CASA UNIVERSE

DAS RÄTSEL UM HUBA UND DIE SPUR DER COOKIES

EINE REISE DURCH DIE ZUKUNFT
DER KRYPTOGRAPHIE UND DIE AUFREGENDE
FORSCHUNGSWELT VON CASA

DAS RÄTSEL UM HUBA UND DIE SPUR DER COOKIES

EINE REISE DURCH DIE ZUKUNFT
DER KRYPTOGRAPHIE UND DIE AUFREGENDE
FORSCHUNGSWELT VON CASA

CASA
CYBER SECURITY IN THE AGE
OF LARGE-SCALE ADVERSARIES

CASA

Cybersicherheit im Zeitalter großskaliger Angreifer

Herausragende Wissenschaftler*innen erforschen und entwickeln im Rahmen des Exzellenzclusters „CASA – Cyber Security in the Age of Large-Scale Adversaries“ starke und nachhaltige Gegenmaßnahmen gegen mächtige Cyber-Angreifer, mit besonderem Fokus auf nationalstaatliche Angriffe. Die Forschung von CASA zeichnet sich durch einen starken interdisziplinären Ansatz aus, der nicht nur technische Fragen, sondern auch das Zusammenspiel von menschlichem Verhalten und IT-Sicherheit untersucht. Dieser einzigartige, ganzheitliche Ansatz bildet die Grundlage für exzellente IT-Sicherheitsforschung.

CASA umfasst vier Forschungsbereiche (Research Hubs):

HUB A „Kryptographie der Zukunft“: Forschung zur zukünftigen Kryptographie mit beweisbarer Sicherheit und Entwicklung von Ansätzen, die auch gegen Quantencomputer sicher sind.

HUB B „Eingebettete Sicherheit“: Untersuchung der Sicherheit eingebetteter Systeme auf der Hardware-Ebene sowie der Interaktion von Sicherheitssystemen mit ihrer physischen Umgebung.

HUB C „Sichere Systeme“: Entwicklung von sicheren und effizienten Systemen auf der Software-Ebene, auch mit Hilfe von Methoden aus dem Bereich des maschinellen Lernens.

HUB D „Benutzerfreundlichkeit“: Konzentration auf benutzerfreundliche Sicherheit und Privatsphäre sowie die Erforschung der Schnittstelle zwischen Mensch und Technik.

Jeder HUB befasst sich mit spezifischen Forschungsherausforderungen (Challenges), die sorgfältig ausgewählt wurden, um Sicherheitsfragen anzugehen, die für den Schutz vor komplexen Angriffen von entscheidender Bedeutung sind.

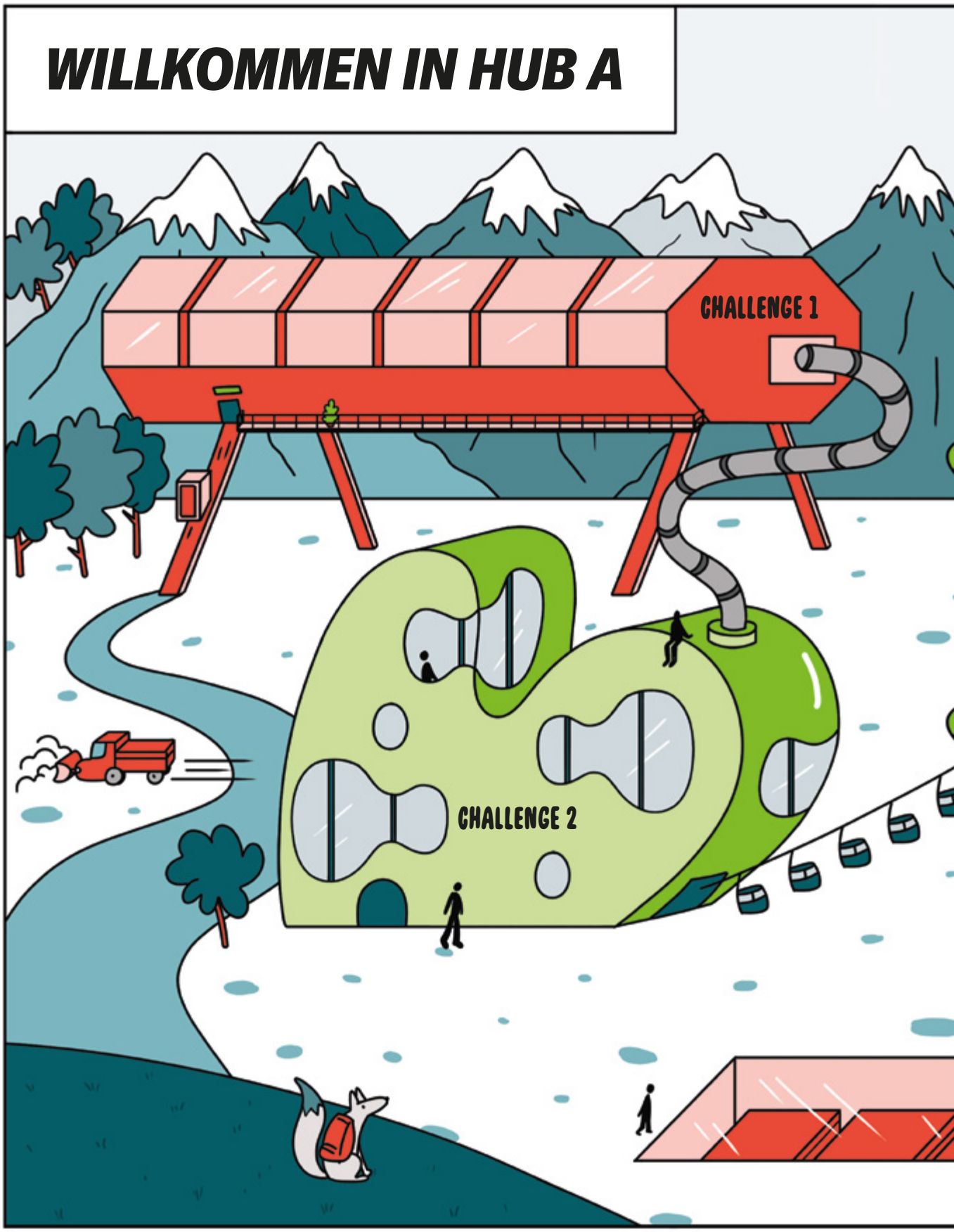
Die Challenges des HUB A sind:
Challenge 1: Kryptographie gegen Massenüberwachung
Challenge 2: Quantenresistente Kryptographie
Challenge 3: Grundlagen der Privatsphäre

Der Winter dauerte schon ewig und war bitterkalt. Fuchs Whitfield ist hungrig und gelangweilt.

Der köstliche Keksduft zieht ihn magisch an und lockt ihn unbemerkt in ein Abenteuer...

Ein cleverer Fuchs wie er ist natürlich neugierig, was es da draußen zu entdecken gibt.

Kekse sind vielleicht nicht das Einzige, das er mit zurück nach Hause bringen wird.


WILLKOMMEN IN HUB A
CHALLENGE 1
CHALLENGE 2

Inhalt

CHALLENGE 1

Kryptographie gegen Massenüberwachung

Wie können wir neue kryptographische Methoden entwickeln, die gegen Massenüberwachung helfen?

CHALLENGE 2

Quantenresistente Kryptographie

Können wir praktische Verschlüsselungs- und Signaturverfahren finden, die beweisbare Sicherheit gegen Quantencomputer bieten?

CHALLENGE 3

Grundlagen der Privatsphäre

Wie können wir mit Kryptographie unsere Privatsphäre schützen, wenn große Datenmengen in der Cloud gespeichert sind?

CASA BACKGROUND

CASA steht für „Cyber Security in the Age of Large-Scale Adversaries“ und wird als Exzellenzcluster (EXC) im Rahmen der Exzellenzstrategie der DFG in Deutschland gefördert. Ziel ist es, nachhaltige Sicherheit gegen komplexe, groß angelegte Angriffe zu ermöglichen. Dazu erforscht ein interdisziplinäres Team nicht nur technische, sondern auch soziale Faktoren und Zusammenhänge. Das Exzellenzcluster ist an der Ruhr-Universität Bochum angesiedelt.

casa.rub.de

KRYPTOGRAPHIE GEGEN MASSENÜBERWACHUNG

CHALLENGE 1

MIT VERGNÜGEN! DU BIST HIER BEI CHALLENGE 1, DER ERSTEN VON DREI CHALLENGES IN HUB A. WIR VERFOLGEN DREI ZIELE:

1 Wir untersuchen, wie man Verschlüsselungsstandards ohne Backdoors garantieren kann.

2 Wir untersuchen alte und aktuelle Standards, um von Angreifern eingebaute Backdoors zu erkennen.

3 Wir entwickeln neue Ansätze zum Erstellen sicherer Parameter, die beweisbaren Angriffen und Backdoors widerstehen können.

PUH! NE LANGE LISTE HABT IHR DA. ABER ICH BIN AUCH KEIN EXPERTE. WAS GIBT'S HEUTE ABEND EIGENTLICH ZU FEIERN?

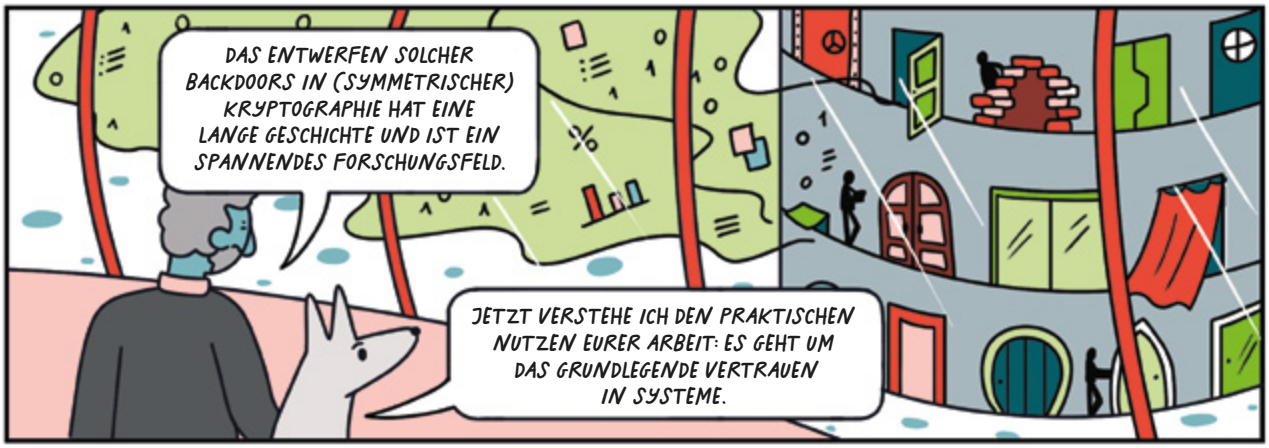
DAS WIRST DU SCHON NOCH SEHEN. ABER JETZT ERSTMAL PFOTEN WEG VON DEN KEKSEN, OK!?

CASA WIKI

Backdoors (Hintertüren) ermöglichen den Zugang zu Computersystemen ohne die Erlaubnis der Benutzer*innen. Sie können entweder das Ergebnis fehlerhafter Programmierung oder absichtlich in Hard- und Software eingebaut worden sein.

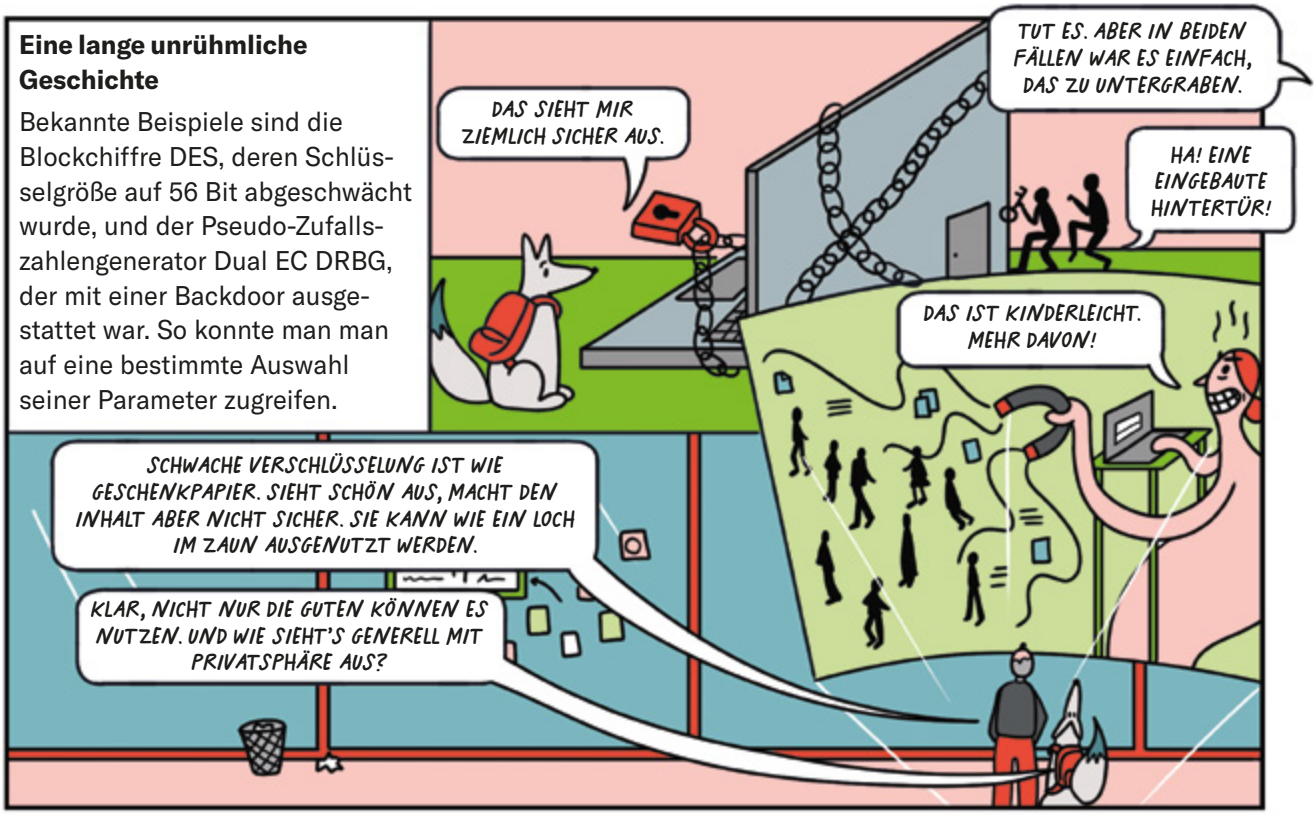
Kryptographie sorgt dafür, dass elektronische Kommunikation sicher bleibt, auch wenn (bösartige) Dritte versuchen, sie zu überwachen oder zu stören. Am häufigsten werden dafür Verschlüsselung und digitale Signaturen verwendet.

Kryptographische Standards sind technische Richtlinien, die sicherstellen, dass Verschlüsselungssysteme gut zusammenarbeiten, kompatibel sind und ein hohes Maß an Sicherheit bieten.



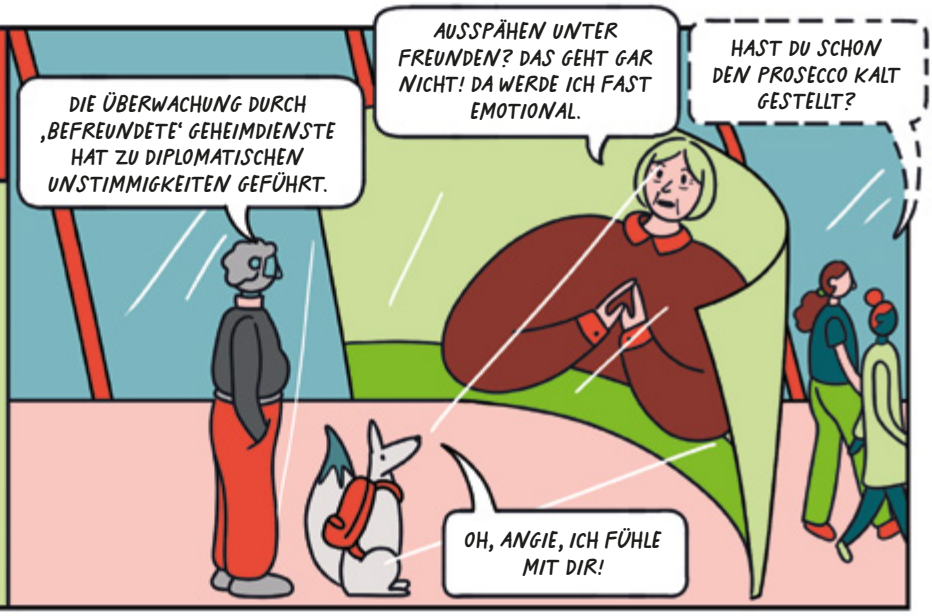
Eine lange unrühmliche Geschichte

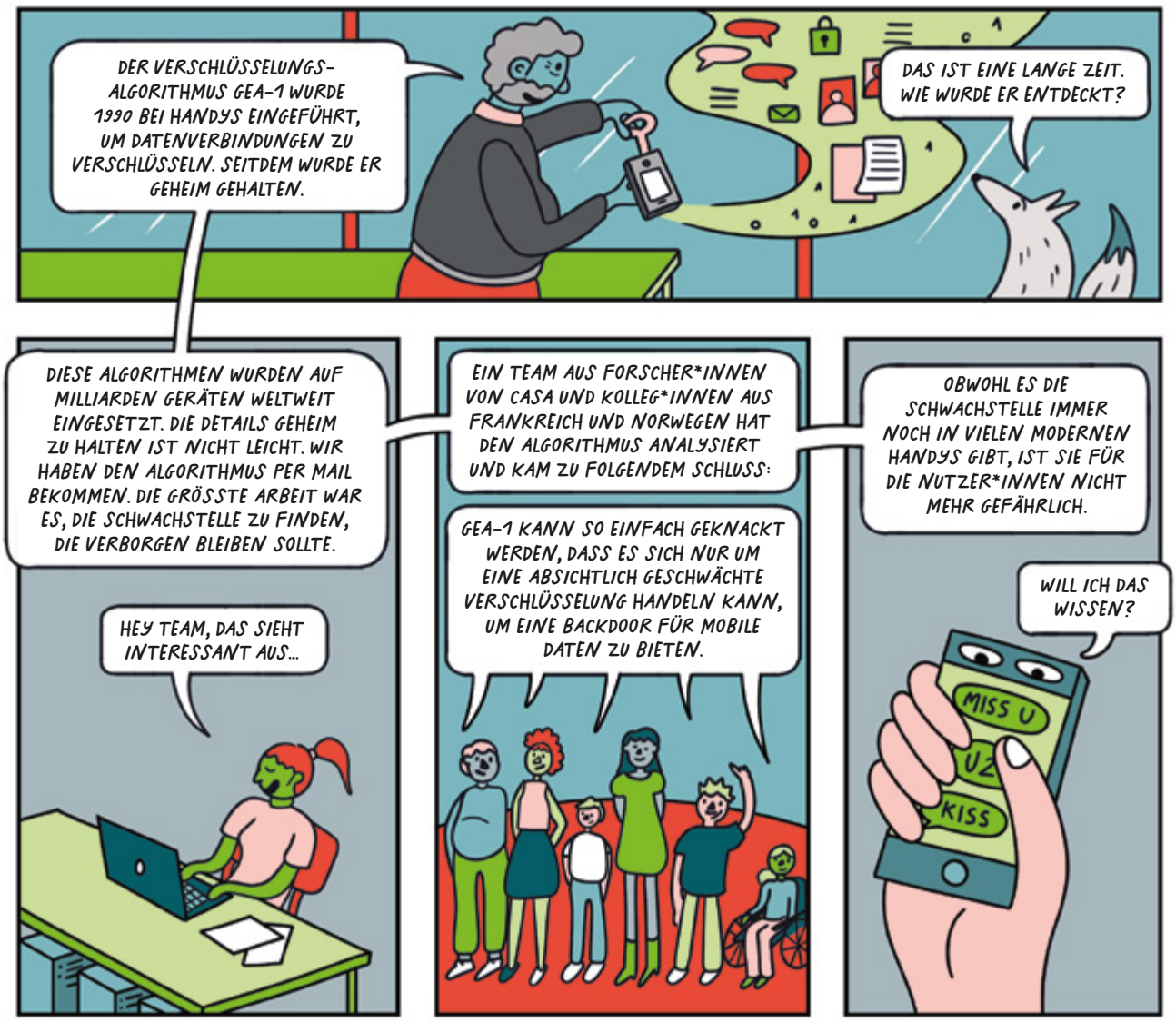
Bekannte Beispiele sind die Blockchiffre DES, deren Schlüsselgröße auf 56 Bit abgeschwächt wurde, und der Pseudo-Zufallszahlengenerator Dual EC DRBG, der mit einer Backdoor ausgestattet war. So konnte man man auf eine bestimmte Auswahl seiner Parameter zugreifen.

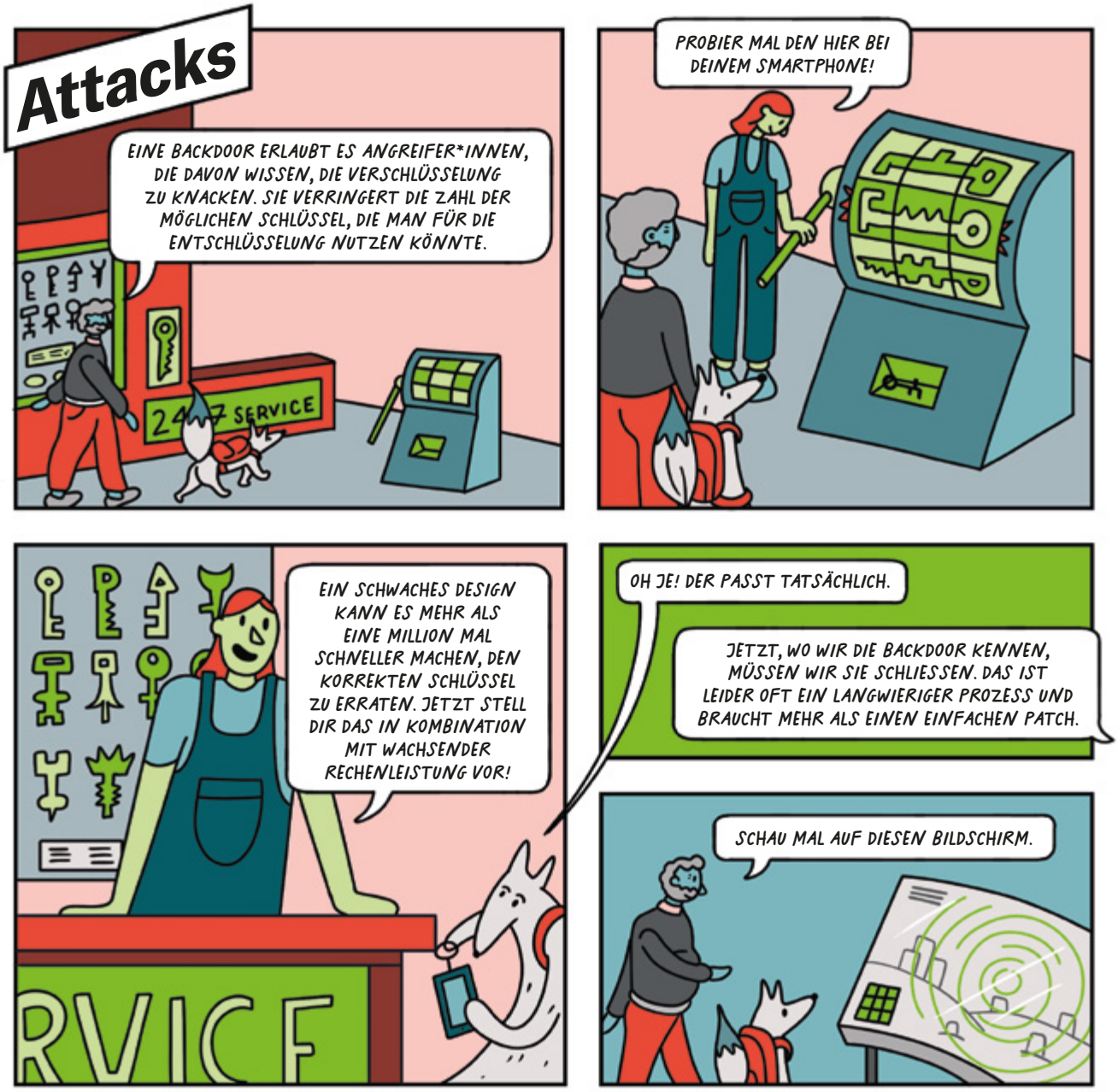


REAL LIFE STORY

In 2015 präsentierte WikiLeaks Beweise dafür, dass die NSA (National Security Agency der USA) seit 2002 das Mobiltelefon der ehemaligen Kanzlerin Angela Merkel abgehört hat. Betroffen war nicht nur ihr eigenes, sondern auch die Telefone von 125 weiteren hochrangigen Politiker*innen und Berater*innen.







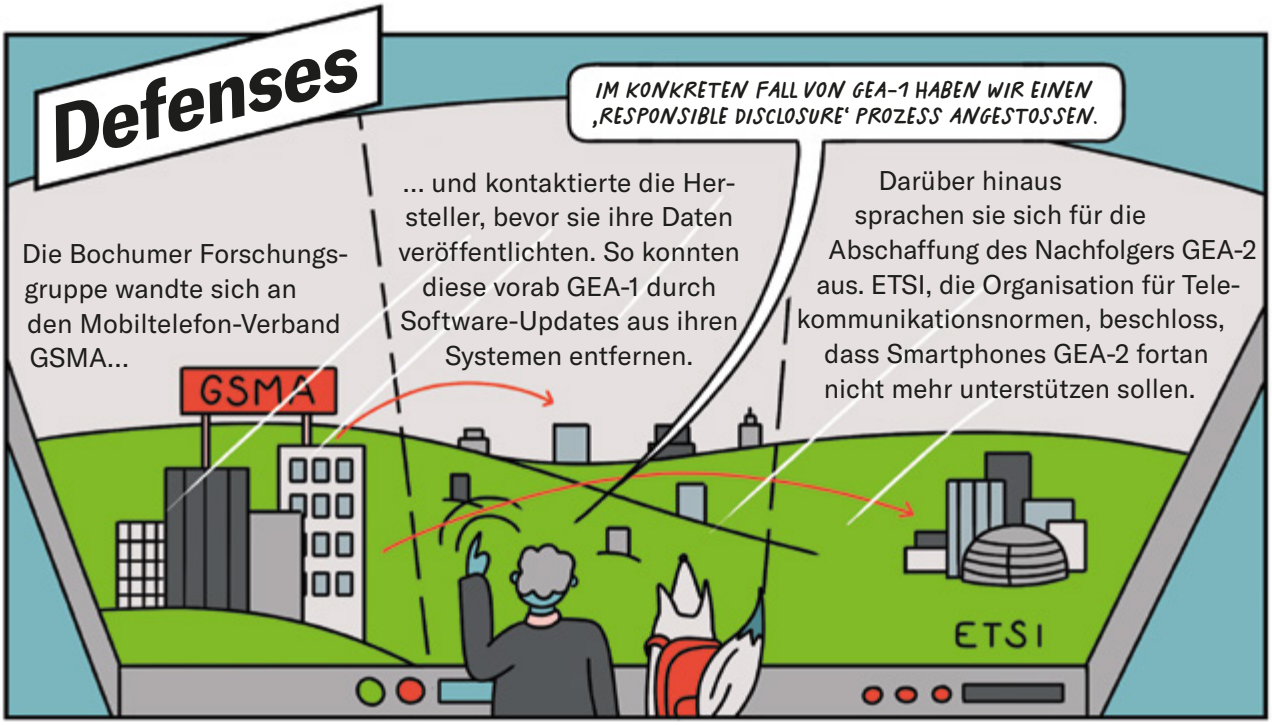
CASA WIKI

Bei **symmetrischer Verschlüsselung** wird derselbe Schlüssel zur Ver- und Entschlüsselung genutzt. Sie eignet sich gut für die Verschlüsselung großer Datenmengen, da sie schnell ist und wenig Ressourcen benötigt.

NIST ist das amerikanische „National Institute of Standards and Technology“.

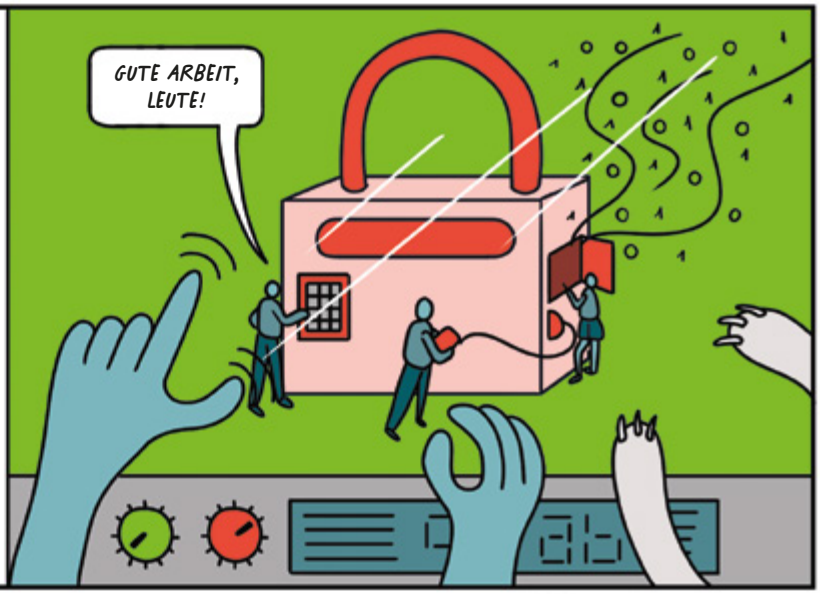
So sieht gute symmetrische Verschlüsselung aus:

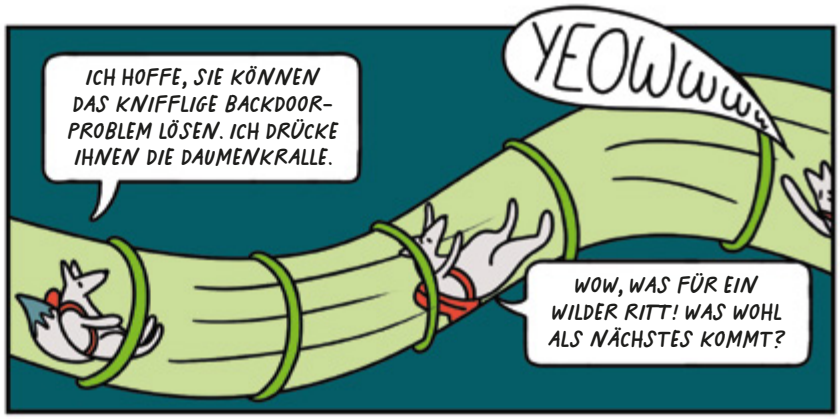
- Bis auf den Schlüssel ist der gesamte Algorithmus bekannt.
- Ohne den Schlüssel kann aus dem Chiffretext keine Information über den Klartext gewonnen werden.
- Die Anzahl der Schlüssel ist zu groß, um erraten zu werden.



Warum Transparenz gut für die Sicherheit ist

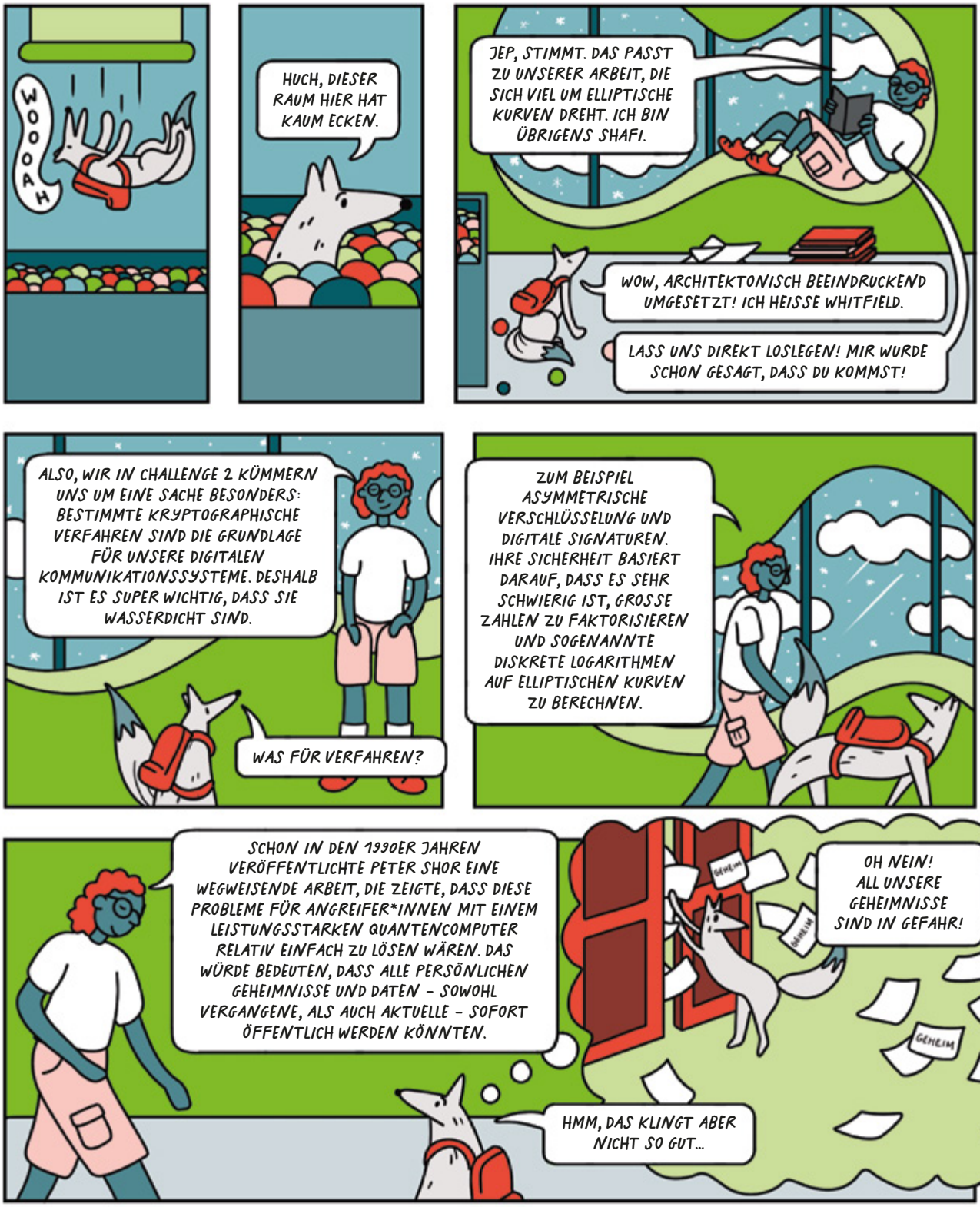
Allgemein sollten kryptographische Algorithmen nicht im Geheimen und mit unklaren Designkomponenten entwickelt werden. Das NIST hat gezeigt, wie es geht: Bei der Auswahl des Advanced Encryption Standard (AES) und neuer Post-Quanten-Algorithmen setzt es auf offene Designwettbewerbe, gefolgt von öffentlichen Diskussionen und Analysen. Es klingt zunächst widersprüchlich, aber je öffentlicher die Entwicklung stattfindet, desto sicherer wird sie.

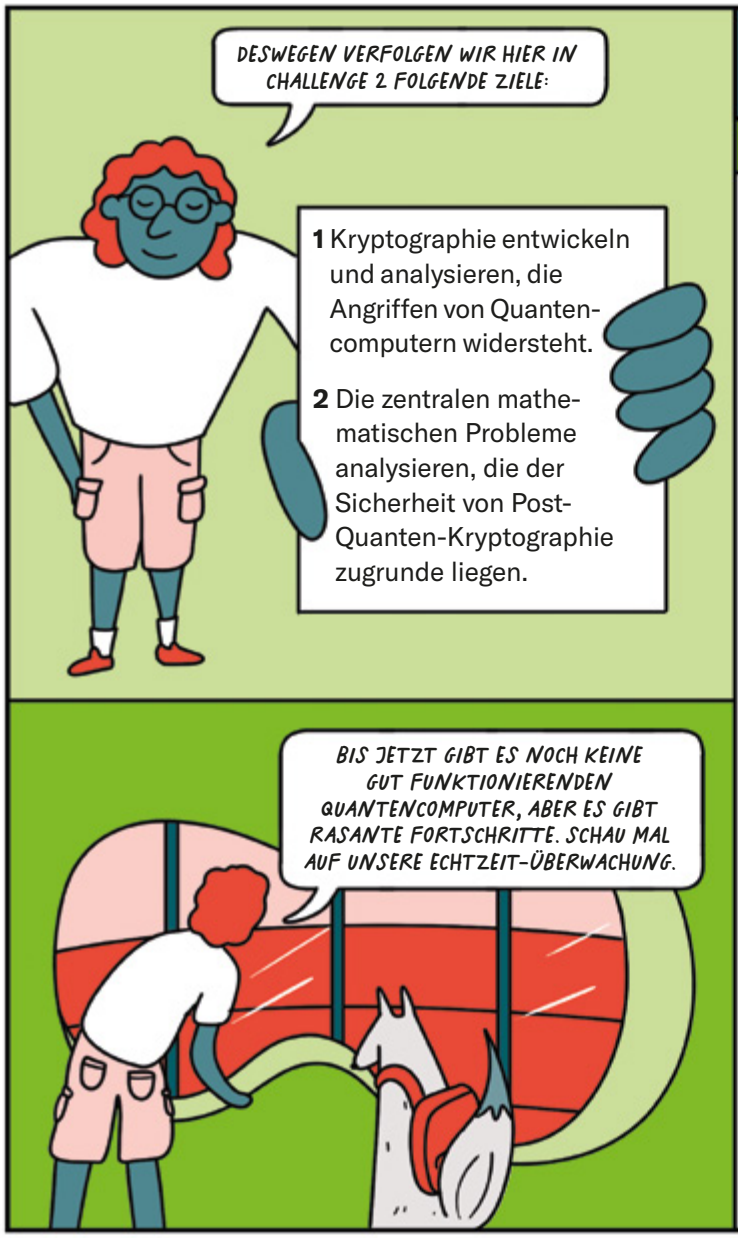




CHALLENGE 2

QUANTEN-RESISTENTE KRYPTOGRAPHIE





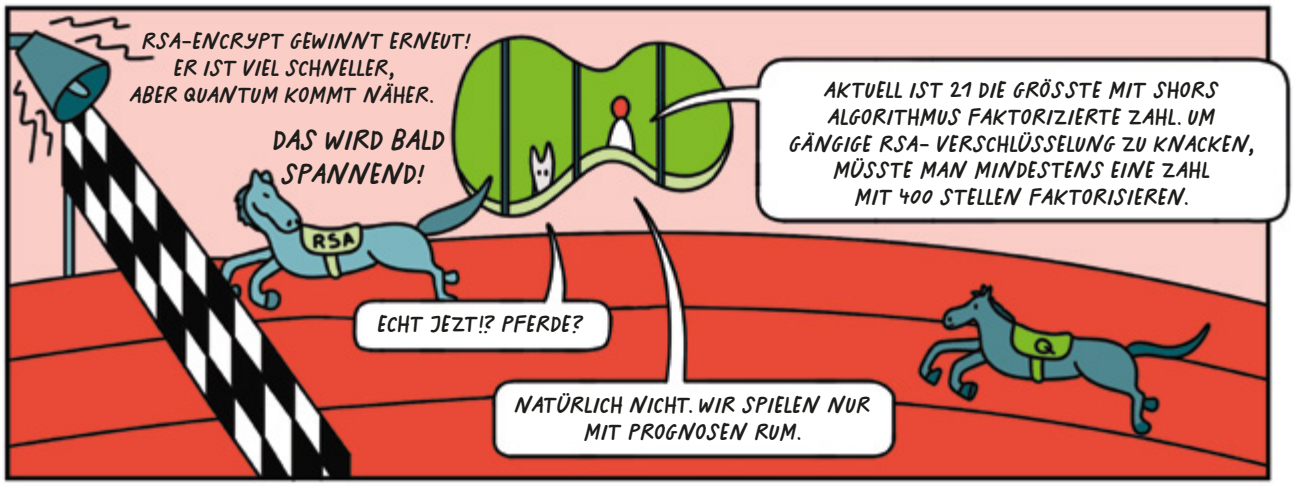
CASA WIKI

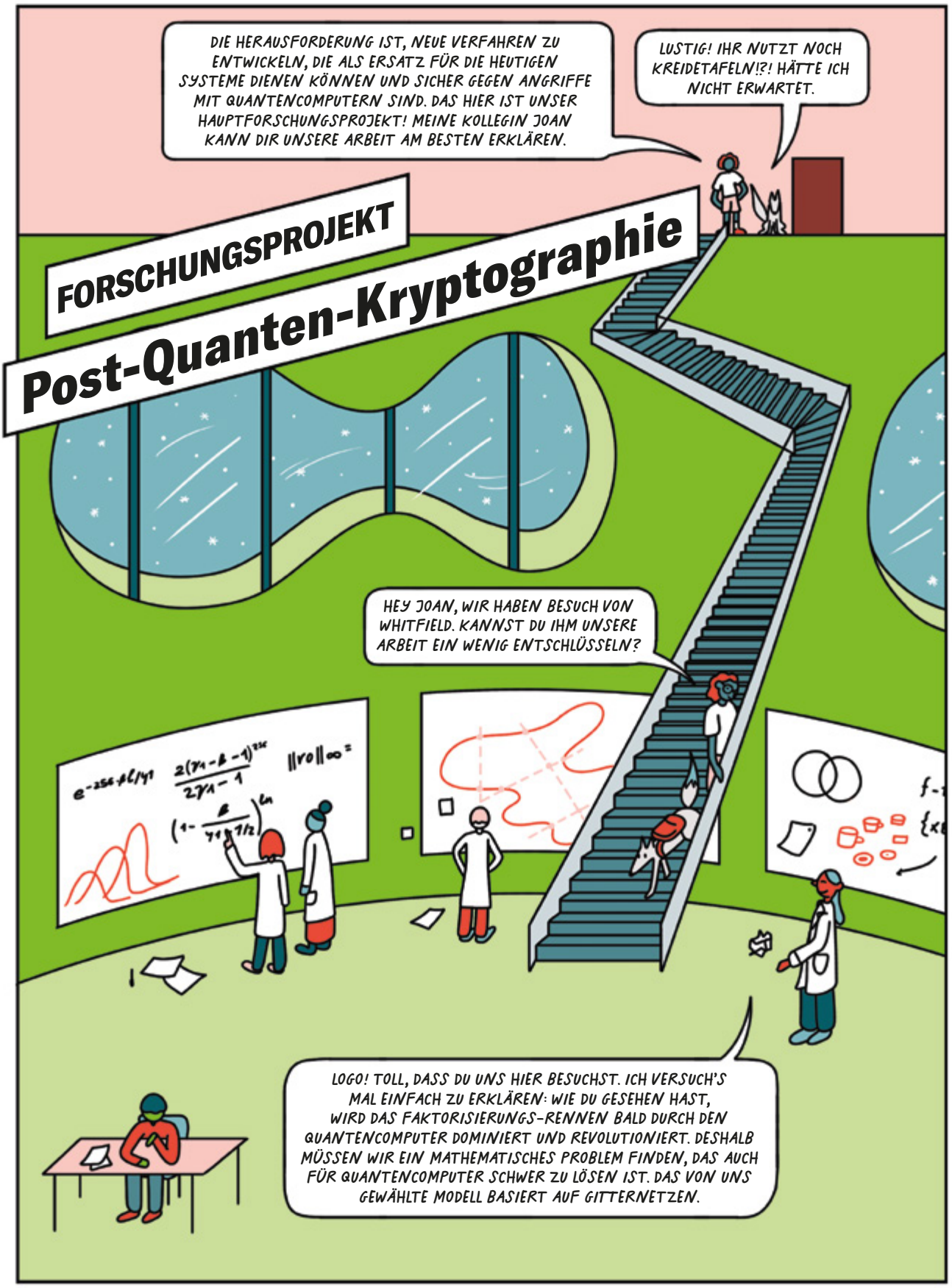
Ein **Quantencomputer** nutzt die Gesetze der Quantenmechanik aus, um bestimmte Probleme schneller zu lösen. So könnte er zum Beispiel die gesamte derzeit eingesetzte asymmetrische Kryptographie schnell brechen. Skalierbare Quantencomputer gibt es noch nicht, aber die Forschung macht große Fortschritte bei ihrer Entwicklung.

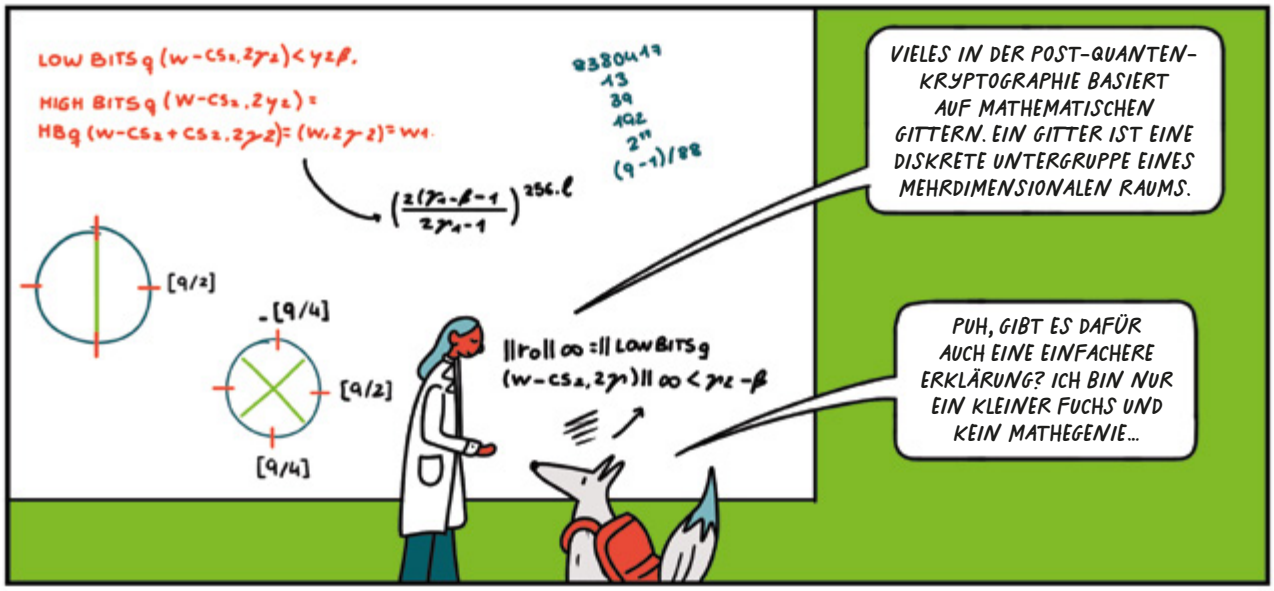
Post-Quanten-Kryptographie bezieht sich auf kryptographische Systeme, die mit Quantencomputern ausgestatteten Angreifer*innen standhalten können.

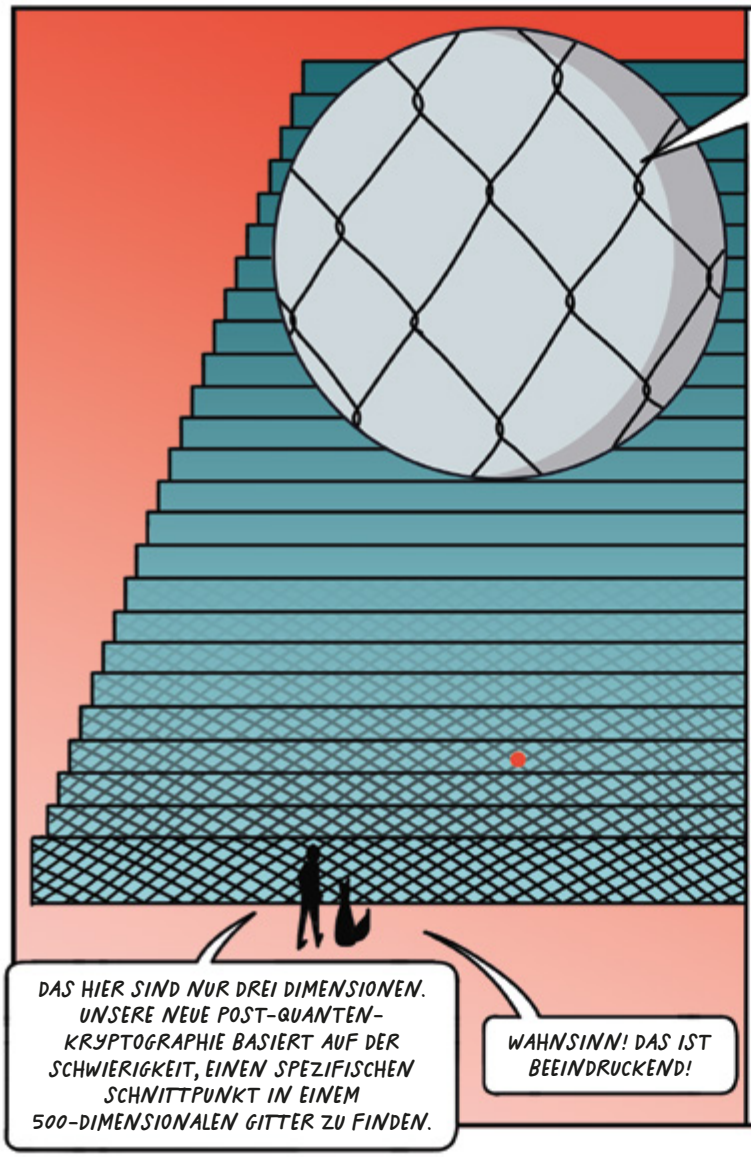
Der **Shor-Algorithmus** ist ein 1994 von Peter Shor entwickelter Algorithmus, der große ganze Zahlen effizient faktorisieren und diskrete Logarithmen über elliptische Kurven berechnen kann. Damit bietet er im Wesentlichen den Rahmen, um alle derzeit eingesetzten Verschlüsselungssysteme mit öffentlichen Schlüsseln zu brechen.

Die **asymmetrische Kryptographie** verwendet einen öffentlichen Schlüssel zur Verschlüsselung und einen privaten Schlüssel zur Entschlüsselung. Sie wird vor allem für Schlüsselvereinbarungen zwischen Parteien verwendet, die sich vorher noch nicht begegnet sind.




DIE HERAUSFORDERUNG IST, NEUE VERFAHREN ZU ENTWICKELN, DIE ALS ERSATZ FÜR DIE HEUTIGEN SYSTEME DIENEN KÖNNEN UND SICHER GEGEN ANGRIFFE MIT QUANTENCOMPUTERN SIND. DAS HIER IST UNSER HAUPTFORSCHUNGSPROJEKT! MEINE KOLLEGIN JOAN KANN DIR UNSERE ARBEIT AM BESTEN ERKLÄREN.
LUSTIG! IHR NUTZT NOCH KREIDETAFELN!?! HÄTTE ICH NICHT ERWARTET.
FORSCHUNGSPROJEKT
Post-Quanten-Kryptographie
HEY JOAN, WIR HABEN BESUCH VON WHITFIELD. KANNST DU IHM UNSERE ARBEIT EIN WENIG ENTSCHLÜSSELN?
LOGO! TOLL, DASS DU UNS HIER BESUCHST. ICH VERSUCH'S MAL EINFACH ZU ERKLÄREN: WIE DU GESEHEN HAST, WIRD DAS FAKTORISIERUNGS-RENNEN BALD DURCH DEN QUANTENCOMPUTER DOMINIERT UND REVOLUTIONIERT. DESHALB MÜSSEN WIR EIN MATHEMATISCHES PROBLEM FINDEN, DAS AUCH FÜR QUANTENCOMPUTER SCHWER ZU LÖSEN IST. DAS VON UNS GEWÄHLTE MODELL BASIERT AUF GITTERNETZEN.

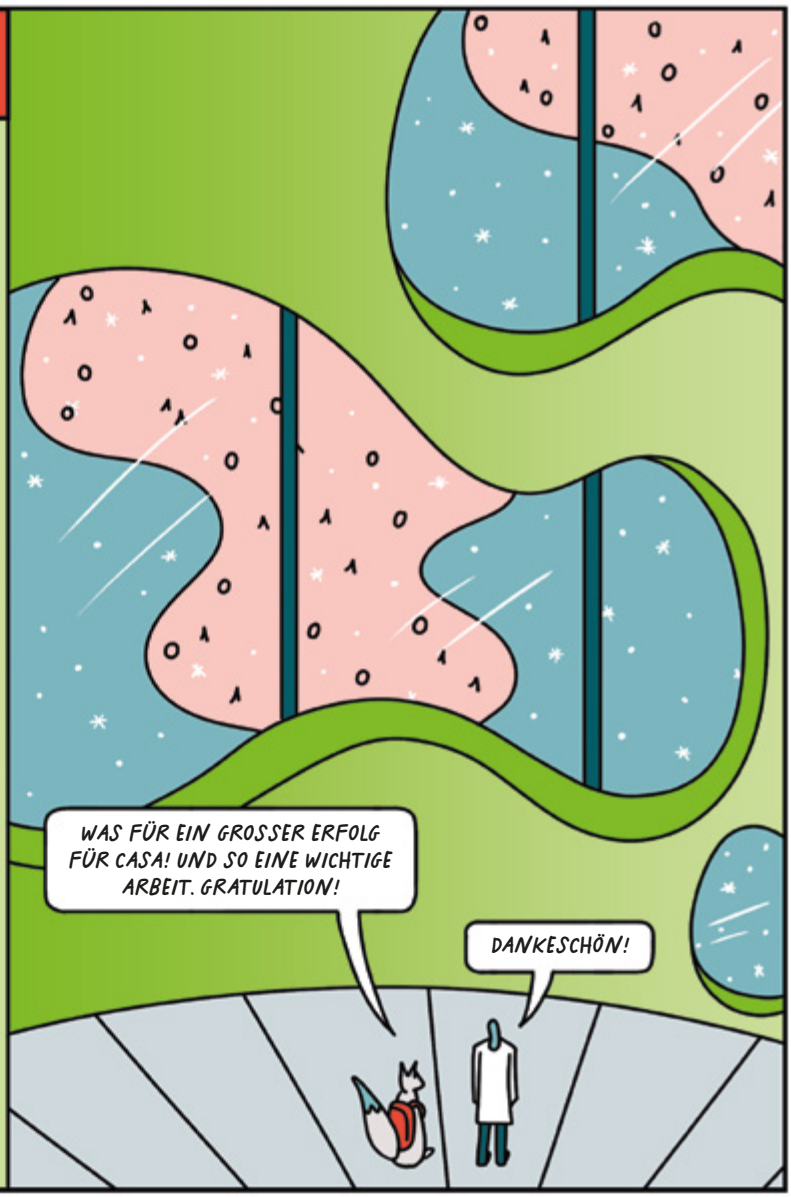


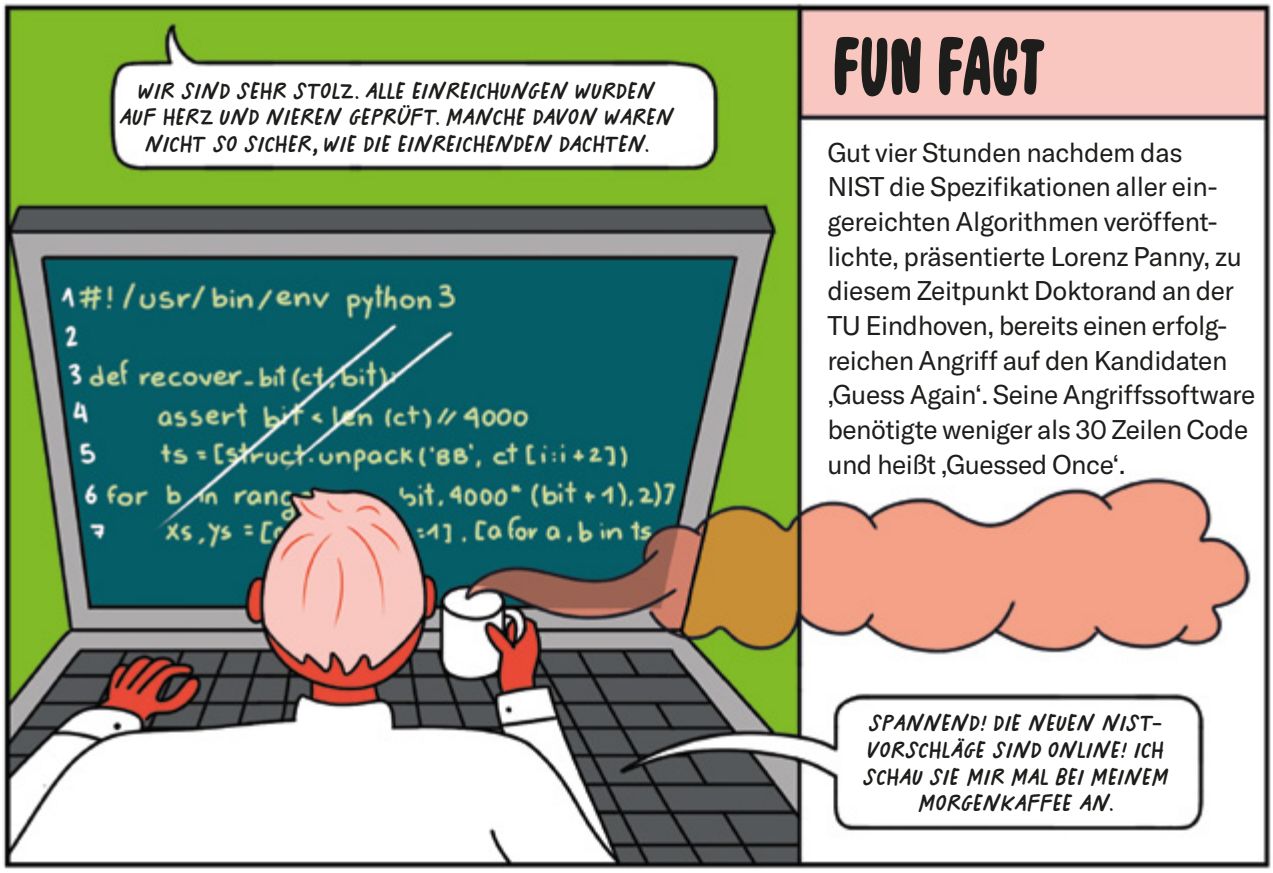


Gitterbasierte Kryptographie
Stell dir einen Maschendrahtzaun vor – das ist ein zweidimensionales Gitter. Die Gitterpunkte sind die Schnittpunkte der Kettenglieder im Zaun (wir nennen diese Glieder Vektoren). Es ist mathematisch äußerst anspruchsvoll, zu versuchen einen ‚kurzen Vektor' in einem hochdimensionalen Gitter zu finden, d. h. ein Kettenglied in der Nähe des Ursprungs des Graphen.

REAL LIFE STORY

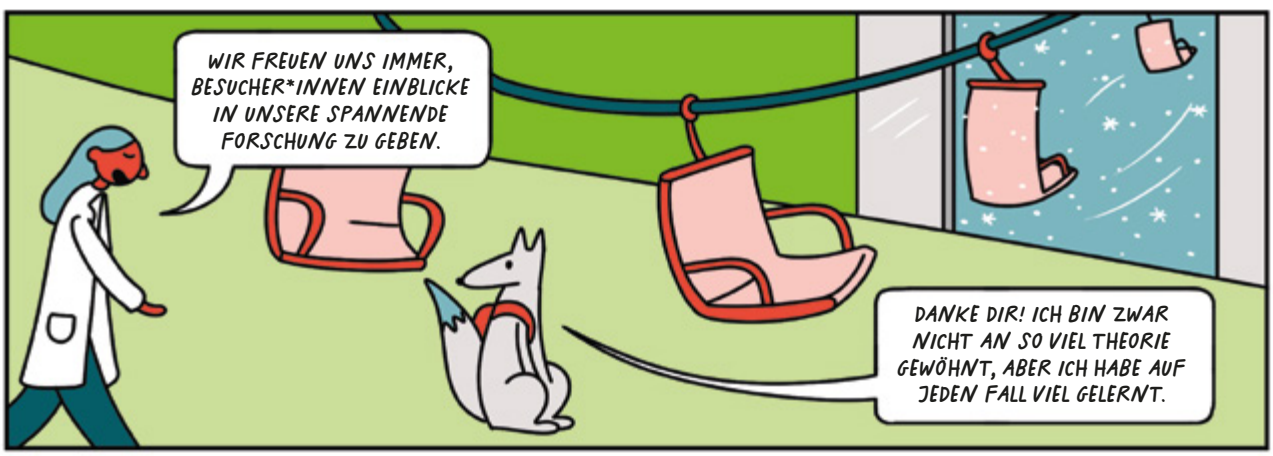
Das amerikanische National Institute for Standards and Technology (NIST) hat die von Quantencomputern ausgehenden Risiken für die sichere Datenverschlüsselung erkannt und 2016 einen Prozess zur Standardisierung der Post-Quanten-Kryptographie gestartet. Weltweit wurden 69 Vorschläge aus der Forschungsgemeinschaft eingereicht, die in einem öffentlichen Verfahren bewertet wurden. Im Juli 2022 wurden vier dieser Vorschläge ausgewählt, um vom NIST standardisiert zu werden: drei digitale Signaturverfahren und ein Verschlüsselungssystem mit öffentlichem Schlüssel. CASA-Forscher*innen haben drei der vier Systeme mitentwickelt. Sie heißen: CRYSTALS-Dilithium, SPHINCS+ und CRYSTALS-Kyber.





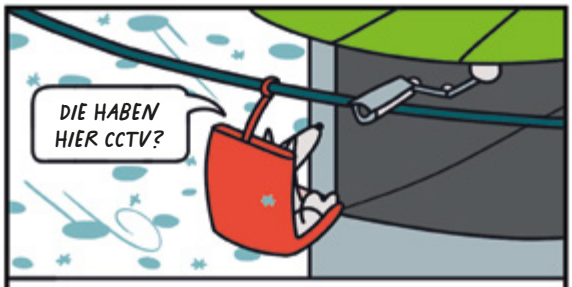
FUN FACT

Gut vier Stunden nachdem das NIST die Spezifikationen aller eingereichten Algorithmen veröffentlichte, präsentierte Lorenz Panny, zu diesem Zeitpunkt Doktorand an der TU Eindhoven, bereits einen erfolgreichen Angriff auf den Kandidaten ‚Guess Again'. Seine Angriffssoftware benötigte weniger als 30 Zeilen Code und heißt ‚Guessed Once'.



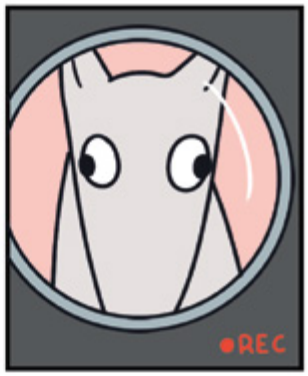
GRUNDLAGEN DER PRIVATSPHÄRE

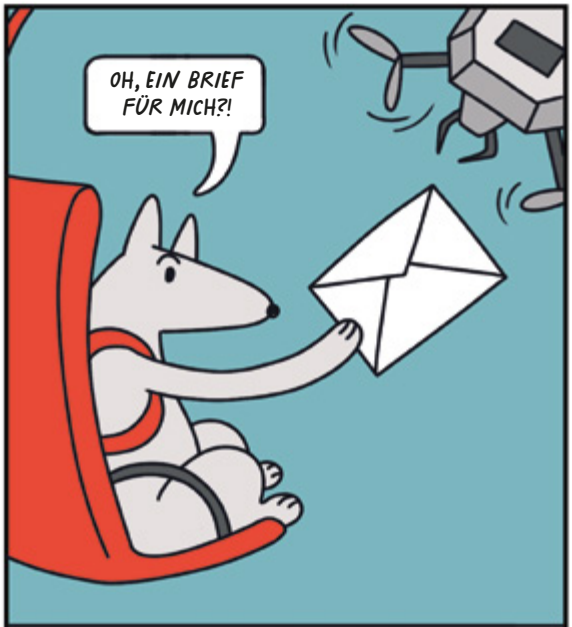
CHALLENGE 3



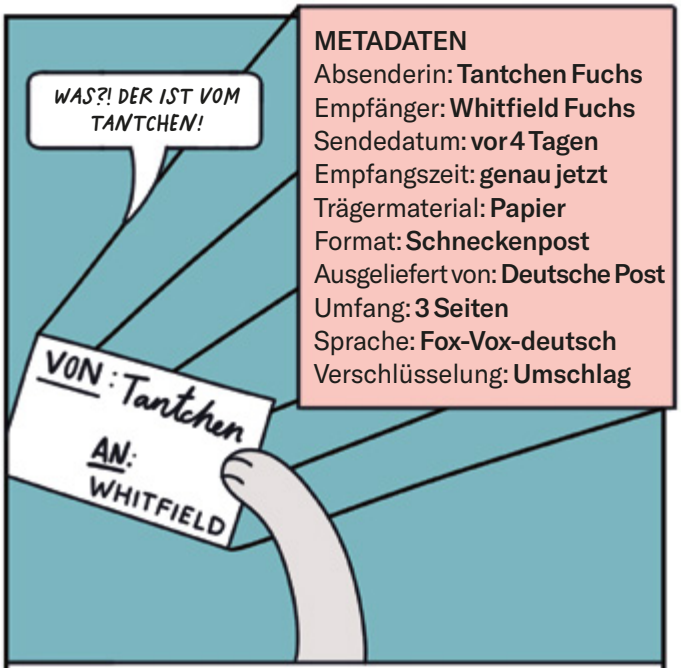
Wie bereits erwähnt, betreiben Geheimdienste Massenüberwachung ...

... der eigenen Bürger*innen und der anderer Länder.



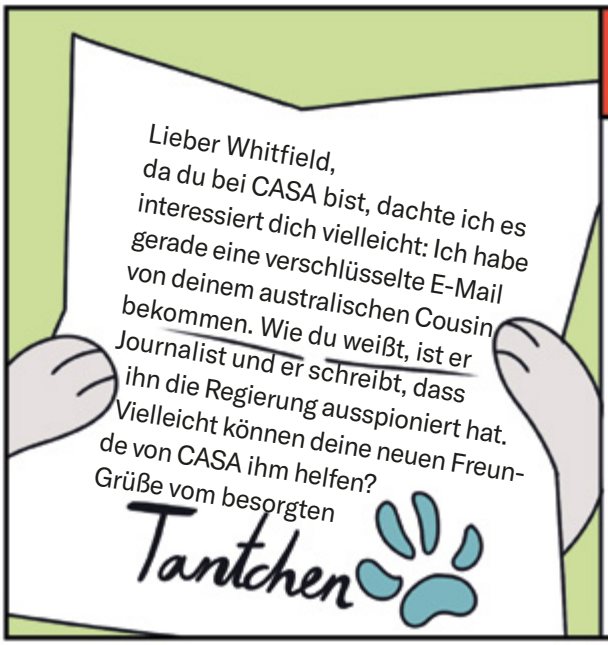


Selbst wenn der Inhalt einer Nachricht verschlüsselt ist, kann man Sender*in und Empfänger*in bei der Übertragung identifizieren.



METADATEN
Absenderin: **Tantchen Fuchs**
Empfänger: **Whitfield Fuchs**
Sendedatum: **vor 4 Tagen**
Empfangszeit: **genau jetzt**
Trägermaterial: **Papier**
Format: **Schneckenpost**
Ausgeliefert von: **Deutsche Post**
Umfang: **3 Seiten**
Sprache: **Fox-Vox-deutsch**
Verschlüsselung: **Umschlag**

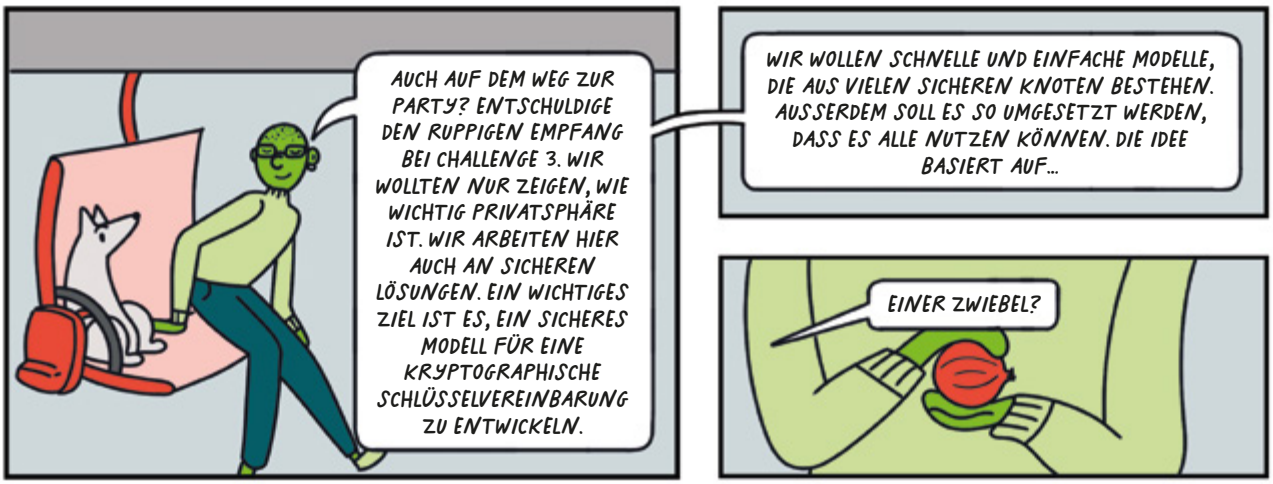
Diese sogenannten ‚Metadaten' enthalten jede Menge wertvoller Informationen.

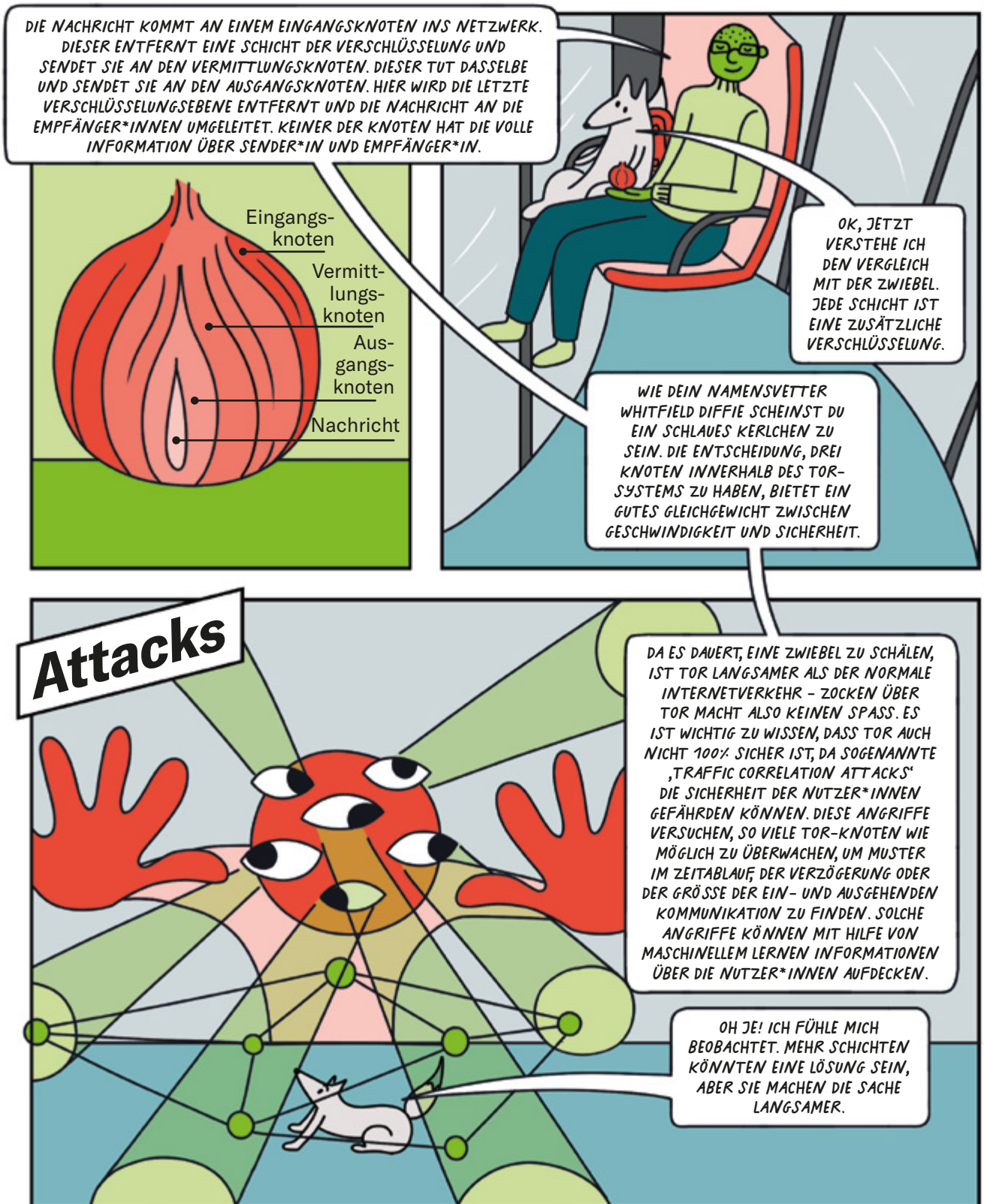


REAL LIFE STORY

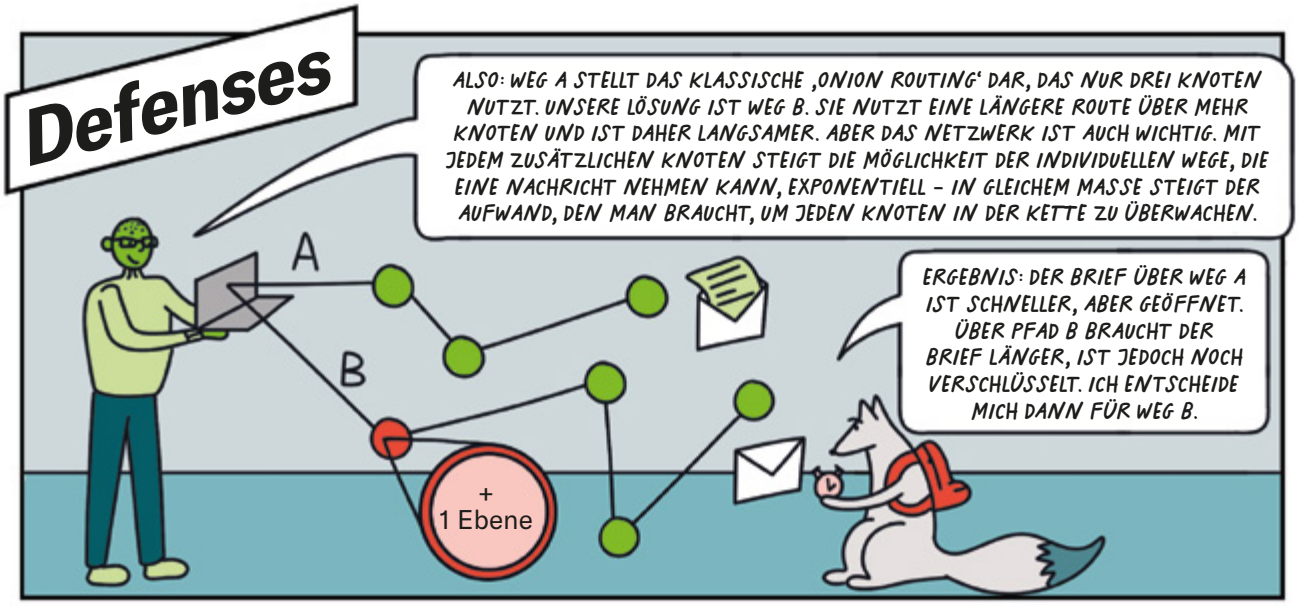
Im Jahr 2016 untersuchte Paul Farrell das Internierungslager für Geflüchtete auf der Insel Nauru, dessen schlechte, unmenschliche Bedingungen scharf kritisiert wurden. Wegen des australischen Gesetzes zur Vorratsdatenspeicherung durfte die Polizei legal alle seine Kommunikationsdaten einsehen und analysieren, um seine Quellen herauszufinden und Informationen über mögliche Whistleblower zu sammeln. Sie sammelten auch die Metadaten von Farrells Handy und analysierten seine E-Mails.

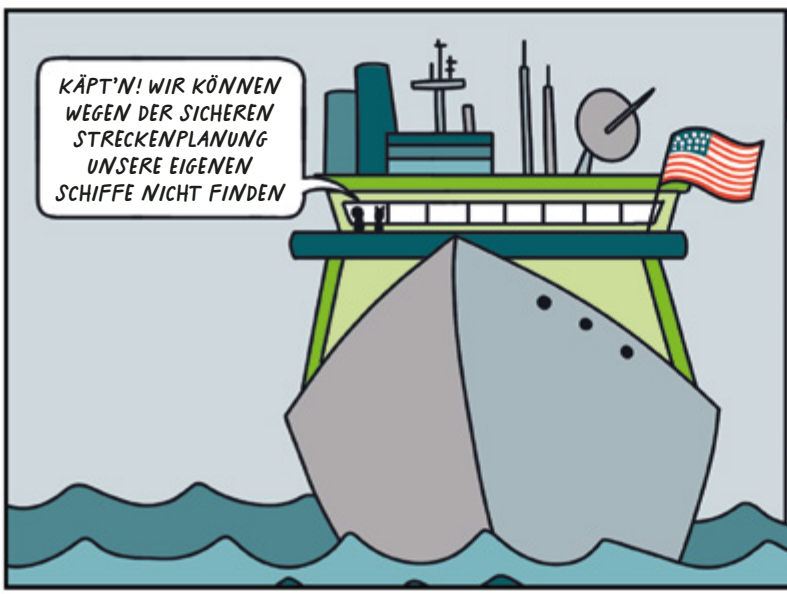
Wenn schon in Demokratien so tief in die Privatsphäre eingegriffen wird, wie sieht es dann erst in autoritären Regimen aus?





Selbst versteckte Knoten können erkannt werden. TOR-spezifischer Code kann durch ‚deep package inspection' erkannt werden, wenn eine Nachricht geschickt wird. Ist der versteckte Knoten bekannt, kann er blockiert werden. Beispielsweise blockiert China alle Versuche, von innerhalb des Landes auf TOR-Eingangsknoten zuzugreifen.





FUN FACT

Trotz ihrer Abneigung gegenüber TOR spielte die US-Regierung eine entscheidende Rolle bei der Entwicklung. Onion Routing wurde in seiner grundlegendsten Form in den 1990er Jahren von der U.S. Navy entwickelt, um die Kommunikation der Geheimdienste zu schützen. Auch das U.S. Department of State Bureau of Democracy, Human Rights and Labor gehört zu den finanziellen Unterstützern von TOR.


GLÜCKWUNSCH! DU HAST ECHT GUT ZUGEHÖRT UND VERSTANDEN, WORUM ES BEI UNSERER ARBEIT GEHT.
TJA, ICH SCHÄTZE, DAS WAR NUR DIE SPITZE DES EISBERGS…
OH, HIER IST ÜBRIGENS EIN BRIEF VON MEINEM TANTCHEN. SIE BITTET UM RAT.
LASS MAL SEHEN…
HMM. ICH DENKE, DEIN COUSIN IST AUF EINEM GUTEN WEG, INDEM ER VERSCHLÜSSELTE MAILS NUTZT. ER SOLLTE NOCH DEN TOR BROWSER UND SICHERE MESSENGER NUTZEN. AUCH WENN MANCHE SICHERHEITS- UND DATENSCHUTZ-TOOLS AKTUELL NOCH UNBEQUEM ZU NUTZEN SIND. ABER UNSERE KOLLEG*INNEN IN HUB D ARBEITEN DRAN! VIELLEICHT SOLLTEST DU SIE DEMNÄCHST MAL BESUCHEN.
HEY, IHR DA! HÖRT AUF ZU QUATSCHEN UND MACHT BEIM DANCE BATTLE MIT!
KLINGT VERFÜHRERISCH, ABER ICH MUSS LOS. TANTCHEN MACHT SICH BESTIMMT SCHON SORGEN.
JETZT HABE ICH EINEN BEUTEL VOLLER KEKSE, DEN KOPF VOLL WISSEN UND SOGAR EIN PAAR TIPPS FÜR TANTCHEN. SIE WIRD STOLZ SEIN. AUSSERDEM HABE ICH GELERNT, DASS SICHERHEIT KEIN ZUSTAND, SONDERN EIN KONTINUIERLICHER PROZESS IST. MAN MUSS ZUKÜNFTIGE SZENARIEN MITBEDENKEN. GUT, DASS SICH DIE LEUTE BEI CASA DARUM KÜMMERN.

ÜBER CASA

CASA: Cyber Security in the Age of Large-Scale Adversaries wurde 2019 gegründet und ist das einzige Exzellenzcluster im Bereich IT-Sicherheit in Deutschland. Von der Deutschen Forschungsgemeinschaft (DFG) wird CASA mit 30 Millionen Euro über sieben Jahre hinweg gefördert, um ausgezeichnete Forschungsbedingungen zu garantieren.

Bei CASA arbeitet eine Kerngruppe führender Forscher*innen mit einem klaren Fokus auf Sicherheit und Datenschutz eng mit ausgewählten Spitzenforscher*innen aus hochrelevanten Nachbardisziplinen zusammen. Dabei deckt das Team sämtliche Disziplinen ab, die erforderlich sind, um die anspruchsvollen Forschungsprobleme im Bereich der modernen IT-Sicherheit zu bewältigen, darunter Informatik, Mathematik, Elektrotechnik und Psychologie.

CASA ist am Horst-Görtz-Institut für IT-Sicherheit (hgi.rub.de) angesiedelt, einem wegweisenden Forschungsinstitut in Deutschland. Außerdem arbeitet CASA eng mit dem Max-Planck-Institut für Sicherheit und Privatsphäre in Bochum (mpi-sp.org) und zahlreichen weiteren Instituten und Universitäten zusammen.

Was ist ein „Exzellenzcluster“?
Mit der Förderlinie „Exzellenzcluster“ werden international wettbewerbsfähige Forschungszentren an Universitäten oder Universitätsverbünden in Deutschland projektbezogen für einen Zeitraum von sieben Jahren gefördert. Innerhalb dieser Cluster arbeiten Wissenschaftler*innen aus verschiedenen Disziplinen und Institutionen gemeinsam an einem Forschungsprojekt. Die Förderung ermöglicht es ihnen, sich intensiv auf ihr Forschungsziel zu konzentrieren, wissenschaftlichen Nachwuchs auszubilden und internationale Spitzenforscher*innen zu gewinnen.

casa.rub.de

TECHNISCHER BACKGROUND

Die in diesem Comic vorgestellten Konzepte und Methoden wurden von den am Exzellenzcluster CASA mitwirkenden Forscher*innen entwickelt. Die Originalveröffentlichungen sind online verfügbar und geben detaillierte Einblicke in ihre Forschung. Zusätzlich veröffentlichen wir zu vielen Publikationen den Quellcode und weitere Forschungsergebnisse. Bei Fragen stehen wir gerne zur Verfügung: info@casa.rub.de

PUBLIKATIONEN

Christof Beierle, Tim Beyne, Patrick Felke, Gregor Leander: **Constructing and Deconstructing Intentional Weaknesses in Symmetric Ciphers**, CRYPTO, 2022

Christof Beierle, Patrick Derbez, Gregor Leander, Gaëtan Leurent, Håvard Raddum, Yann Rotella, David Rupprecht, Lukas Stennes: **Cryptanalysis of the GPRS Encryption Algorithms GEA-1 and GEA-2**, EUROCRYPT, 2021

Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, Damien Stehlé: **CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM**, IEEE European Symposium on Security and Privacy, 2018

Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, Damien Stehlé: **CRYSTALS-Dilithium: Digital Signatures from Module Lattices**, Transactions on Cryptographic Hardware and Embedded Systems, Volume 2018-1

Sebastian Lauer, Kai Gellert, Robert Merget, Tobias Handirk, Jörg Schwenk: **TORTT: Non-Interactive Immediate Forward-Secret Single-Pass Circuit Construction**, Proceedings on Privacy Enhancing Technologies, 2020

CASA HUB A

1. Auflage 2025

Redaktion
Mirjam Stricker (CASA/Ruhr-Universität Bochum)
Annika Gödde (CASA/Ruhr-Universität Bochum)
Niels Jansen (Ellery Studio)
Eike Kiltz (CASA/Ruhr-Universität Bochum)
Gregor Leander (CASA/Ruhr-Universität/Bochum)
Peter Schwabe (CASA/Max Planck Institute for Security and Privacy)
Jörg Schwenk (CASA/Ruhr-Universität Bochum)
Christian Mainka (CASA/Ruhr-Universität Bochum)

Ellery Studio
Art Direction and Design: Luca Bogoni
Illustration: Lucia Cordero,
Hannah Schrage, David Ramirez Fernandez
Projektmanagement: Niels Jansen

Umschlaggestaltung
Hannah Schrage

Druck
Schmidt, Ley + Wiegandt GmbH + Co. KG,
Lünen, www.slw-medien.de

Herausgeber
CASA: Cyber Security in the Age
of Large-Scale Adversaries
Universitätsstraße 150
44780 Bochum

hgi-presse@rub.de
casa.rub.de

Scanne den QR-Code, um zur digitalen Version dieses Comics und zu den Comics (Englisch/Deutsch) der anderen Research HUBs zu gelangen:

Auf Englisch sind folgende Comics erschienen:

- The Secrets of HUB A and the Traces of the Cookies
- A Deep Dive Into HUB B and the Swirl of Embedded Security
- What's the Fuzz About HUB C and the Missing Carrots?
- HUB D and the Rumble in the Jungle of Usability

CASA
Cyber Security in the Age of Large-Scale Adversaries

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

RUHR UNIVERSITÄT BOCHUM
RUB

ellery studio

WAS HEUTE SICHER IST, KANN MORGEN SCHON EIN OFFENES GEHEIMNIS SEIN. DAS GILT BESONDERS FÜR DIE DIGITALE WELT: VON MASSENÜBERWACHUNG UND POST-QUANTEN-KRYPTOGRAPHIE BIS HIN ZU SICHEREM ROUTING UND VERSCHLÜSSELUNG.

BEGLEITE DEN NEUGIERIGEN KLEINEN FUCHS WHITFIELD AUF SEINER JAGD DURCH HUB A. WIRD ER ALLE HERAUSFORDERUNGEN AUF SEINEM WEG MEISTERN?

FINDE ES HERAUS!