

Science & Technology Café: Kryptologie zwischen Geschichte und Zukunft der IT-Sicherheit

30.9.2026 - | Deutsche Akademie der Technikwissenschaften

Wie lassen sich Informationen sicher übermitteln? Welche Prinzipien liegen moderner Verschlüsselung zugrunde und welchen Aufgaben muss sich die IT-Sicherheit der Zukunft stellen? Diesen Fragen widmete sich das acatech Science & Technology Café „Kryptologie - von geheimen Botschaften aus der Antike zur Zukunft der IT-Sicherheit“ auf der 134. Versammlung der Gesellschaft Deutscher Naturforscher und Ärzte (GDNÄ) in Bremen.

Die Deutsche Akademie der Technikwissenschaften (acatech) lädt seit vielen Jahren im Rahmen der Versammlungen der GDNÄ zu Diskussionsveranstaltungen ein, die aktuelle und kontroverse Themen behandeln. Das Science & Technology Café ermöglicht den Teilnehmenden, wissenschaftliche Entwicklungen aus unterschiedlichen Perspektiven kennenzulernen und mit ausgewiesenen Expertinnen und Experten ins Gespräch zu kommen.

Marc-Denis Weitze aus der acatech Geschäftsstelle konzipierte und moderierte die Veranstaltung. Den historischen und methodischen Einstieg gab Carola Dahlke, Abteilungsleiterin „Informatik und Kryptologie“ im Deutschen Museum. In ihrem Impuls erläuterte sie, was unter Kryptologie zu verstehen ist und welche zentralen Methoden sich im Laufe der Zeit herausgebildet haben. Dabei schlug sie den Bogen von frühen Formen der Verschlüsselung bis hin zu maschinellen Verfahren.

Der Schlüssel zu Kryptologie, Kryptografie und Kryptoanalyse

Dabei wurde deutlich, dass Kryptologie weit mehr ist als das Verbergen geheimer Botschaften. Sie umfasst sowohl die Kryptografie – also die Entwicklung von Verfahren zur sicheren Kommunikation – als auch die Kryptoanalyse, mit der Verschlüsselungen untersucht und gegebenenfalls gebrochen werden. Anhand ausgewählter Beispiele, mitgebrachter Exponate und Entschlüsselungsaufgaben veranschaulichte Carola Dahlke, wie sich Verschlüsselungsverfahren entwickelt haben: von einfachen, per Hand anzuwendenden Methoden zu komplexen maschinellen Systemen.

Anschließend richtete acatech Mitglied Jörn Müller-Quade vom Karlsruher Institut für Technologie (KIT) den Blick auf die Gegenwart und Zukunft. In seinem Impuls ging es um den aktuellen Stand sicherer IT-Systeme und um die Aufgaben, die die digitale Gesellschaft zu lösen hat. Verschlüsselung ist eine wesentliche Grundlage, um sensible Informationen zu schützen – etwa bei der digitalen Kommunikation, in der Wirtschaft, in der Verwaltung und in kritischen Infrastrukturen. Gleichzeitig hängt ihre Wirksamkeit davon ab, dass Verfahren korrekt implementiert, Schlüssel geschützt und Systeme regelmäßig an neue Bedrohungen angepasst werden.

Schlüsseltechnologien für mehr Sicherheit und Risikobewusstsein

Ein besonderer Schwerpunkt lag auf der Frage, welche Auswirkungen Quantencomputer auf

etablierte Verschlüsselungsverfahren haben könnten. Ihre enorme Rechenleistung könnte perspektivisch dazu führen, dass künftig bestimmte, heute verwendete Verfahren nicht mehr als ausreichend sicher gelten. Damit stellt sich bereits heute die Aufgabe, digitale Infrastrukturen auf sogenannte Post-Quanten-Kryptografie vorzubereiten. Quantencomputer sind aber nicht ausschließlich eine Bedrohung: Quantenbasierte Verfahren und neue technologische Ansätze könnten künftig auch zur Verbesserung von Sicherheitslösungen beitragen.

Der anschließende Austausch mit dem Publikum schlug eine Brücke zwischen historischen Grundlagen der Kryptologie und aktuellen Fragen der digitalen Sicherheit. Die Diskussion verdeutlichte, dass IT-Sicherheit nicht allein eine technische Aufgabe ist. Sie erfordert ebenso ein Verständnis für gesellschaftliche Abhängigkeiten, verantwortungsvolle politische Gestaltung und die kontinuierliche Weiterentwicklung wissenschaftlicher Methoden.

Das Science & Technology Café brachte die enge Verbindung zwischen der Kryptologie-Geschichte, den Herausforderungen der Gegenwart und den Zukunftsfragen der Digitalisierung hervor. Von geheimen Botschaften der Antike bis zur Vorbereitung auf das Zeitalter der Quantencomputer bleibt die zentrale Aufgabe unverändert: Informationen zuverlässig schützen – und zugleich verstehen, welchen neuen Risiken sie ausgesetzt sind.

<https://www.acatech.de/allgemein/science-technology-cafe-kryptologie-zwischen-geschichte-und-zukunft-der-it-sicherheit>