



Bundesministerium
des Innern
und für Heimat

POSTANSCHRIFT Bundesministerium des Innern und für Heimat, 10557 Berlin

Mitglied des Deutschen Bundestages
Herrn Dr. Rainer Rothfuß
Platz der Republik 1
11011 Berlin

HAUSANSCHRIFT Alt-Moabit 140, 10557 Berlin

POSTANSCHRIFT 10557 Berlin

TEL +49 (0)30 18 681-11117

FAX +49 (0)30 18 681-11019

INTERNET www.bmi.bund.de

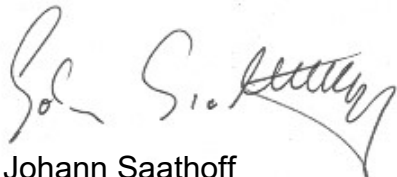
DATUM 10. September 2024

BETREFF **Schriftliche Frage Monat August 2024**
HIER Arbeitsnummer 8/457

Sehr geehrter Herr Abgeordneter,

auf die mir zur Beantwortung zugewiesene schriftliche Frage übersende ich Ihnen die beigefügte Antwort.

Mit freundlichen Grüßen
in Vertretung



Johann Saathoff

ZUSTELL- UND LIEFERANSCHRIFT Alt-Moabit 140, 10557 Berlin

VERKEHRSANBINDUNG S-Bahnhof Berlin Hauptbahnhof

Bushaltestelle Berlin Hauptbahnhof

Schriftliche Frage des Abgeordneten Dr. Rainer Rothfuß
vom 29. August 2024
(Monat August 2024, Arbeits-Nr. 8/457)

Frage

Wurde nach Kenntnis der Bundesregierung ein wesentlicher Teil der westlichen Fernmelde- und Cybersicherheitsarchitektur, insbesondere auch im Banken- und Finanzwesen, auf die in der in Mathematik unbewiesene Annahme gestützt, dass eine Primfaktorzerlegung (Faktorisierungsverfahren) einer großen Zahl nur langsam und ineffizient gelingen kann, obwohl nach meiner Ansicht gerade die Mathematik der einzige Wissenschaftsbereich ist, welcher definitive und unwiderlegbare Beweisführung pro oder contra einer These erlaubt und es daher meiner Ansicht nach mindestens unklug oder gefährlich erscheint, große Teile der Sicherheit auf eine unklare mathematische Sachlage aufgrund fehlender Beweise zu stützen, und hätte es nach Einschätzung der Bundesregierung das Bekanntwerden einer schnellen und effizienten Methode zur Primfaktorzerlegung großer Zahlen mittels bspw. des dem „Qubit“ zu Grunde liegenden geometrischen Zahlensystems, d. h. also auch ohne „Quanten“-Computer, Auswirkungen für die Integrität des gesamten westlichen Wirtschafts-, Finanz- und Kommunikationswesens, falls dieses Wissen den Weg zu Hackergruppen findet, und wenn ja, welche (www.cybersecurity.blog.aisec.fraunhofer.de/post-quanten-kryptografie/)?

Antwort

Verschlüsselungsalgorithmen bestehen in der Regel aus der Kombination eines symmetrischen Verfahrens mit einem asymmetrischen Verfahren. Asymmetrische Verfahren dienen dabei dem Austausch eines symmetrischen Schlüssels, den die Kommunikationspartner dann für die eigentliche Verschlüsselung ihrer Daten nutzen können. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt in der Technischen Richtlinie TR-02102 (https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html) unter anderem auch den Algorithmus RSA (benannt nach seinen Erfindern Ronald Rivest, Adi Shamir und Leonard Adleman), neben einer Reihe weiterer asymmetrischer Verschlüsselungsverfahren. Die Sicherheit all dieser asymmetrischer kryptografischer Verfahren basiert auf speziellen mathematischen Problemen, von denen man annimmt, dass sie sehr schwierig zu lösen sind.

Mit dem Faktorisierungsproblem, die Grundlage von RSA, beschäftigen sich seit Jahrzehnten viele exzellente Mathematiker und nach wie vor ist kein effizienter Faktorisierungsalgorithmus für so große Zahlen, wie sie bei RSA verwendet werden, bekannt. Asymmetrische Kryptographie, insbesondere RSA und Verfahren basierend auf dem diskreten Logarithmus-Problem, sind weltweit seit vielen Jahren ein zentraler Bestandteil zur Absicherung digitaler Kommunikationswege. Es ist bekannt, dass ein ausreichend starker Quantencomputer das Faktorisierungsproblem und das diskrete Logarithmus-Problem effizient lösen kann. Um dieser potentiellen Bedrohung zu begegnen, werden derzeit auf internationaler Ebene neue asymmetrische Algorithmen standardisiert. Auch die Sicherheit dieser neuen Algorithmen basiert auf mathematischen Problemen, für die die weltweite Forschungsgemeinschaft nach aktuellem Stand keine effizienten Lösungsalgorithmen kennt.