Verschlüsselte Botschaften reizen zum Knacken

Autor(en): **Gassmann, Fritz / Adrion, Denise**

Objekttyp: **Article**

Zeitschrift: **Bulletin.ch : Fachzeitschrift und Verbandsinformationen von Electrosuisse, VSE = revue spécialisée et informations des associations Electrosuisse, AES**

Band (Jahr): **95 (2004)**

Heft 24-25

PDF erstellt am: **13.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-858024

Verschlüsselte Botschaften reizen zum Knacken

Von Herodot zum Onlinebanking – Verschlüsselungstechniken im Laufe von 2500 Jahren

Die Versuche, Botschaften für ungewünschte Empfänger unlesbar zu machen, sind so alt wie die Menschheit. Kamen früher vor allem Politiker und Generäle mit der Kryptografie in Kontakt, ist dies im Internet-Zeitalter praktisch jedermann.

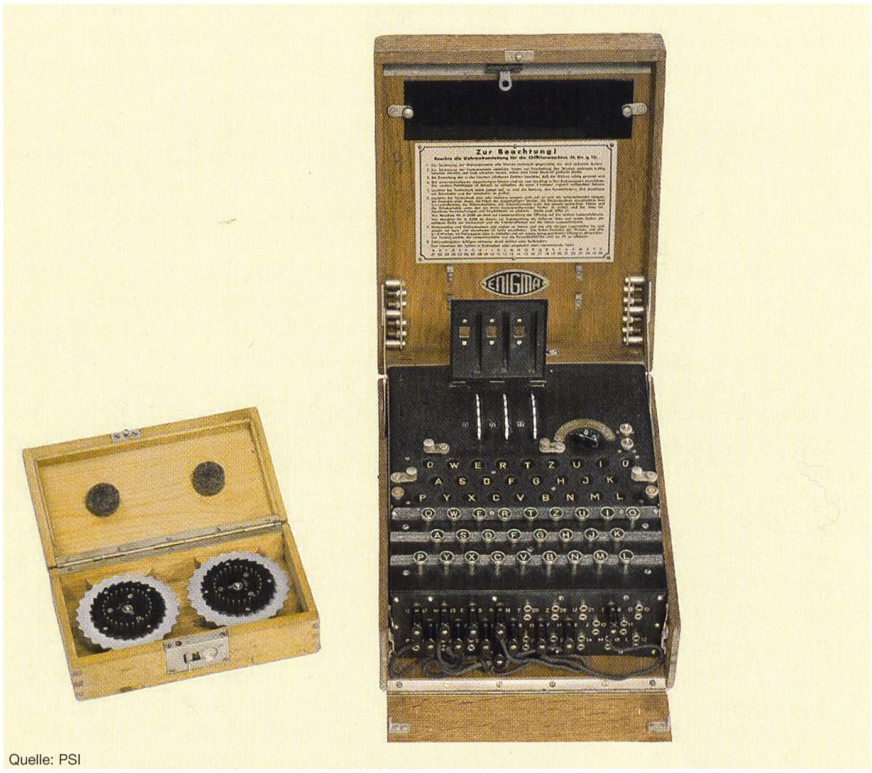
Der Begriff **Kryptografie** stammt aus dem griechischen «kryptein» (verbergen) und «graphé» (Schriftstück). Er beschreibt die Beschäftigung mit Verfahren, die sich mit der Ver- und Entschlüsselung von Informationen auseinander setzen. In der Literatur wird die Entschlüsselung auch häufig als Kryptoanalyse bezeichnet.

Meist unbewusst kommt heute fast jede Person im täglichen Leben mit Verschlüsselung in Berührung. Man denke zum Beispiel an Onlinebanking, Kreditkartenzahlungen und Bankautomaten.

Fritz Gassmann und Denise Adrion

Schon früh wurde mit verschiedensten Methoden der Kryptografie experimentiert. Das erste schriftliche Zeugnis lieferte Herodot im 5. Jahrhundert v. Chr., indem er zwei bekannte Verfahren beschrieb, wie man Nachrichten verbergen kann.

Bei einem dieser Verfahren liess man einem Boten die Haare abrasieren und brannte die Nachricht in die Kopfhaut ein. Dann wartete man, bis die Haare nachgewachsen waren und schickte den Boten zum Empfänger. Dieser rasierte die Haare wieder ab und erhielt so die geheime Botschaft. Weitere bekannte Figuren der Geschichte wie Cäsar und Maria Stuart bedienten sich der Kryptografie. Zwischen den Entwicklern von Verschlüsselungsalgorithmen und den Entschlüsslern ist bis heute eine Art Ko-Evolution im Gange: Wenn ein neuer Verschlüsselungsalgorithmus entdeckt wird, hat der Entschlüssler das Nachsehen. Sobald er jedoch die Verschlüsselung geknackt hat, ist der Vorteil auf seiner Seite.



Quelle: PSI

Während des Zweiten Weltkrieges wurden 100 000 bis 200 000 Enigma-Maschinen gebaut

Ständig ändernde Buchstaben

Eine entscheidende Station in der Entwicklung der Kryptografie bildet das monoalphabetische Substitutionsverfahren, bei dem ein Buchstabe einer Nachricht durch einen bestimmten Buchstaben oder ein bestimmtes Zeichen ersetzt wird. Doch durch die Analyse spezifischer Häufigkeiten bestimmter Buchstaben in der jeweiligen Sprache kann dieses Verfahren entschlüsselt werden (unser Tipp: Lösen Sie das Rätsel auf Seite 34). Der nächste grosse Schritt wurde durch die Entwicklung der polyalphabetischen Substitution gemacht, bei der sich der Buchstabe, der einen anderen verschlüsselt, ständig ändern kann.

Die geknackte Enigma

Unter den Spezialmaschinen, die zur routinemässigen Chiffrierung und Dechiffrierung erfunden und über Jahre und Jahrzehnte weiterentwickelt wurden, ist die Enigma wahrscheinlich weltweit die bekannteste. Mit ihr wurden während des Zweiten Weltkriegs der grösste Teil der Funksprüche der deutschen Wehrmacht und Marine vor dem Absenden verschlüs-

Definition	Beispiel (mit kleinen Zahlen)
Wähle zufällig zwei grosse Primzahlen p, q	p = 5, q = 17
Berechne n = pq	n = pq = 5*17 = 85
Wähle eine relativ kleine ungerade positive Zahl e, die zu φ(n) = (p-1)(q-1) teilerfremd ist	φ(n) = (p-1)(q-1) = 4*16 = 64, dazu teilerfremd beispielsweise e = 11
Berechne d aus der Gleichung *ed* mod φ(n) = 1, (dies gelingt mit dem erweiterten Euklidischen Algorithmus)	*d* = -29 mod(64) = 35
Gib das Paar (*e,n*) bekannt als **öffentlichen Schlüssel**	öffentlicher Schlüssel: (11,85)
Halte das Paar (*d,n*) geheim als **geheimen Schlüssel**	geheimer Schlüssel: (35,85)

Tabelle Schlüsselerzeugung für das RSA-Verfahren

selt und nach dem Empfang wieder entschlüsselt. Man nimmt an, dass während des Zweiten Weltkrieges 100 000 bis 200 000 Enigma-Maschinen gebaut wurden.

Die Maschine besteht aus einem Steckbrett zur Vertauschung der Buchstabenpaare, drei Walzen und einem Reflektor. Bei jeder Walze wird für eine Permutation gesorgt. Der Reflektor bewirkt, dass kein Buchstabe auf sich selbst verschlüsselt wird und dass die Enigma sich ohne Veränderung der Walzen und des Steckbretts zum Ver- und Entschlüsseln benutzen lässt. Da der Schlüssel dauernd verändert wurde, galt sie als nicht knackbar. Doch vor dem Genie Alan Turing musste selbst die Enigma kapitulieren.

Das RSA-Verfahren

In der modernen Kryptologie hat sich die RSA-Verschlüsselung, benannt nach den Entwicklern Rivest, Shamir und Adleman, als eine der sichersten und zugleich einfachsten Methoden durchgesetzt. Sie wird heute zum Beispiel im Bankwesen zur Verschlüsselung von Geheimzahlen oder bei der Verschleierung von Pay-TV-Programmen verwendet.

Wollen zwei Teilnehmer sich gegenseitig eine Nachricht senden, die der Öffentlichkeit verborgen bleiben soll, so müssen diese zuerst zwei Schlüssel festlegen, wie es in der Tabelle erklärt wird. Entscheidend an diesem Verfahren ist, dass es für einen Dritten zwar einfach ist, d zu bestimmen, wenn er e, p und q kennt, aber nahezu unmöglich, nur durch Kenntnis des öffentlichen Schlüssels (e,n) den geheimen Schlüssel (d,n) herauszufinden; dies vor allem, wenn die Primzahlen p und q gross gewählt sind.

Im folgenden Beispiel will Thomas eine geheime Nachricht an Anna übermitteln:

1. Zuerst erzeugt Anna einen öffentlichen Schlüssel (e,n), den sie via Internet an Thomas übergibt, um Mitteilungen an sie zu verschlüsseln. Dann berechnet Anna mit dem Euklidischen Algorithmus den geheimen Schlüssel (d,n).
2. Thomas verschlüsselt nun die in Segmente B_i unterteilte Botschaft mit Hilfe des öffentlichen Schlüssels (e,n) folgendermassen: $K_i = (B_i)^e \bmod(n)$
3. Anna entschlüsselt die Botschaft mit Hilfe des geheimen Schlüssels (d,n) folgendermassen: $B_i = (K_i)^d \bmod(n)$. Es kann mathematisch bewiesen werden, dass $B_i = [(B_i)^e \bmod(n)]^d \bmod(n)$.

Ist RSA zu knacken?

Wie man sieht, ist eine nach RSA verschlüsselte Nachricht nur mit Hilfe des Schlüssels d zu knacken. Die Variable d lässt sich aber nur mit den beiden Primzahlen p und q errechnen. Daher liegt das Grundproblem darin, die bekannte Zahl n in ein Produkt zweier Primzahlen zu zerlegen. Dies wird bei Verwendung grosser Primzahlen fast unmöglich. Kryptologen empfehlen daher, für n Zahlen mit mindestens 512 Bits (das entspricht 155 Stellen) zu benutzen. Bei Zahlen dieser Grössenordnung sind auch modernste Computeralgebra-Programme nicht in der Lage, deren Produkt zu faktorisieren.

100% sicher dank Quanten

Den nächsten Evolutionsschritt bringt möglicherweise der Quantencomputer, für den die Zerlegung selbst grosser Primzahlen ein Leichtes sein könnte. Eine vielleicht mögliche Antwort der Verschlüssler würde ebenfalls auf der Quantenmechanik beruhen: Benutzt würde ein eigenartiger Zusammenhang zwischen zwei geeignet erzeugten Photonen (Lichtquellen). Deren Polarisation bleibt selbst über grosse Distanzen korreliert. Man

Rätsel: Warum Maria Stuart hingerichtet wurde

Im 16. Jahrhundert leitete Thomas Phelippe eine Chiffrierschule in London. Er war einer der ersten, der statistische Analysen von Texten anfertigte. In der deutschen Sprache haben die Buchstaben folgende Häufigkeiten:

E	17%
N	10%
A, I, R, S, T	6 bis 8%
D, H, U	4 bis 5%
Rest	kleiner als 3%

FTKBT LMNTKM PNKWX HIYXK BAKXK OXKLVAENXLLXEMXG GTVAKBVAMXG. LBX EXUMX BF LXVASXAGMXG CTAKANGWXKM, SN XBGXK SXBM, WT XGZETGW IKHMXLMTGMBLVA PNKWX. TNYZXPTVALXG BG YKTGDKXBVA, PNKWX LBX DTMAHEHLVA XKSHZXG. TEL LBX GTVA LVAHMMETGW SNKNXVDDTF, OXKLNVAMX LBX, WTL ETGW SN KXDTMAHEBLBXKXG. GTVA FXAKXKXG TYYTXKXG, AHVASXBMXG NGW DHFIEHMMXG FNLL LBX TUXK SN BAKXK XGZEBLVAXG LVAPXLMXK XEBLTUXMA YEBXAXG. WBXLX KXZBXKMX WTL IKHMXLMTGMBLVAX XGZETGW. LBX OXKATYMXM FTKBT NGW ATXEM LBX GXNGSXAG CTAKX ETGZ ZXYTGZXG. PTXAKXGW WBXLXK SXBM DHFFNGBSBXKM FTKBT NXUXK OXKLVAENXLLXEMX GTVAKBVAMXG FBM WXF DTMAHEBLVAXG PBWXKLMTGW. WBX GTVAKBVAMXG PXKWXG TUXK TUZXYTGZXG NGW XGMLVAENXLLXEM – NGMXK TGWXKXF TNVA XBG UKBXY, BG WXF XL NF XBG FHKWDHFIEHMM ZXZXG XEBLTUXMA ZXAM. FTKBT PBKW OXKNKMXBEM NGW TNY WXF LVATYHMM ABGZXKBVAMXM.

Der verschlüsselte Text steht elektronisch zur Verfügung:
www.electrosuisse.ch -> Verband -> Bulletin -> Download

spricht von «verschränkten Photonenpaaren» (engl. entangled photon pairs). Gemäss der heutigen Auffassung der Quantentheorie sollte diese Verschlüsselung definitiv nicht zu knacken sein.

Angaben zu den Autoren

Fritz Gassmann, Dr. sc. nat., forscht als Senior Scientist am Paul Scherrer Institut. Er beschäftigt sich mit der dynamischen Simulation nichlinearer Systeme. Eine Anwendung ist der globale Klimawechsel.
Paul Scherrer Institut, 5232 Villigen PSI, gassmann@psi.ch
Denise Adrion war Praktikantin am Paul Scherrer Institut.

Les messages cryptés donnent envie de les craquer

De Hérodote à l'on-line banking – les techniques de cryptage au fil de 2500 ans

Les tentatives de rendre les messages illisibles pour tous les autres que leurs destinataires sont aussi anciennes que l'humanité. Tandis qu'autrefois, c'étaient surtout les politiques et les généraux qui s'occupaient de cryptographie, à l'ère d'Internet, c'est pratiquement tout le monde.