Kontrollzentrum des **Satellitenaufklärungsystems Onyx** in Zimmerwald: Ein Ohr ins Weltall. YOSHIKO KUSANO/KEYSTONE

Die Sprache der Agenten

Sind Nachrichten **nach mathematischen Vorschriften verschlüsselt,** ist es unmöglich, sie zu knacken

Der Schweizer Nachrichtendienst hat ein Fax des ägyptischen Aussenministeriums abgefangen. Das wirft auch technische Fragen auf: Wie werden Daten verschlüsselt und wie sicher sind elektronisch übermittelte Inhalte?

MARTIN ARNOLD

Die Affäre um die «SonntagsBlick»-Veröffentlichung eines brisanten Faxes der ägyptischen Diplomatie über US-amerikanische Geheimgefängnisse in Europa wirft auch ein Schlaglicht auf das Satellitenaufklärungssystem Onyx. Von Zimmerwald und Heimenschwand im Kanton Bern und von Leuk im Kanton Wallis horcht Onyx in Richtung Satelliten und fängt elektromagnetische Wellen ein.

Satelliten senden ihre Wellen auf ein breites Gebiet, sonst könnten Fernsehprogramme gar nicht überall auf einem Kontinent empfangen werden. Mittels Stichwörtern filtert ein Computerprogramm brisante Botschaften heraus. Das ist ein einfacher Vorgang – wenn die Botschaft unverschlüsselt ist. Dies scheint beim fraglichen Fax zwischen den ägyptischen Behörden in Kairo und London der Fall gewesen zu sein.

Sollte die Botschaft entgegen den bisherigen Meldungen doch verschlüsselt gewesen sein, gibt es zwei Möglichkeiten der Enttarnung. Entweder war sie schlecht verschlüsselt oder jemand in der Schweiz kannte den Schlüssel zur Dechiffrierung. «Ein gut verschlüsselter Text ist nicht zu knacken», sagt Ueli Maurer, Informatikprofessor an der ETH Zürich und Experte für Kryptografie. Er arbeitet mit seinem Team an sicheren Verschlüsselungsmethoden.

Ein Geschäft voller Geheimnisse

Roman Weissen, Mediensprecher beim Strategischen Nachrichtendienst, gibt sich zugeknöpft. Er will weder bestätigen, noch dementieren, ob die Nachricht verschlüsselt war. Dem Nachrichtendienst ist die Sache unangenehm, denn er lebt von der Geheimhaltung und dem Austausch von Informationen.

Die Geheimhaltung garantieren Chiffriergeräte von Firmen wie Crypto AG oder ihrer Konkurrentin Omnisec AG. Sie verändern – chiffrieren – Informationen so, dass sie niemand mehr lesen kann, ausser Berechtigten, die den Schlüssel kennen. Giuliano Otth, geschäftsführender Direktor der Crypto AG, spricht von einer «umfassenden Sicherheitsarchitektur».

Neben Algorithmen – genauen Vorschriften zur Lösung eines Problems – kommen Methoden zum Einsatz, die Information zusätzlich vor Zugriffen schützen. Technische Massnahmen sorgen dafür, dass die Chiffriergeräte keine elektromagnetischen Wellen abstrahlen, die wiederum in Echttext verwandelt werden könnten. Details will Otth nicht bekannt geben: «Unsere Kunden erwarten Diskretion.» Zu den Klienten der Zuger Firma gehören Regierungsstellen und ihre Organisationen sowie Banken und Finanzunternehmen.

Für das Versenden einer chiffrierten Botschaft braucht es im Prinzip einen Schlüssel (den Versender einer verschlüsselten Botschaft) und ein Schloss (denjenigen, der die Information entschlüsselt). Mit der Verwendung von Hieroglyphen setzten bereits die alten Ägypter auf Kryptografie – die Wissenschaft der Verschlüsselung. Doch erst im 20. Jahrhundert erlangte diese grosse Bedeutung.

Im Zweiten Weltkrieg setzten beide Seiten neue, auch elektromechanische Systeme ein. Danach begann das Zeitalter der mathematischen Kryptografie. Mit dem Data Encryption Standart – einem Algorithmus – entwickelte IBM ein System, das auch sichere Bankdienstleistungen ermöglicht.

Erst vor wenigen Jahren wurde das Problem der Schlüsselübergabe gelöst. Früher musste der Schlüssel zwischen den Kommunikationspartnern etwa über einen vertrauenswürdigen Kurier ausgetauscht werden. Heute benutzen sie einen öffentlichen und einen privaten Schlüssel: der öffentliche wird zur Verschlüsselung verwendet und ist oft mehren Personen bekannt; der private zur Entschlüsselung muss geheim gehalten werden.

Verschlüsselung per Zufall

Wer chiffrierte Texte entschlüsseln will, bedient sich der Kryptoanalyse. Als die Menschen noch von Hand verschlüsselten, mussten sie einfache Algorithmen anwenden, damit sie die Botschaft auch wieder lesen konnten. Diese Verfahren folgen bestimmten Gesetzmässigkeiten, die heute ein Computer in Sekunden knacken kann. Derzeit in der Verschlüsselung verwendete Algorithmen sind sehr kompliziert.

Ein häufig verwendeter privater Schlüssel ist eine per Zufallsgenerator ermittelte Bit-Folge; ein typischer Schlüssel hat 128 Bits. Die Anzahl möglicher Schlüssel (vergleichbar mit der Anzahl Kombinationen eines Zahlenschlosses) ist 2 hoch 128: eine Zahl mit etwa 40 Stellen. Selbst die schnellsten Computer benötigten Jahrtausende, um alle Möglichkeiten eines solchen Schlüssels zu berechnen .

Die moderne Kryptografie verfolgt vier Ziele: Sie soll verhindern, dass Dritte eine Nachricht lesen können; der Empfänger soll feststellen können, ob der Inhalt seit der Übertragung gelesen wurde; der Empfänger soll den Absender identifizieren, und Letzterer gegebenenfalls das Versenden bestreiten können.

Ein Angreifer probiert wohl zuerst alle möglichen Schlüssel durch. Wenn er mehrere verschiedene, gleich verschlüsselte Texte hat, kann er vergleichen, um eine Entschlüsselung zu finden. Er kann auch nach mehreren markanten Wörtern fahnden, die wahrscheinlich vorkommen. Diese Methode wird dann angewendet, wenn der ungefähre Inhalt erahnt wird.

Privatsphäre schützen

Der Angreifer könnte aber auch eine Finte schlagen wie die britische Royal Navy im Zweiten Weltkrieg. Gezielt verlegte sie immer wieder Minenfelder. Die deutschen Aufklärer übermittelten jeweils die neuen Daten, bis die Briten den Schlüssel für den deutschen Informationsaustausch in der Hand hatten. Heute geht es vor allem um den Schutz der Privatsphäre im Zeitalter des elektronischen Datenaustausches. Das macht die Kryptografie notwendiger denn je.

Latsis-Preis an ETH-Physiker

BERN Der Ingenieurwissenschaftler Patrick Jenny von der ETH Zürich hat gestern Donnerstag im Berner Rathaus den mit 100 000 Franken dotierten Latsis-Preis 2005 entgegengenommen. Diese Auszeichnung gilt als der Nobelpreis der Schweiz.

Der 40-jährige Patrick Jenny wird für die Entwicklung der computergestützten Modellierung komplexer Strömungssysteme in Natur und Technik ausgezeichnet. Seine Arbeiten seien bahnbrechend, heisst es in einer Mitteilung des Schweizerischen Nationalfonds, der die Grundlagenforschung fördert. Mit Jennys Methode lässt sich zum Beispiel die Rentabilität von Ölbohrungen errechnen oder feststellen, wie Abwässer aus einer Kanalisation in einen See fliessen, aber auch, wie Schadstoffe bei der Verbrennung von Gasgemischen reduziert werden können.

Patrick Jenny doktorierte an der ETH Zürich und forschte als Postdoc an der Cornell-Universität in den USA. Danach arbeitete er dreieinhalb Jahre bei einem US-amerikanischen Öl-Konzern, wo er in der Forschungsabteilung Ölreservoir-

100 000 Franken für **Patrick Jenny**, ETH Zürich. ZVG

Simulationen entwickelte. Eine Förderungsprofessur des Schweizerischen Nationalfonds brachte ihn 2003 zurück in die Schweiz – ans Institut für Fluiddynamik der ETH Zürich.

Der Nationale Latsis-Preis ist eine der wichtigsten wissenschaftlichen Auszeichnungen der Schweiz. Er wird jedes Jahr vom Schweizerischen Nationalfonds im Auftrag der Genfer Latsis-Stiftung verliehen. Die mit 100 000 Franken verknüpfte Auszeichnung honoriert besondere wissenschaftliche Leistungen eines Forschers oder einer Forscherin im Alter von höchstens 40 Jahren in der Schweiz. (sda)

ERFORSCHT

Rasend schneller Pulsar

ASTRONOMIE Ein Neutronenstern im Sternbild Schütze stellt mit 716 Umdrehungen pro Sekunde einen neuen Geschwindigkeitsrekord auf. Dies hat das Fachblatt «Science» gestern online veröffentlicht. Der Stern hat einen Durchmesser von nur 20 Kilometern und ist der schnellste bekannte Pulsar. Pulsare nennen Astronomen Neutronensterne, die wie ein kosmisches Leuchtfeuer in kurzen, sehr regelmässigen Abständen aufleuchten. (sda)

Leuchtende Schweine

GENTECHNIK Taiwanische Forscher haben drei Schweine gezüchtet, die im Dunkeln grün leuchten. Dafür haben sie ein fluoreszierendes Protein in den Zellkern eines Schweineembryos injiziert, das sie aus Quallen gewonnen hatten. Den Wissenschaftlern sei ein «wichtiger Fortschritt» in der Stammzellforschung gelungen, weil Schweine zu den Tieren zählten, die dem Menschen besonders nahe seien, erklärte Wu Shinn Chih von der Nationalen Universität Taiwans, der das Forscherteam leitete. (sda)

Gicht neu behandeln

MEDIZIN Forscher der Universität Lausanne haben in einer im Fachblatt «Nature» publizierten Studie zwei Moleküle identifiziert, die für die Gichtentzündungen mitverantwortlich sind. Diese Moleküle könnten nun zum Ziel neuer medikamentöser Behandlungen werden, wie die Universität Lausanne diese Woche mitteilte. (sda)

WISSENSTIPP

Viel Lärm um den Lärm

Knatternde Autos, Krach am Arbeitsplatz: Vermutlich kann niemand von sich behaupten, er habe noch nie unter Lärm gelitten. Und so gilt die Bekämpfung von Lärm unter Umweltschützern als eines der wichtigsten Anliegen – dem nun auch das Forum für Allgemeine Ökologie der Universität Bern gerecht werden will.

Für eine öffentliche Vortragsreihe hat es Forscher und Praktiker eingeladen, die das Thema Lärm aus unterschiedlicher Perspektive beleuchten. Dabei geht es um Fragen, wie Lärm akustisch definiert wird oder welches die rechtlichen Aspekte des Fluglärmstreits mit Deutschland sind. Am **Dienstag, den 17. Januar,** spricht Rainer Guski von der Ruhr-Universität über die Auswirkungen des Lärms auf die menschliche Psyche. **18.15 Uhr,** Hauptgebäude der Universität, **Hochschulstrasse 4.** (pid/pim)

ABTEILUNG FÜR LEBENSMITTELKUNDE

Das Brot der Träume

Einst gab es ein Land, in dem «die Mauern aus Barschen, Lachsen und Heringen gemacht sind, das Dachwerk besteht aus Stören und das Dach selbst aus Schinken und die Holme aus Würsten», alle Kornfelder sind gesäumt von «Stücken gebratenen Fleisches», und «es ist die hochheilige Wahrheit, dass in dieser glückseligen Gegend ein Fluss voll Wein fliesst», und zwar zur Hälfte roter und weisser.

•

So berichtet ein französisches Märchen aus dem Reich der stets gedeckten Tische. Im Schlaraffenland, dieser volkstümlichen Version von Eden, schlug man sich aber nicht nur den Bauch voll: Es gab hier auch freie und glückliche Liebe, prachtvolle Kleider und ewige Jugend. Auf eine reine Magenfrage reduzierte sich die Utopie im 16. und 17. Jahrhundert: Während die Tafeln der Fürsten und Kardinäle unter der Last der Gelage ächzten, wurde die Ernährung breiter Schichten in Europa immer prekärer. Das machte den Traum der vollen Bäuche so beliebt – er narkotisierte den Hunger.

•

Es gibt kaum etwas, aus dem die Menschen damals kein Brot gemacht hätten. Wassernüsse, Feldrüben, Vogelbeeren, Ulmenblätter, Farnwurzeln, Saubohnen – gekocht, getrocknet, gestampft. Nicht aus Lust auf Abwechslung, sondern aus Not. Von Brot im heutigen Sinn konnten viele nur träumen; sie assen etwas, «das schwarz wie Kohle oder aschgrau wie die Haut eines Esels ist und von einem Gemisch, dass nicht einmal die Strasse es verdauen möchte». So nannte es ein italienischer Chronist um 1600.

Wen der Hunger plagt, der sorgt sich nicht, ob im Brot verdorbenes

Traum gegen den Hunger. Brueghels «Schlaraffenland», 1567. ADI

Korn sein könnte, schädliches oder giftiges Gewächs. Mutterkorn etwa, ein Pilz, der auf dem Roggen wächst und lange schwarze Krümel bildet. Diese enthalten Alkaloide, Gifte, die zu Darmkrämpfen führen, zu Durchblutungsstörungen, zum Absterben der Finger, zu Sinnestäuschungen und auch zum Tod. Es gab im vorindustriellen Europa immer wieder Mutterkornvergiftungen, durch die ganze Dörfer und Städte ins Delirium fielen. Und oft kam das Gift mit Absicht ins Brot. Denn der Rausch betäubte – bei aller toxischen Gefahr – das Nagen im Bauch, und so fanden die Armen und Ausgezehrten im Brot den Weg zu unerwarteten Paradiesen. Der Historiker Piero Camporesi hat in seinem Buch über das «Brot der Träume» eine Welt gezeichnet, wo der Hunger so normal war wie die Halluzination und «die Geisterseherei nicht der Kontrolle durch eine Liturgie unterlag».

•

Von einem «neuen Bewusstsein der Wirklichkeit» sprach jener Chemiker, der 1943 in einem Basler Labor einen Stoff namens Lysergsäurediäthylamid entdeckte. Albert Hofmann heisst der Chemiker, LSD das Kürzel der Substanz. Sie ist ein synthetischer Abkömmling des Mutterkorngifts.

Daniel Di Falco