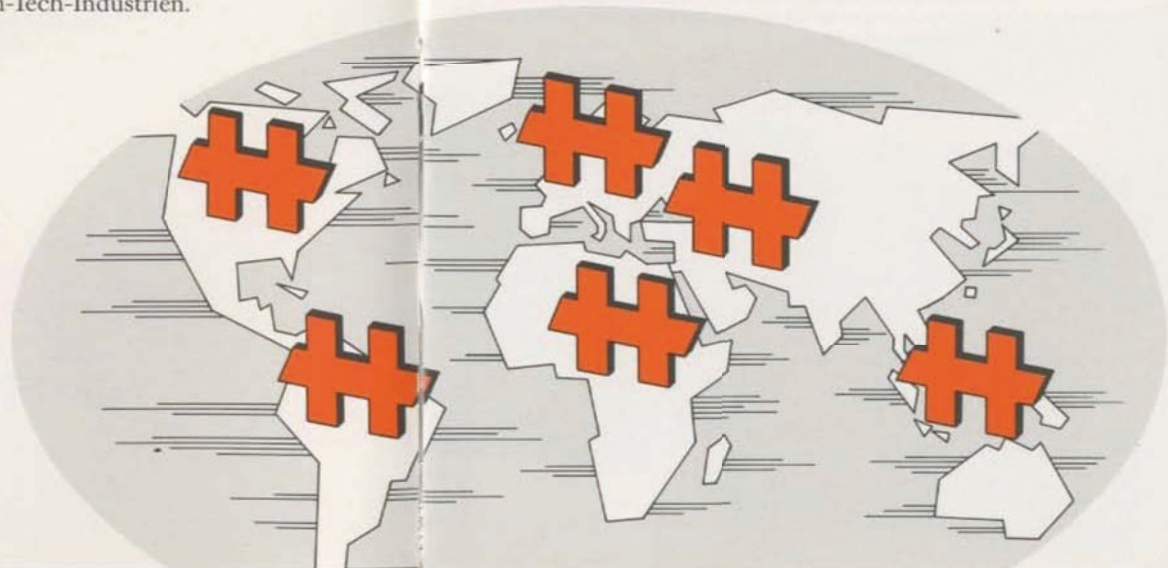
Die gute Infrastruktur von Zug und die Nähe des interkontinentalen Flughafens Zürich ermöglichen Crypto ständigen Kontakt zu den Kunden in aller Welt und zu den eigenen Niederlassungen.

Der Einsatz der Crypto-Mitarbeiter.



Seit ihrer Gründung 1952 ist Crypto kontinuierlich gewachsen. Beheimatet in Zug, im Herzen der Schweiz, kann Crypto sich auf Mitarbeiterinnen und Mitarbeiter stützen, denen Sorgfalt, Gewissenhaftigkeit und Kompetenz noch besonders wichtig sind. Zug ist ein attraktiver Produktionsstandort für Handel und High-Tech-Industrien.

Crypto ist auf allen Kontinenten präsent.



**Crypto hat den Funkverkehr
abhörsicher gemacht.**

**Crypto kann jede Kommuni-
kation sicher verschlüsseln.**

**Sicherheit in kleinen oder grossen
Funknetzen: RS-3400 von Crypto.**



Das modulare Konzept des Systems RS-3400 schützt Übermittlungsinhalte sowohl in kleinen Funknetzen zwischen einzelnen Stationen wie auch in grossen integrierten Netzen, die über eine Zentrale mit anderen Funknetzanschlüssen, Satelliten-Links und Einspeisungsmöglichkeit für Telefonverbindungen verfügen. Die Funkverbindung kann konventionell (unverschlüsselt) erfolgen oder in digitalisierter chiffrierter Form, für Sprechverkehr oder Datenübermittlung über dasselbe Verschlüsselungsmodul.

■ **Sprachverschlüsselung für geschützten
Funkverkehr: CRYPTOCOM® HC-265.**
Für mobile oder stationäre HF-Funkgeräte, auch für
VHF/UHF-Netze geeignet.

■ **Mehrkanal-Chiffriergerät: CRYPTOPLEX® HC-865.**
Chiffriert Signale von Multiplexergeräten mit mehreren
Millionen Bit pro Sekunde.

■ **Digitales Sprachchiffriergerät für Duplex-
Telefonkommunikation: CRYPTOVOX® HC-3300.**
Hohe Sicherheit und hervorragende Sprachqualität auch bei
schlechten Verbindungen.

VOICE

CRYPTOCOM®
Telefon- und Funkchiffrierung.

CRYPTOVOX®
Digitale Sprachverschlüsselung.

FACSIMILE

CRYPTOFAX®
Digitale Telefaxchiffrierung.

TEXT

CRYPTOMATIC®
Universelle Textchiffriergeräte.

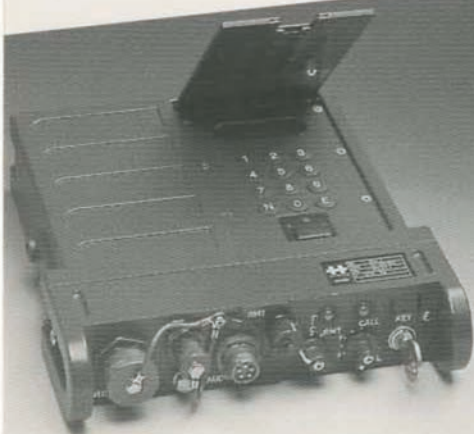
CRYPTROL®
On-line-Textverschlüsselung.

DATA

CRYPTRONIC®
Datenverschlüsselungsgeräte.

MULTICHANNEL

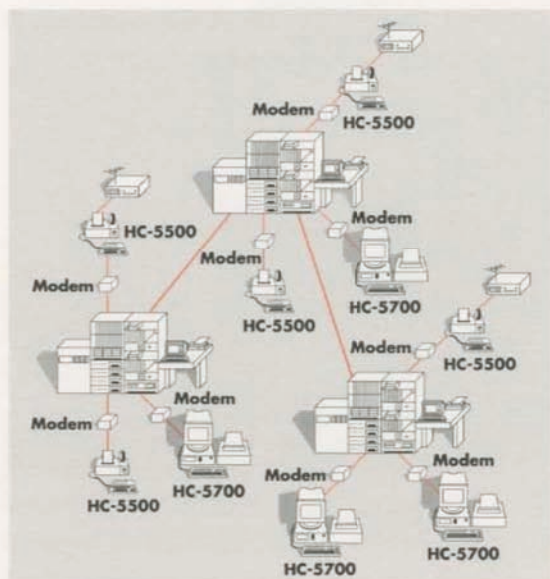
CRYPTOPLEX®
Digitale Mehrkanalchiffrierung.



Crypto macht Kommunikationsnetze systematisch sicher.

Crypto bietet Geräte und Systeme mit Know-how.

System CETUS von Crypto.



Das System CETUS zum Beispiel, mit seiner automatischen Verschlüsselung, der Meldungsvermittlung und der selbständigen Wahl der Funk-, Radio- oder Telefon-Übermittlungsstrecke schafft Sicherheit rund um die Uhr, an jedem Ort der Welt.

■ **Digitales Desktopgerät für chiffrierten Telefax-Verkehr: CRYPTO FAX® HC-4400.**

Mit allen CCITT-Telefaxstandards voll kompatibel und von hohem Bedienungskomfort.

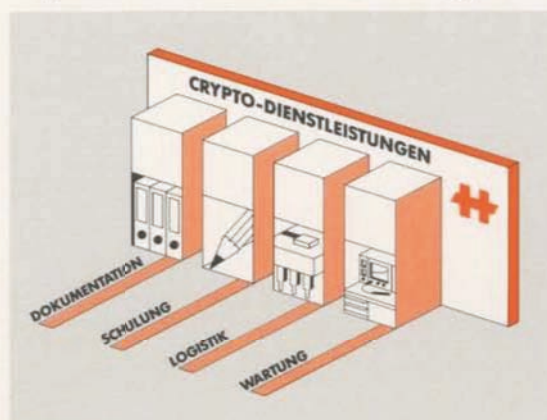
■ **Desktopterminal für chiffrierte Textübertragung: CRYPTOMATIC® HC-5700/5750.**

Mit weiteren Komponenten ausbaubar zum integrierten Kommunikationssystem.

■ **Chiffriergerät für die Datenkommunikation: CRYPTRONIC® HC-7400.**

Hohe Datensicherheit zwischen Endgeräten und Vermittlungsrechnern.

Zu jedem Gerät: Know-how von Crypto.



Das vierstufige Bedienungs- und Unterhaltskonzept von Crypto erfüllt die Anforderungen von staatlichen Stellen:

- Stufe I Bedienung und Wartung im Einsatz.
- Stufe II Reparatur eines defekten Geräts durch Modultausch.
- Stufe III Fehlerlokalisierung und Reparatur bis zur einzelnen Komponente durch Spezialisten.
- Stufe IV Reparatur durch Crypto.

Für Stufe I werden die Benutzer durch Crypto ausgebildet und geschult. Für Stufe II und III erhalten die Techniker des Kunden die erforderlichen Kenntnisse in Spezialkursen bei Crypto.

