CASA UNIVERSE

THE SECRETS OF HUBA AND THE TRACES OF THE COOKIES

A JOURNEY THROUGH THE FUTURE
OF CRYPTOGRAPHY AND THE EXCITING
RESEARCH WORLD OF CASA

THE SECRETS OF HUBA AND THE TRACES OF THE COOKIES

A JOURNEY THROUGH THE FUTURE
OF CRYPTOGRAPHY AND THE EXCITING
RESEARCH WORLD OF CASA

CASA
CYBER SECURITY IN THE AGE
OF LARGE-SCALE ADVERSARIES

CASA

Cyber Security in the Age of Large-Scale Adversaries

Outstanding scientists within the Cluster of Excellence “CASA - Cyber Security in the Age of Large-Scale Adversaries” research and develop strong and sustainable countermeasures against powerful cyber attackers, with a particular focus on nation-state attackers. Research in CASA is characterized by a highly interdisciplinary approach that examines not only technical issues, but also the interplay between human behavior and IT security. This unique, holistic approach forms the basis for excellent IT security research.

CASA unites four main research areas:

HUB A “Future Cryptography”: Researching future cryptography and developing quantum-resistant approaches with provable security.

HUB B “Embedded Security”: Tackling the task of strengthening the security of embedded systems at the hardware level by investigating the interaction of security systems with their physical environment.

HUB C “Secure Systems”: Developing secure and efficient systems at the software level. Machine Learning is one of the many methods used to explore and expand this field.

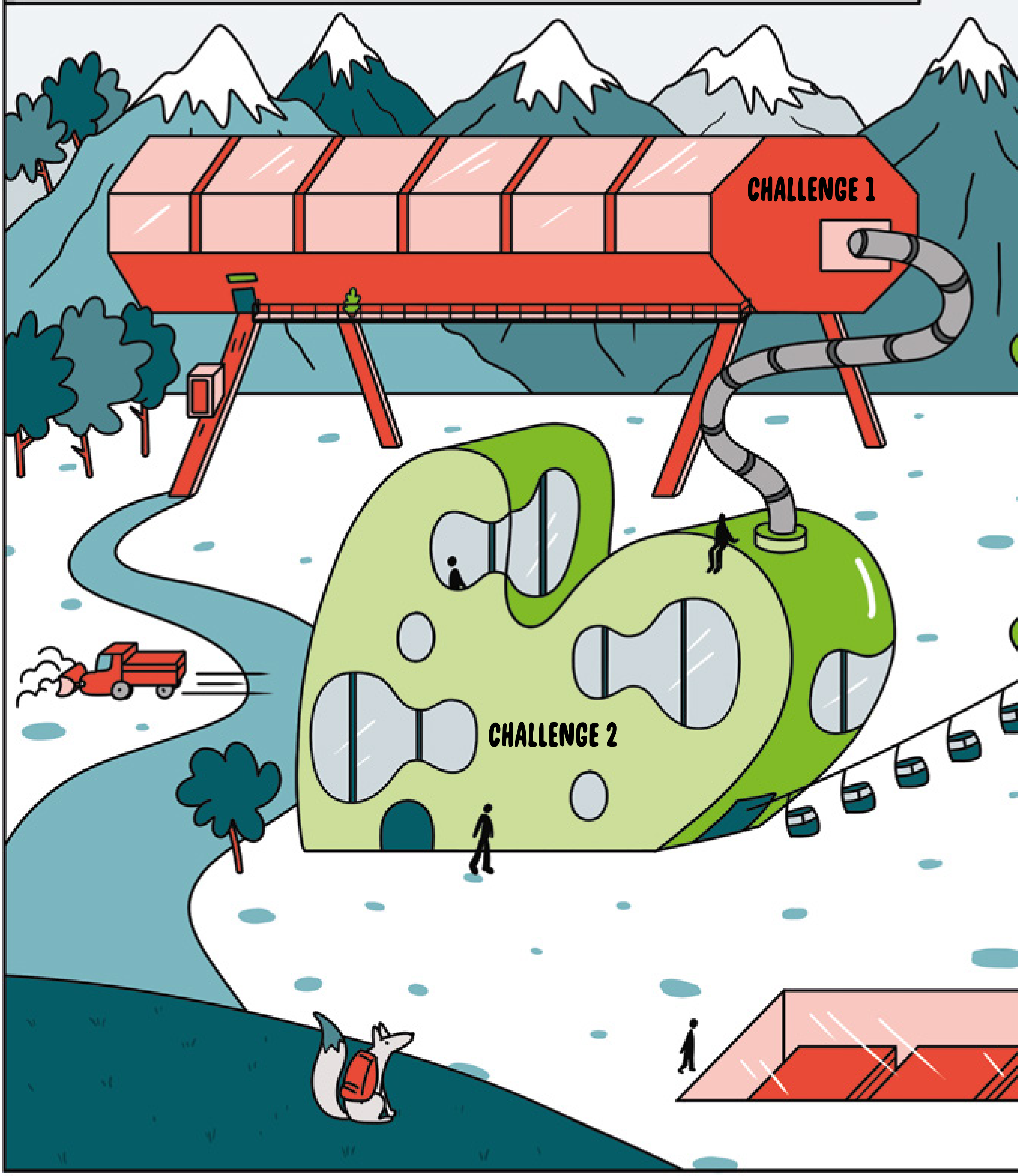
HUB D “Usability”: Focusing on usable security and privacy and researching the interface between humans and technology.

Each HUB addresses specific major research challenges that have been carefully selected to address security issues critical to the protection against large-scale attackers. The challenges of HUB A are:

Research Challenge 1: Cryptography Against Mass Surveillance
Research Challenge 2: Quantum-Resistant Cryptography
Research Challenge 3: Foundations of Privacy


I'M STARVING, AUNTY. I WOULD GIVE ANYTHING FOR SOME CANDY!
I KNOW, MY DEAR! WINTER WILL BE OVER SOON. BUT... WAIT. WHAT'S THAT SMELL?
The winter has been cold and going on for months. Whitfield the fox is hungry and bored.
THAT SMELLS WONDERFUL! IT TAKES ME BACK TO MY FAVORITE PASTRY SHOP.
He is naturally drawn to the delicious smell of cookies and lured into an adventure...
MMMM... SOMETHING IS DEFINITELY BEING COOKED UP IN THE CASA BUILDING BACK THERE IN THE MOUNTAINS.
I'M GOING TO GO AND SEE WHAT I CAN FIND...
I DON'T FEEL GOOD ABOUT THIS, IT'S SUCH A TRICKY PATH THROUGH THE HILLS.
A witty fox like Whitfield is very curious about all that can be found out there. Who knows...
JUST IMAGINE SOMETHING TO NIBBLE ON THAT BRINGS US THROUGH THE WINTER.
OH, BE CAREFUL! AND TRY NOT TO LEAVE TOO MANY TRACES!
Cookies might not be the only thing that he brings home.
I WONDER WHAT THEY HAVE BAKING IN THE OVENS HERE...

WELCOME TO RESEARCH HUB A



Content

CHALLENGE 1

Cryptography Against Mass Surveillance

How can we develop new cryptographic solutions that protect against mass surveillance?

CHALLENGE 2

Quantum-Resistant Cryptography

Can we find practical encryption and signature schemes that offer provable security against quantum computers?

CHALLENGE 3

Foundations of Privacy

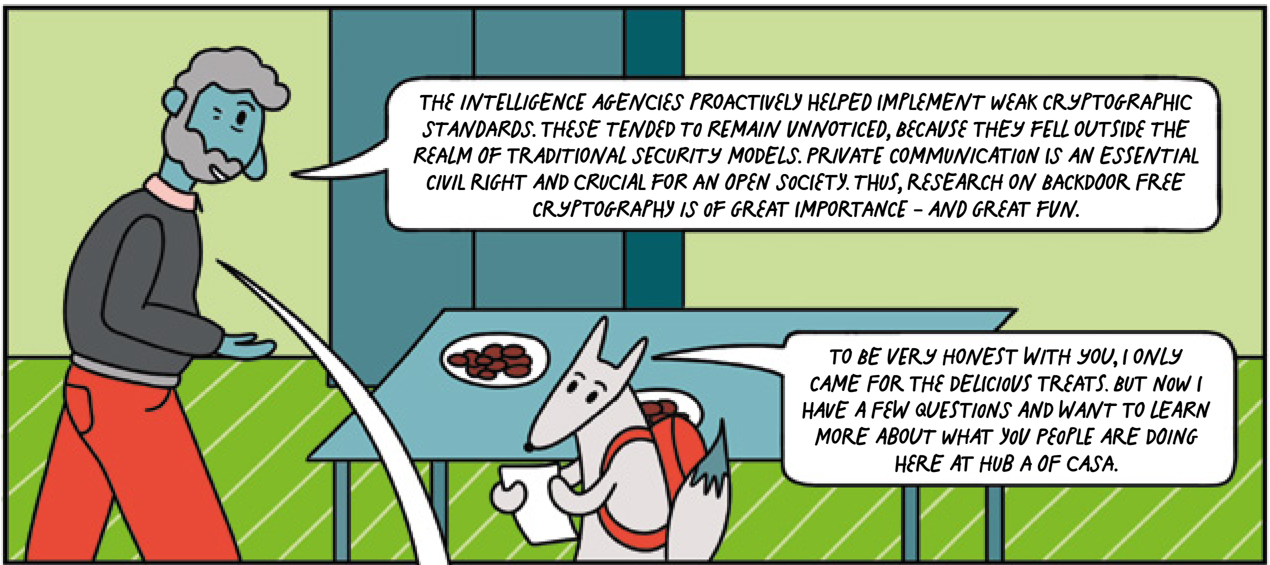
How can we use cryptography to protect our privacy when Big Data is stored in the Cloud?

CASA BACKGROUND

CASA stands for ‘Cyber Security in the Age of Large-Scale Adversaries’ and is funded as a Cluster of Excellence (EXC) within the Excellence Strategy of the DFG in Germany. Its goal is to enable sustainable security against sophisticated large-scale attacks. Therefore, an interdisciplinary team explores not only technical, but also social factors and implications. The Cluster of Excellence is located at Ruhr University Bochum.

casa.rub.de


CRYPTOGRAPHY AGAINST MASS SURVEILLANCE
THE FRONT DOOR IS LOCKED!
AND THE SMELL SEEMS TO BE COMING RIGHT OUTTA THE WALL. BUT I CAN'T SEE ANY ENTRANCE. MY NOSE NORMALLY DOESN'T LET ME DOWN.
AHA! HERE IS A BACKDOOR – QUITE WELL HIDDEN. AND LUCKY ME: HERE ARE THE COOKIES. OH, THANK YOU, WONDERFUL NOSE.
OH, YES!
HEY! YOU!
HUH?
DID YOU THINK YOU COULD JUST WALK IN HERE AND NICK THE SWEETS FOR TONIGHT'S CELEBRATION WITHOUT BEING NOTICED?
EHM, WELL... I CAME THROUGH THE HIDDEN BACKDOOR AND I JUST FOLLOWED THE TRACE OF THE COOKIES.
I'M MONI, BY THE WAY. AND IT JUST SO HAPPENS THAT WE WORK ON HIDDEN BACKDOORS IN SOFTWARE AND ELECTRONIC DEVICES HERE AT HUB A.
DO YOU KNOW THE SNOWDEN DOCUMENTS? THEY PROVED THAT NATION STATES HAVE BEEN EXPLOITING TECHNOLOGY TO PERFORM MASS SURVEILLANCE ON BOTH THEIR OWN AND OTHER STATES' CITIZENS. SOME OF THEIR ACTIONS CONCERN THE DOMAIN OF CRYPTOGRAPHY.
WOW, THATS A BIG STACK OF DOCUMENTS. CAN YOU GIVE ME THE GIST?



1 We will study on how to guarantee that cryptographic standards are backdoor free.

2 We will study past and ongoing cryptographic standards to identify adversarially planted backdoors.

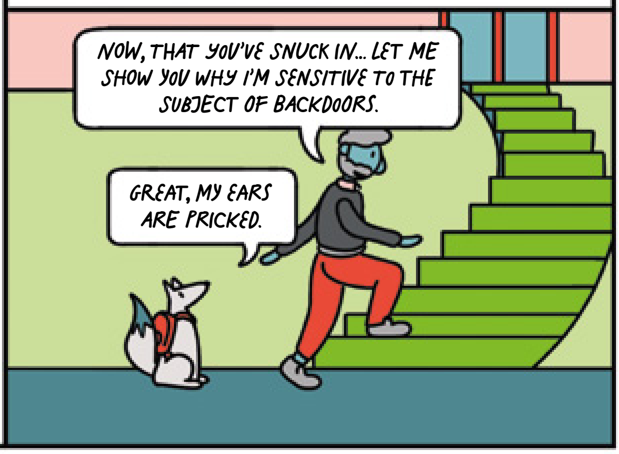
3 We will develop novel approaches for safe parameter generation that can provably withstand parameter subversion attacks and backdoors.

CASA WIKI

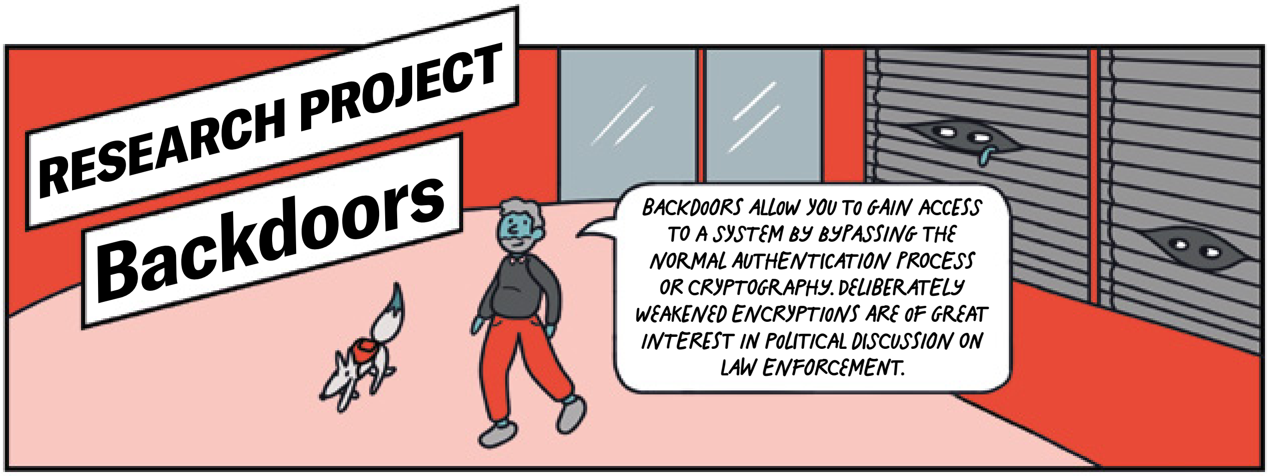
Backdoors allow access to computer systems without the the owner's permission. They can result from faulty programming or be intentionally built into software and hardware.

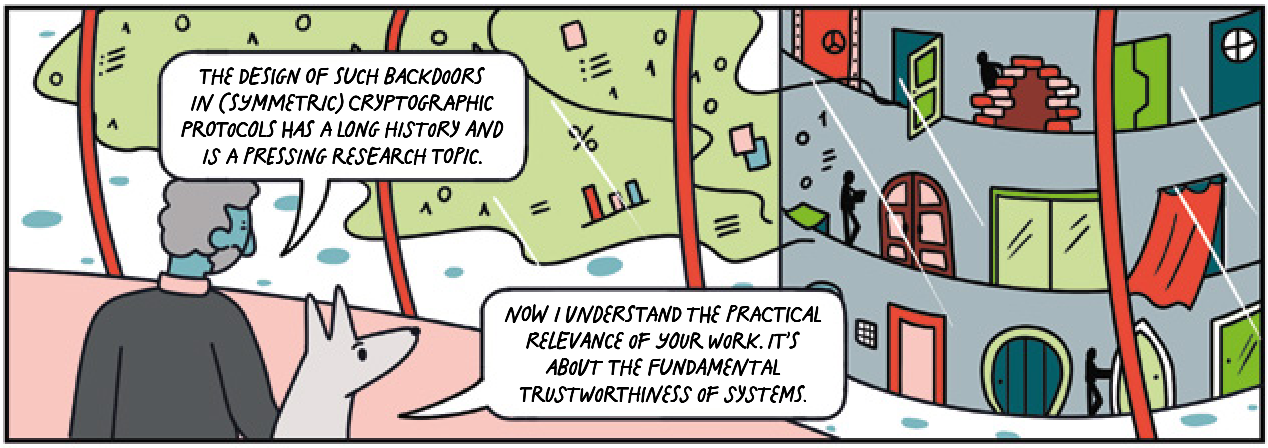
Cryptography is about secure electronic communication in the presence of malicious third parties. The most commonly used cryptography is encryption and signatures.

Cryptographic standards are technical standards that help to maximize the compatibility, interoperability, and security of encryption.



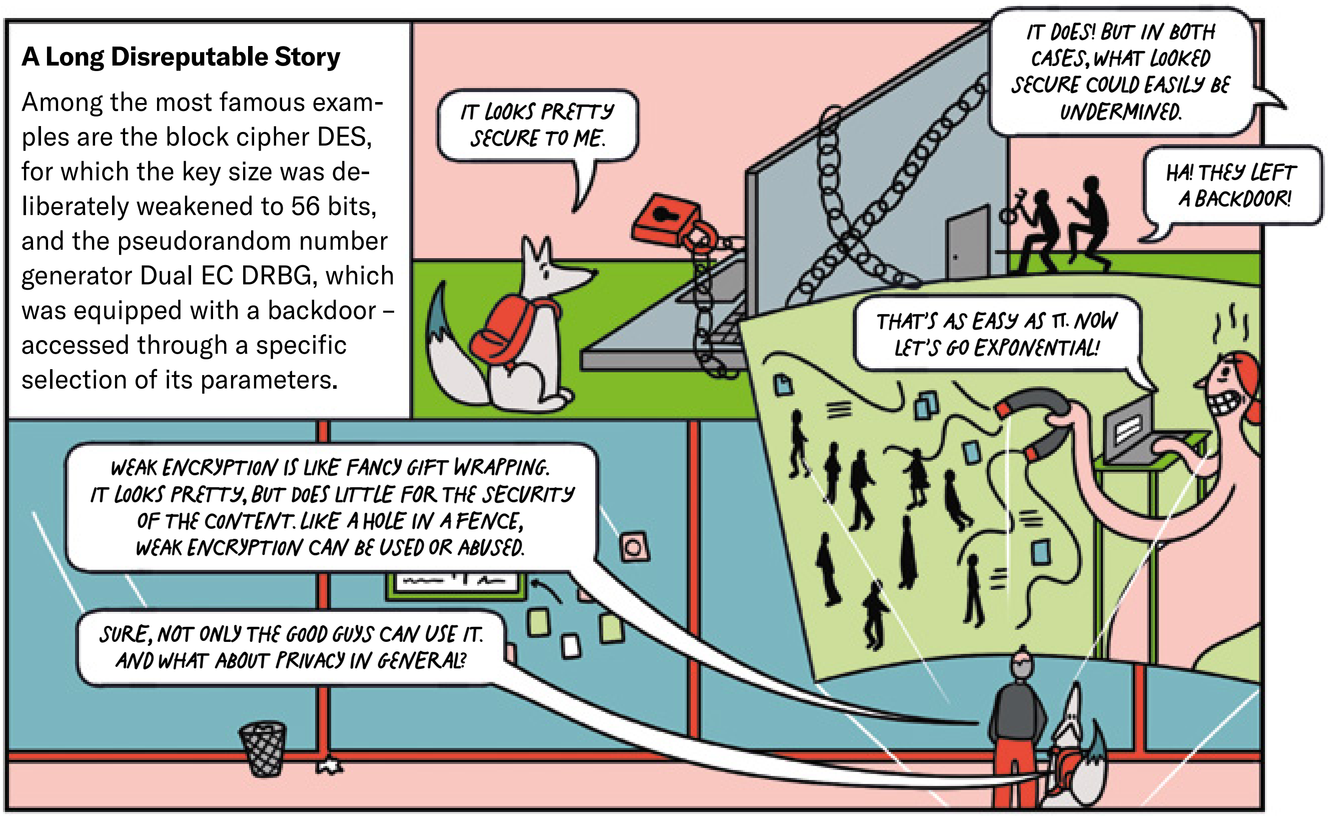
RESEARCH PROJECT
Backdoors





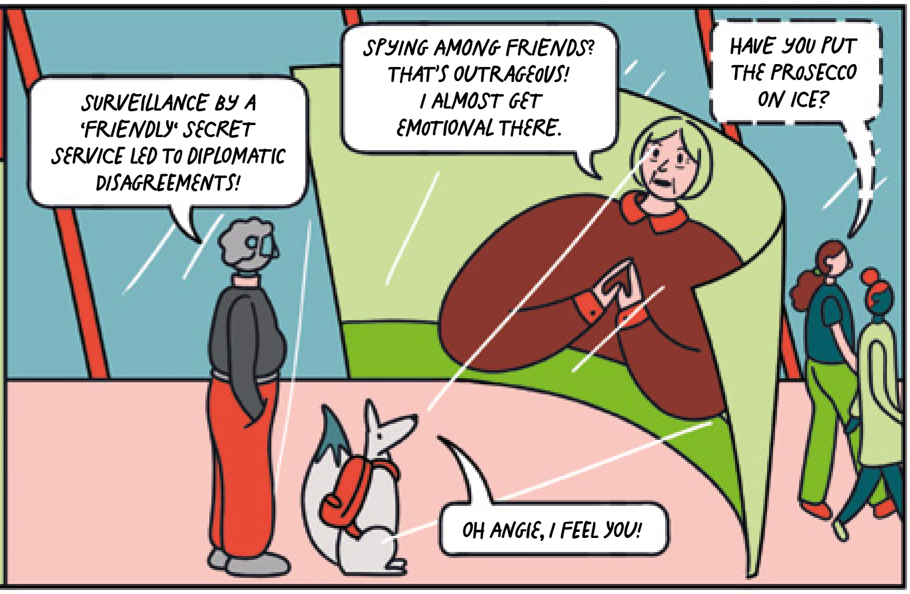
A Long Disreputable Story

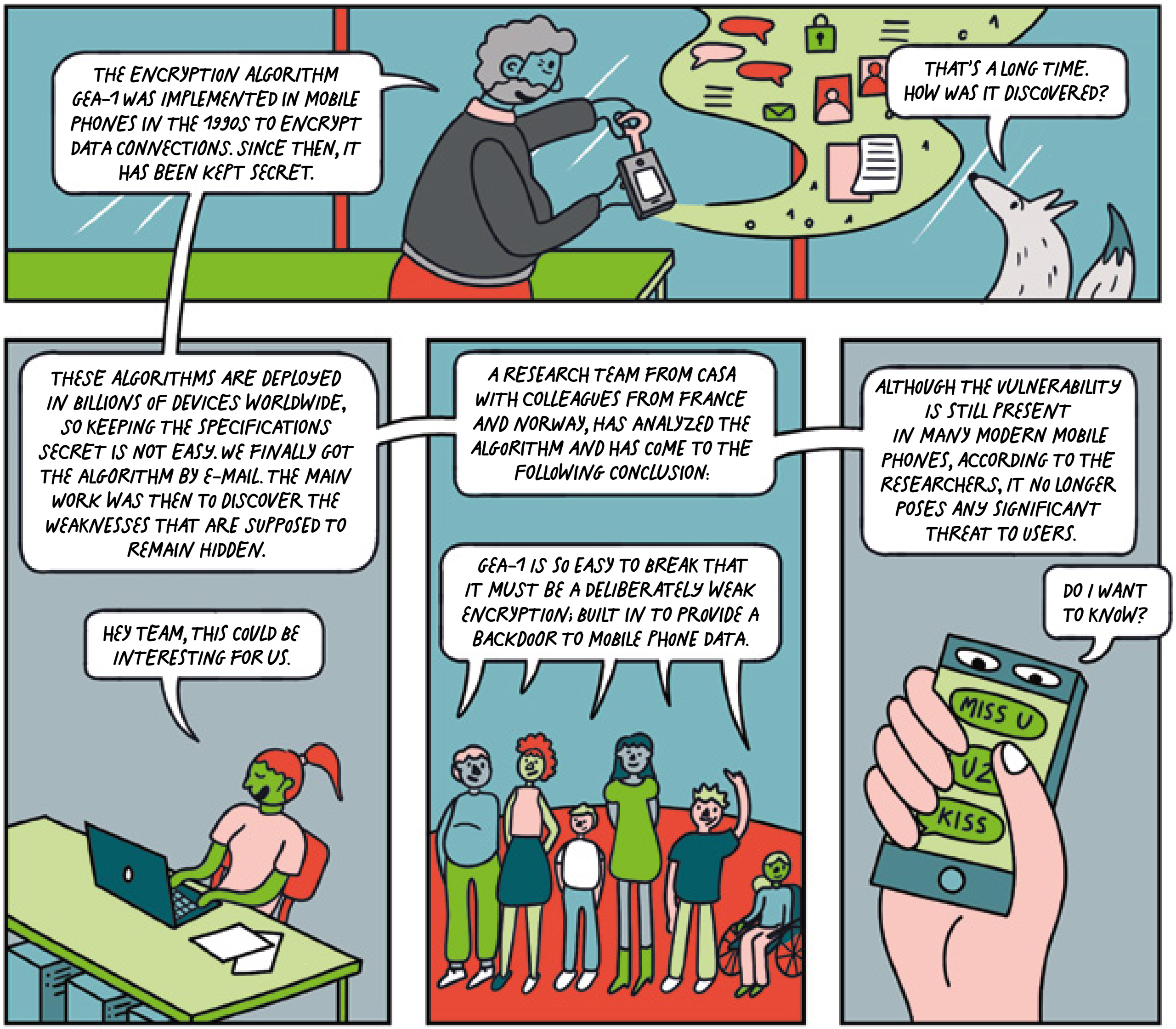
Among the most famous examples are the block cipher DES, for which the key size was deliberately weakened to 56 bits, and the pseudorandom number generator Dual EC DRBG, which was equipped with a backdoor – accessed through a specific selection of its parameters.

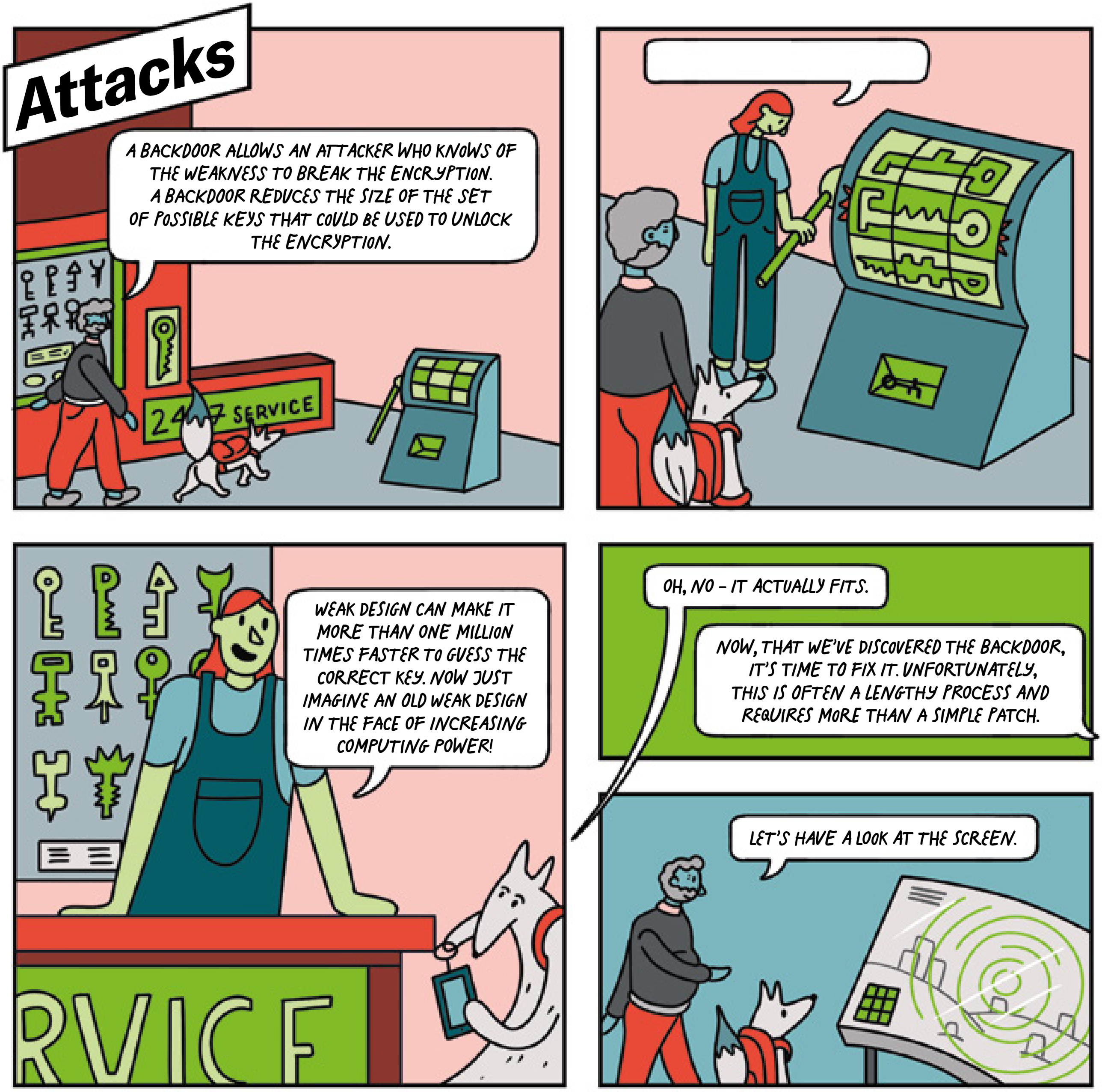


REAL LIFE STORY

In 2015, WikiLeaks presented evidence that the NSA had been wire-tapping the mobile phone of former chancellor Angela Merkel since 2002. The spying operation was also not restricted to her: the phones of 125 high-ranking politicians and advisors were also tapped.







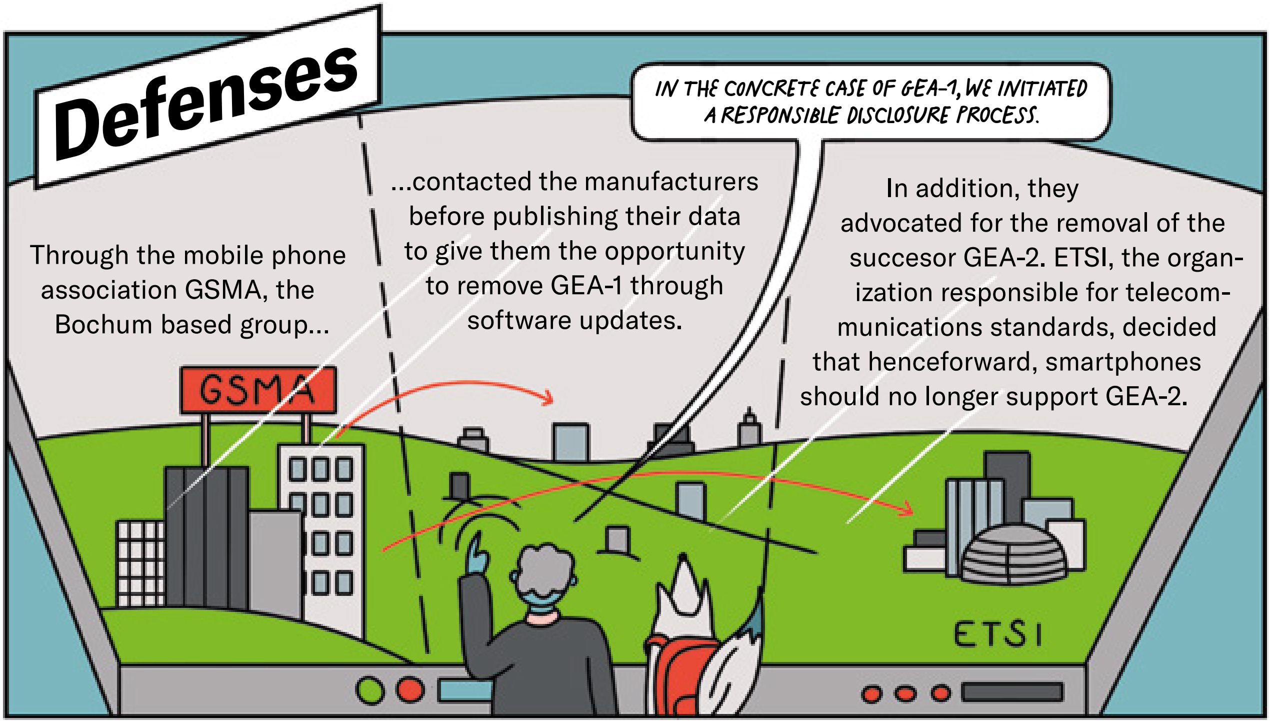
CASA WIKI

Symmetric Encryption uses the same key for encryption and decryption. It is well suited for bulk encryption as it is fast and needs few resources.

NIST is the US-based National Institute of Standards and Technology.

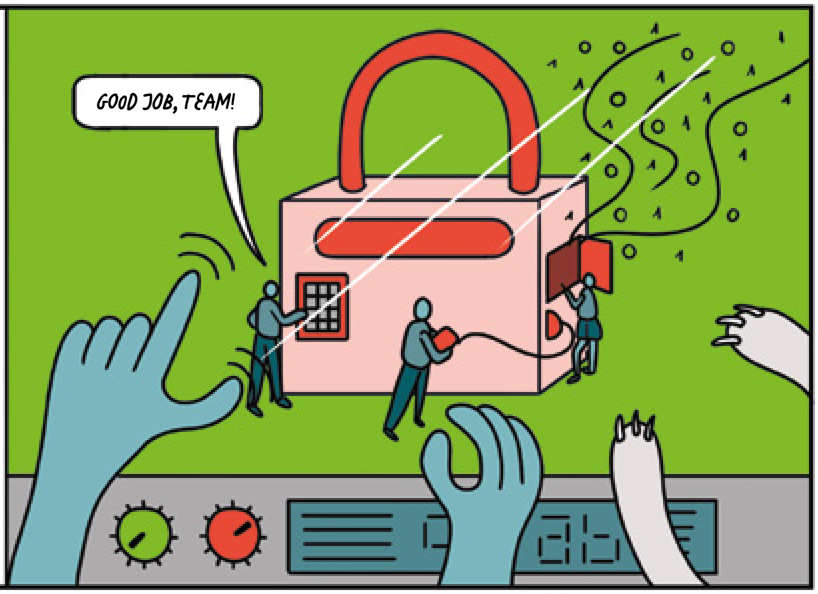
Good Symmetric Encryption

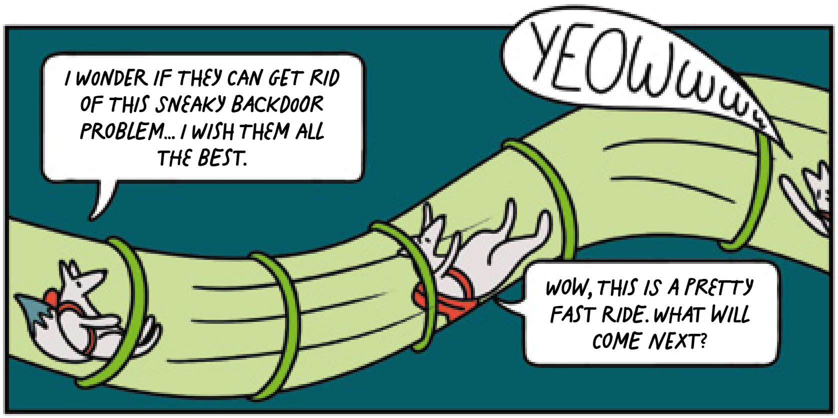
- Everything is known about the algorithm but the key.
- Without the key, no information about the plaintext can be gained from the ciphertext.
- The number of keys is too large to be guessed.



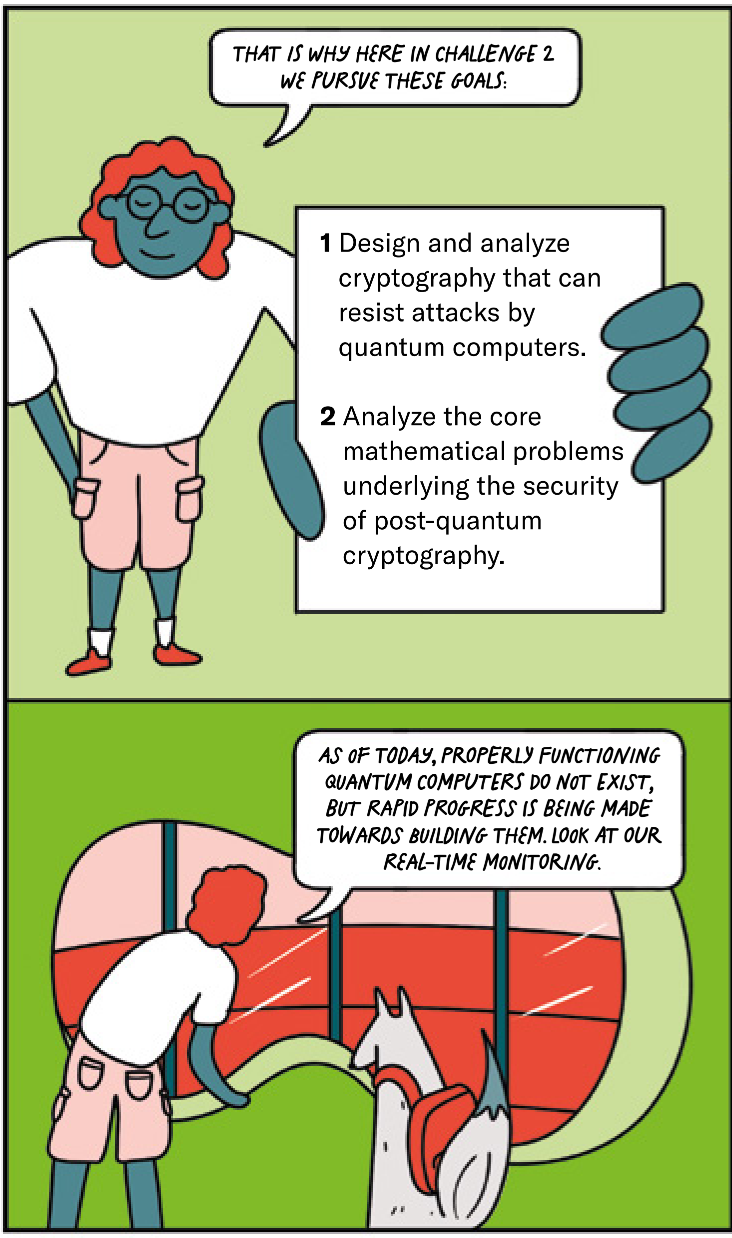
Why Transparency helps Security

In general, cryptographic algorithms should not be developed in secret and with unclear design components. NIST has lead the way in their process of selecting the Advanced Encryption Standard (AES) and upcoming post-quantum algorithms: using open design competitions followed by public discussions and analysis. It sounds contradictory but security gets better the more it is developed in public.





QUANTUM-RESISTANT CRYPTOGRAPHY



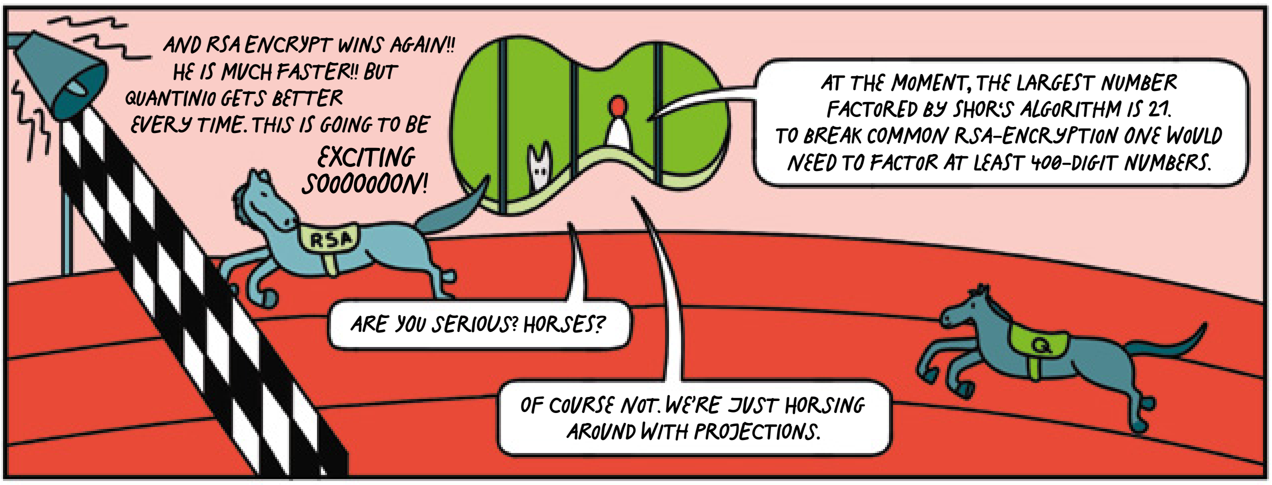
CASA WIKI

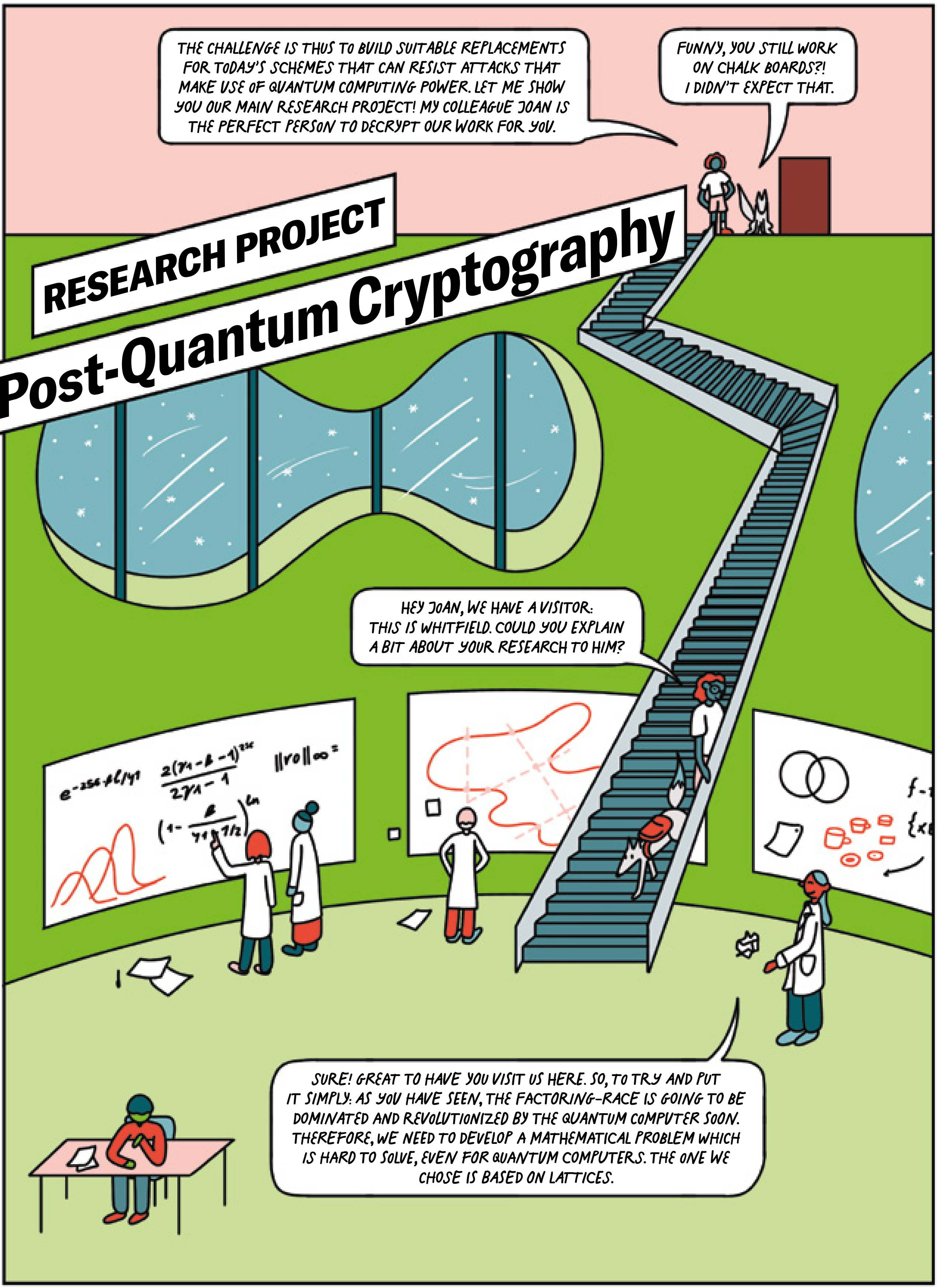
A **Quantum Compute**r is a computer that exploits the laws of quantum mechanics in order to solve certain problems faster. For example, it could quickly break all currently deployed asymmetric cryptography. Scalable quantum computers do not yet exist but the larger research community is making great progress in building them.

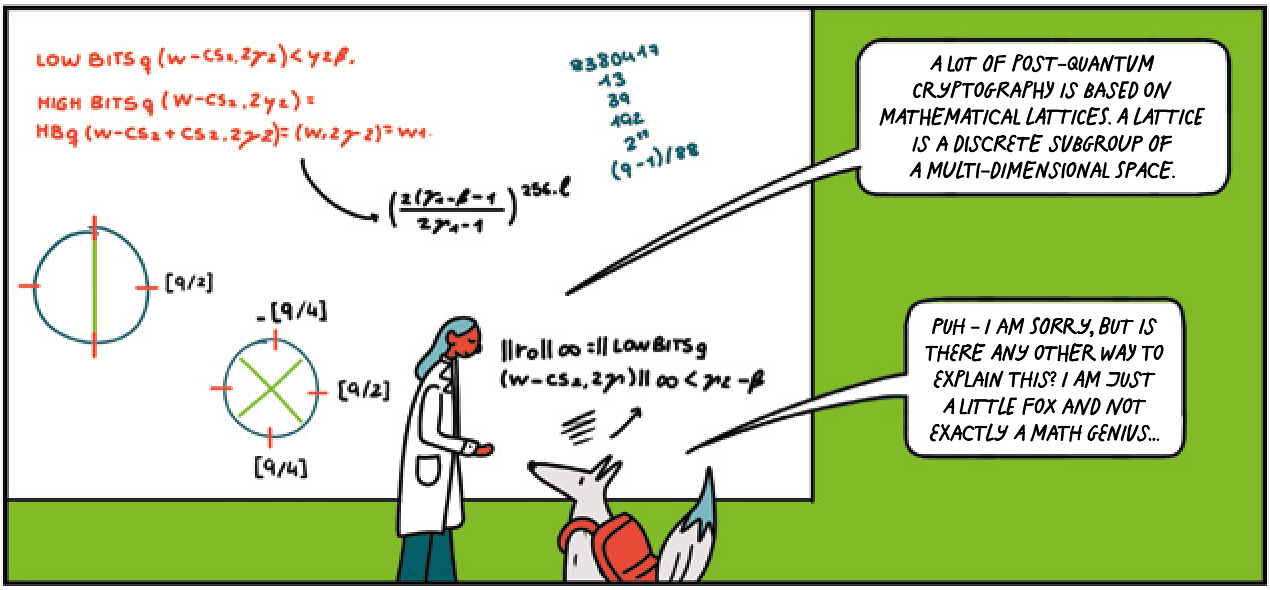
Post-Quantum Cryptography refers to cryptographic systems that can withstand attackers equipped with quantum computers.

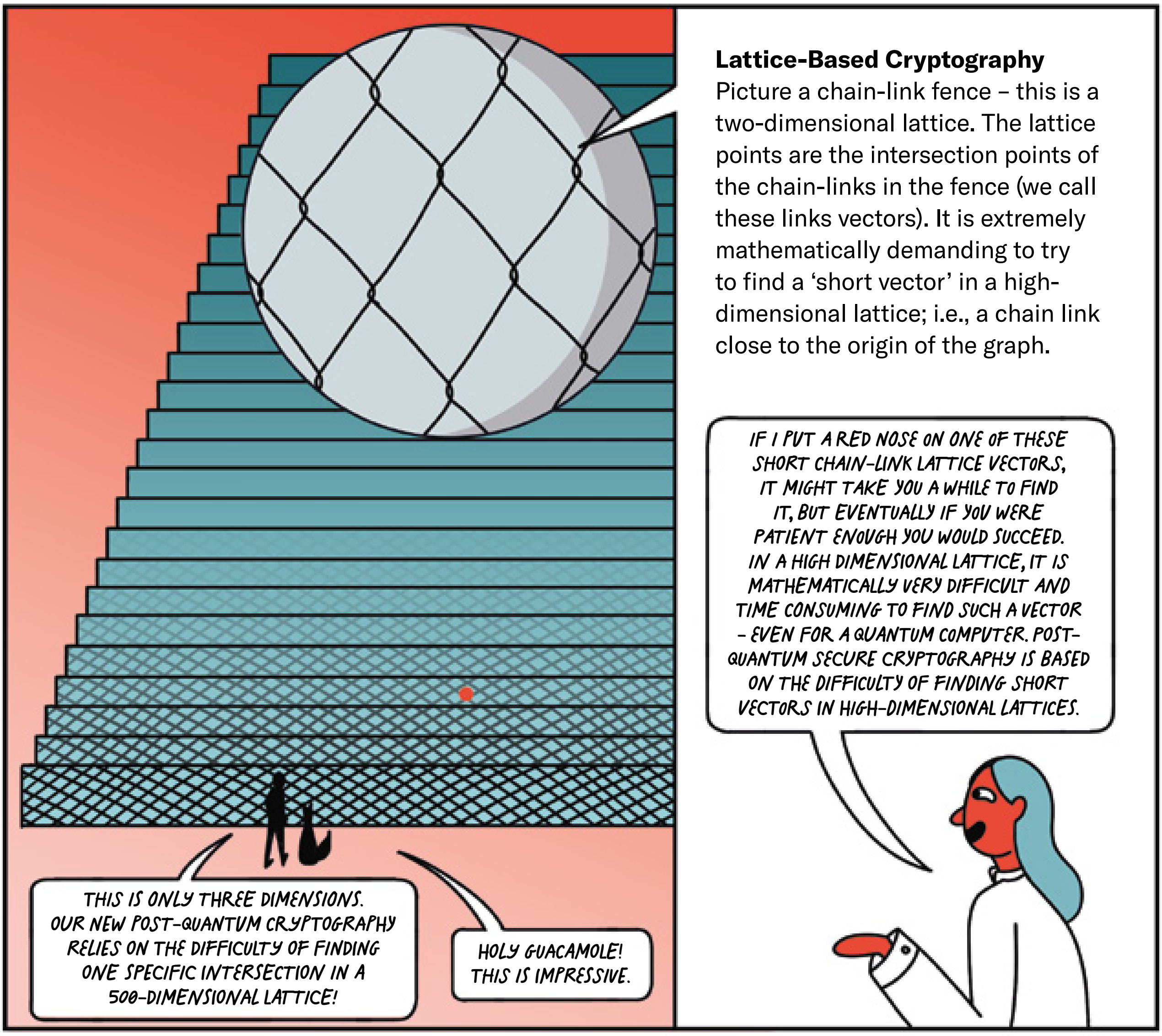
Shor's algorithm is an algorithm designed by Peter Shor in 1994 that can efficiently factor large integers and compute discrete logarithms over elliptic curves: Thus, essentially providing the framework to break all currently deployed public-key cryptography schemes.

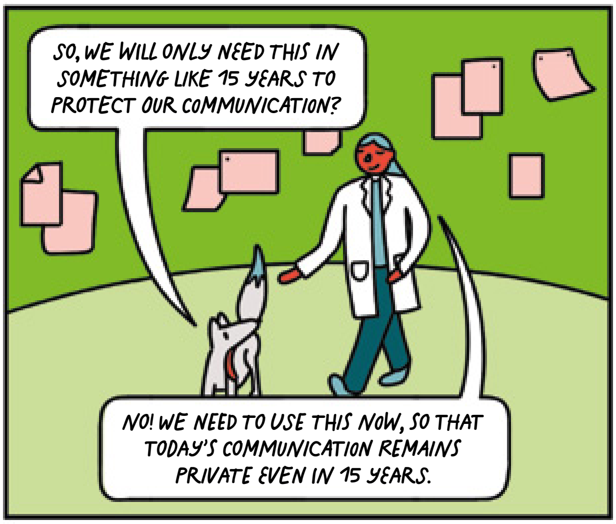
Asymmetric Cryptography uses a public key for encryption and a private key for decryption. It is mostly used for key agreement between parties that have not previously met.




THE CHALLENGE IS THUS TO BUILD SUITABLE REPLACEMENTS FOR TODAY'S SCHEMES THAT CAN RESIST ATTACKS THAT MAKE USE OF QUANTUM COMPUTING POWER. LET ME SHOW YOU OUR MAIN RESEARCH PROJECT! MY COLLEAGUE JOAN IS THE PERFECT PERSON TO DECRYPT OUR WORK FOR YOU.
FUNNY, YOU STILL WORK ON CHALK BOARDS?! I DIDN'T EXPECT THAT.
RESEARCH PROJECT
Post-Quantum Cryptography
HEY JOAN, WE HAVE A VISITOR: THIS IS WHITFIELD. COULD YOU EXPLAIN A BIT ABOUT YOUR RESEARCH TO HIM?
SURE! GREAT TO HAVE YOU VISIT US HERE. SO, TO TRY AND PUT IT SIMPLY: AS YOU HAVE SEEN, THE FACTORING-RACE IS GOING TO BE DOMINATED AND REVOLUTIONIZED BY THE QUANTUM COMPUTER SOON. THEREFORE, WE NEED TO DEVELOP A MATHEMATICAL PROBLEM WHICH IS HARD TO SOLVE, EVEN FOR QUANTUM COMPUTERS. THE ONE WE CHOSE IS BASED ON LATTICES.

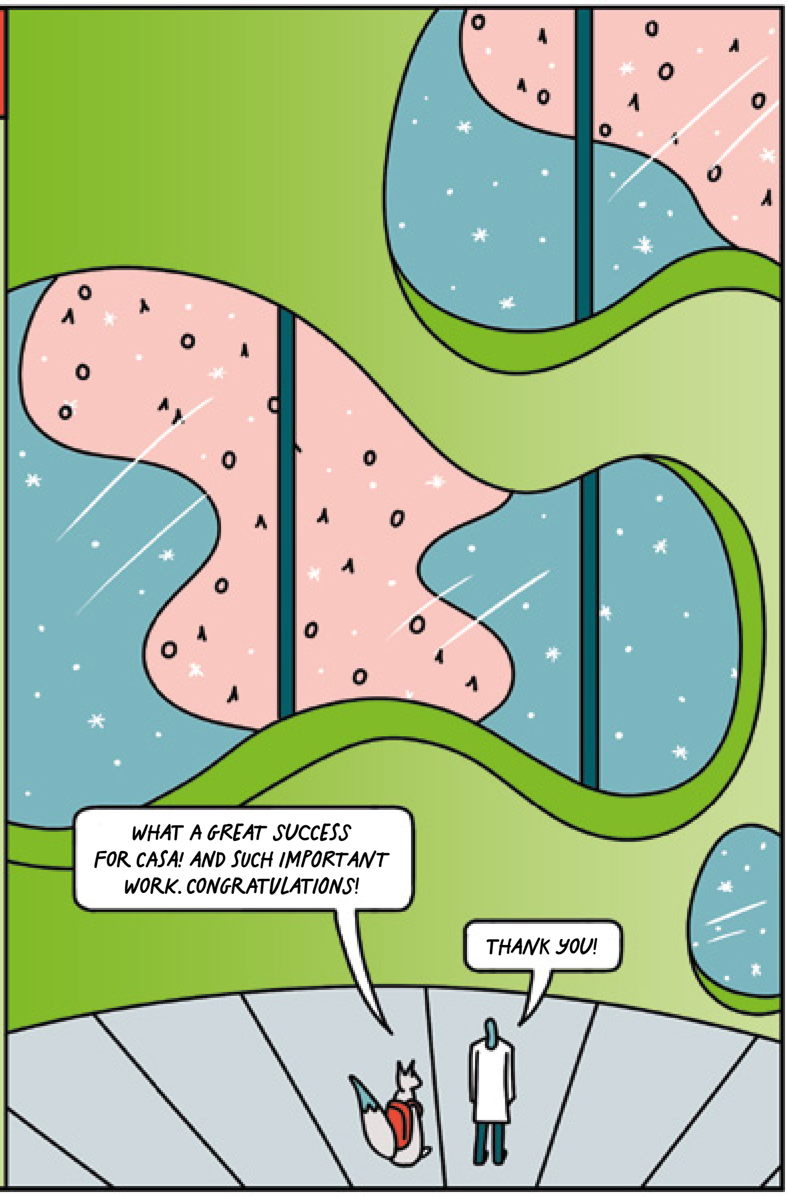

A LOT OF POST-QUANTUM CRYPTOGRAPHY IS BASED ON MATHEMATICAL LATTICES. A LATTICE IS A DISCRETE SUBGROUP OF A MULTI-DIMENSIONAL SPACE.
PUH – I AM SORRY, BUT IS THERE ANY OTHER WAY TO EXPLAIN THIS? I AM JUST A LITTLE FOX AND NOT EXACTLY A MATH GENIUS...

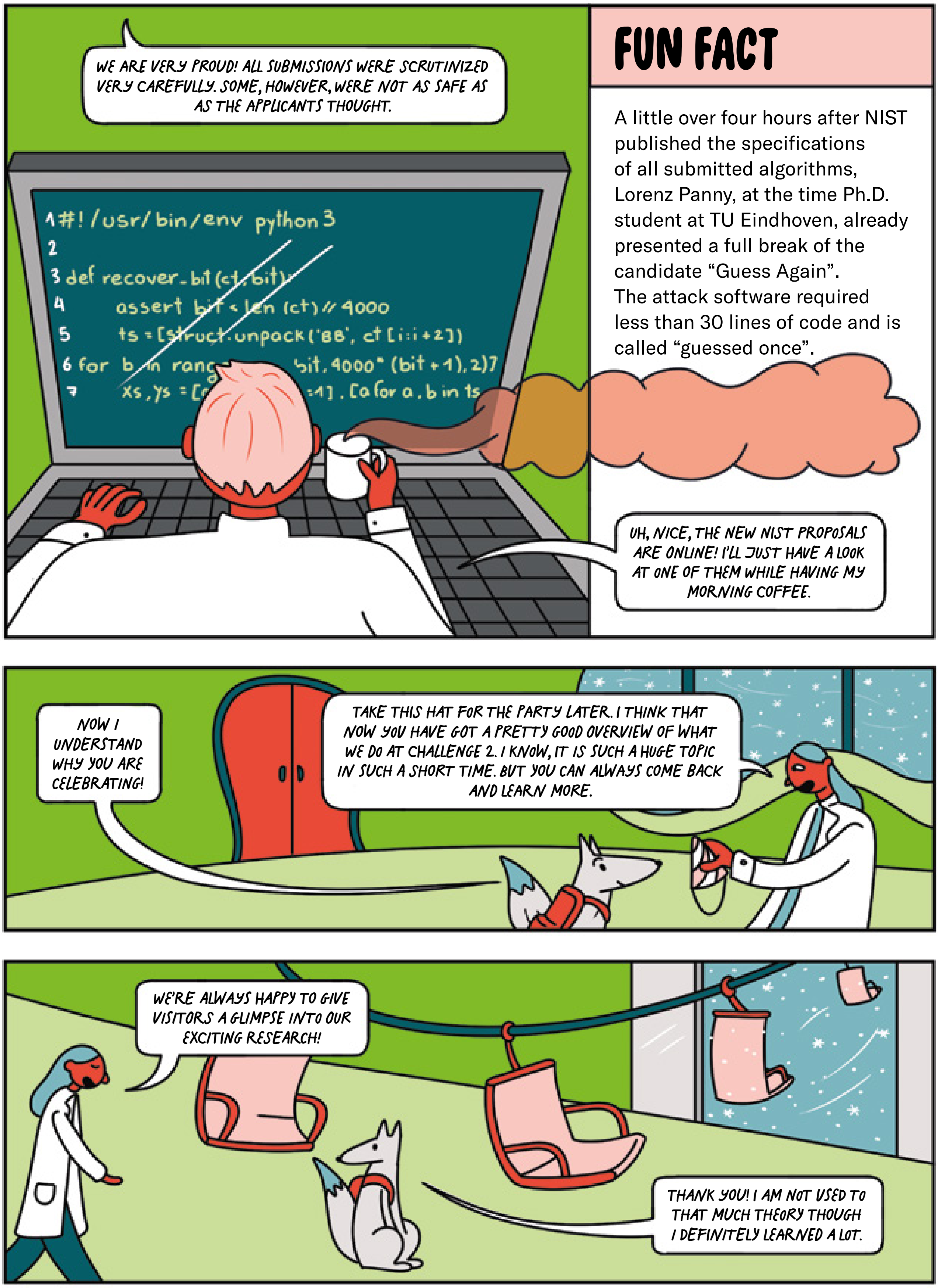

Lattice-Based Cryptography
Picture a chain-link fence – this is a two-dimensional lattice. The lattice points are the intersection points of the chain-links in the fence (we call these links vectors). It is extremely mathematically demanding to try to find a 'short vector' in a high-dimensional lattice; i.e., a chain link close to the origin of the graph.
IF I PUT A RED NOSE ON ONE OF THESE SHORT CHAIN-LINK LATTICE VECTORS, IT MIGHT TAKE YOU A WHILE TO FIND IT, BUT EVENTUALLY IF YOU WERE PATIENT ENOUGH YOU WOULD SUCCEED. IN A HIGH DIMENSIONAL LATTICE, IT IS MATHEMATICALLY VERY DIFFICULT AND TIME CONSUMING TO FIND SUCH A VECTOR – EVEN FOR A QUANTUM COMPUTER. POST-QUANTUM SECURE CRYPTOGRAPHY IS BASED ON THE DIFFICULTY OF FINDING SHORT VECTORS IN HIGH-DIMENSIONAL LATTICES.
THIS IS ONLY THREE DIMENSIONS. OUR NEW POST-QUANTUM CRYPTOGRAPHY RELIES ON THE DIFFICULTY OF FINDING ONE SPECIFIC INTERSECTION IN A 500-DIMENSIONAL LATTICE!
HOLY GUACAMOLE! THIS IS IMPRESSIVE.



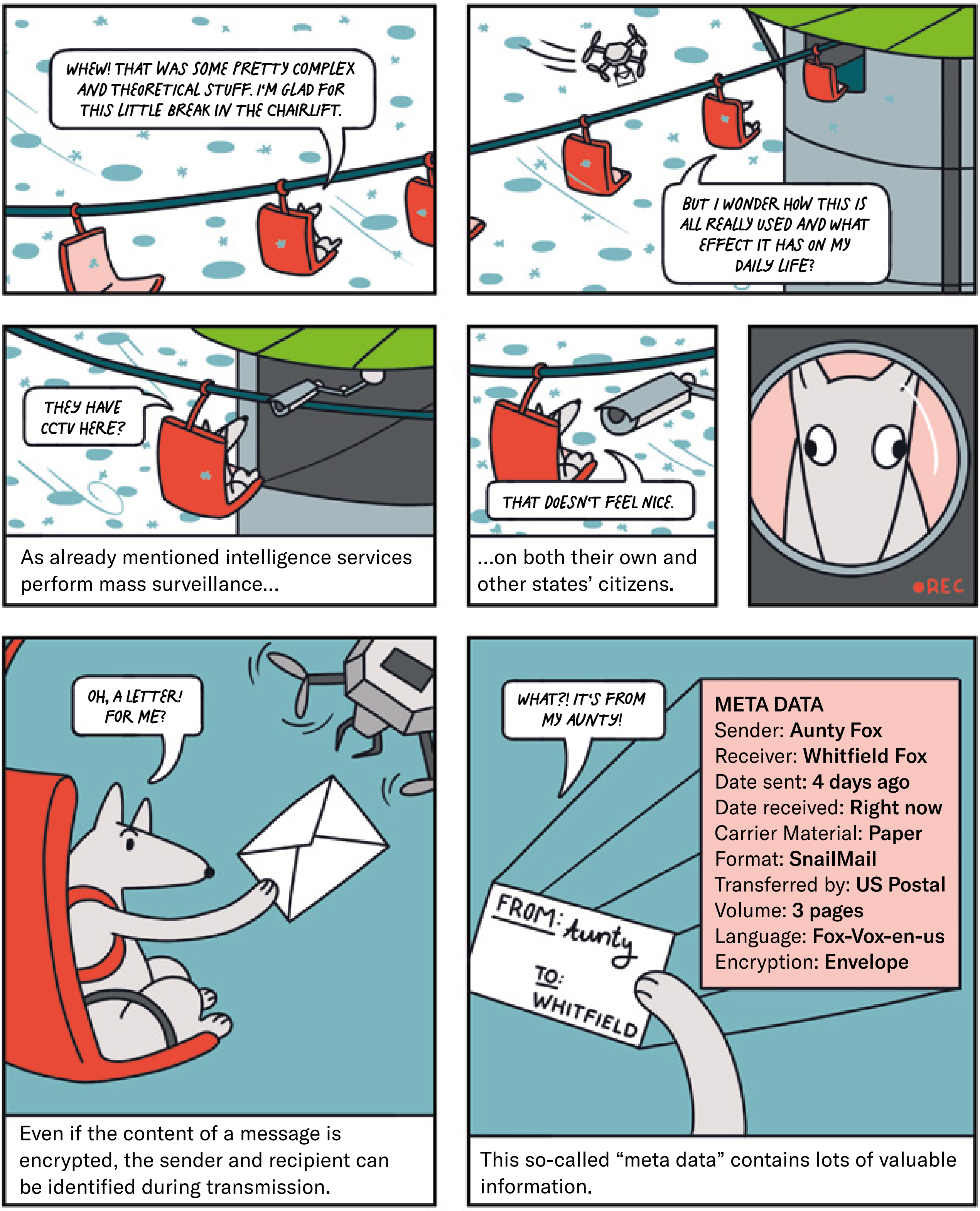
REAL LIFE STORY

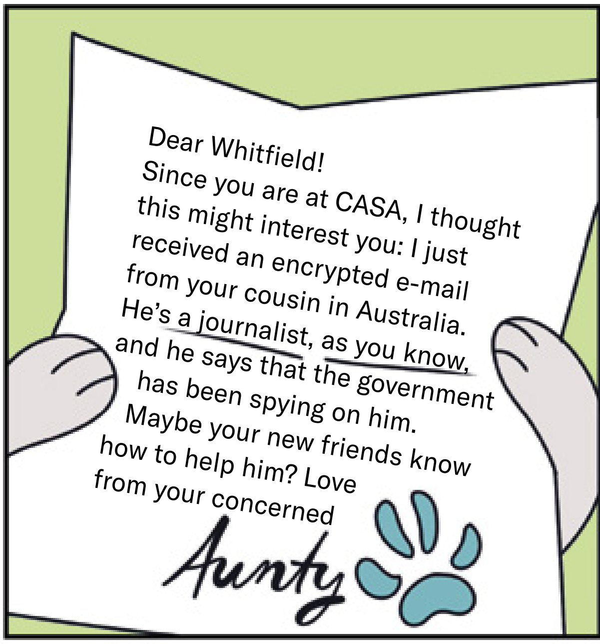
The American National Institute for Standards and Technology (NIST) has recognized the risks for secure data encryption posed by quantum computers and, in 2016, started a process to standardize post-quantum cryptography. 69 proposals were submitted from the research community world-wide which were evaluated in a public process. In July 2022, four of these were selected to be standardized by NIST: three digital signature schemes and one public-key encryption system. CASA researchers contributed to three of the four systems: CRYSTALS-Dilithium, SPHINCS+ and CRYSTALS-Kyber.




WE ARE VERY PROUD! ALL SUBMISSIONS WERE SCRUTINIZED VERY CAREFULLY. SOME, HOWEVER, WERE NOT AS SAFE AS AS THE APPLICANTS THOUGHT.
1#!/usr/bin/env python3
2
3 def recover_bit(ct, bit):
4 assert bit < len(ct) // 4000
5 ts = [struct.unpack('BB', ct[i:i+2])
FUN FACT
A little over four hours after NIST published the specifications of all submitted algorithms, Lorenz Panny, at the time Ph.D. student at TU Eindhoven, already presented a full break of the candidate “Guess Again”. The attack software required less than 30 lines of code and is called “guessed once”.
UH, NICE, THE NEW NIST PROPOSALS ARE ONLINE! I'LL JUST HAVE A LOOK AT ONE OF THEM WHILE HAVING MY MORNING COFFEE.
NOW I UNDERSTAND WHY YOU ARE CELEBRATING!
TAKE THIS HAT FOR THE PARTY LATER. I THINK THAT NOW YOU HAVE GOT A PRETTY GOOD OVERVIEW OF WHAT WE DO AT CHALLENGE 2. I KNOW, IT IS SUCH A HUGE TOPIC IN SUCH A SHORT TIME. BUT YOU CAN ALWAYS COME BACK AND LEARN MORE.
WE'RE ALWAYS HAPPY TO GIVE VISITORS A GLIMPSE INTO OUR EXCITING RESEARCH!
THANK YOU! I AM NOT USED TO THAT MUCH THEORY THOUGH I DEFINITELY LEARNED A LOT.

FOUNDATIONS OF PRIVACY

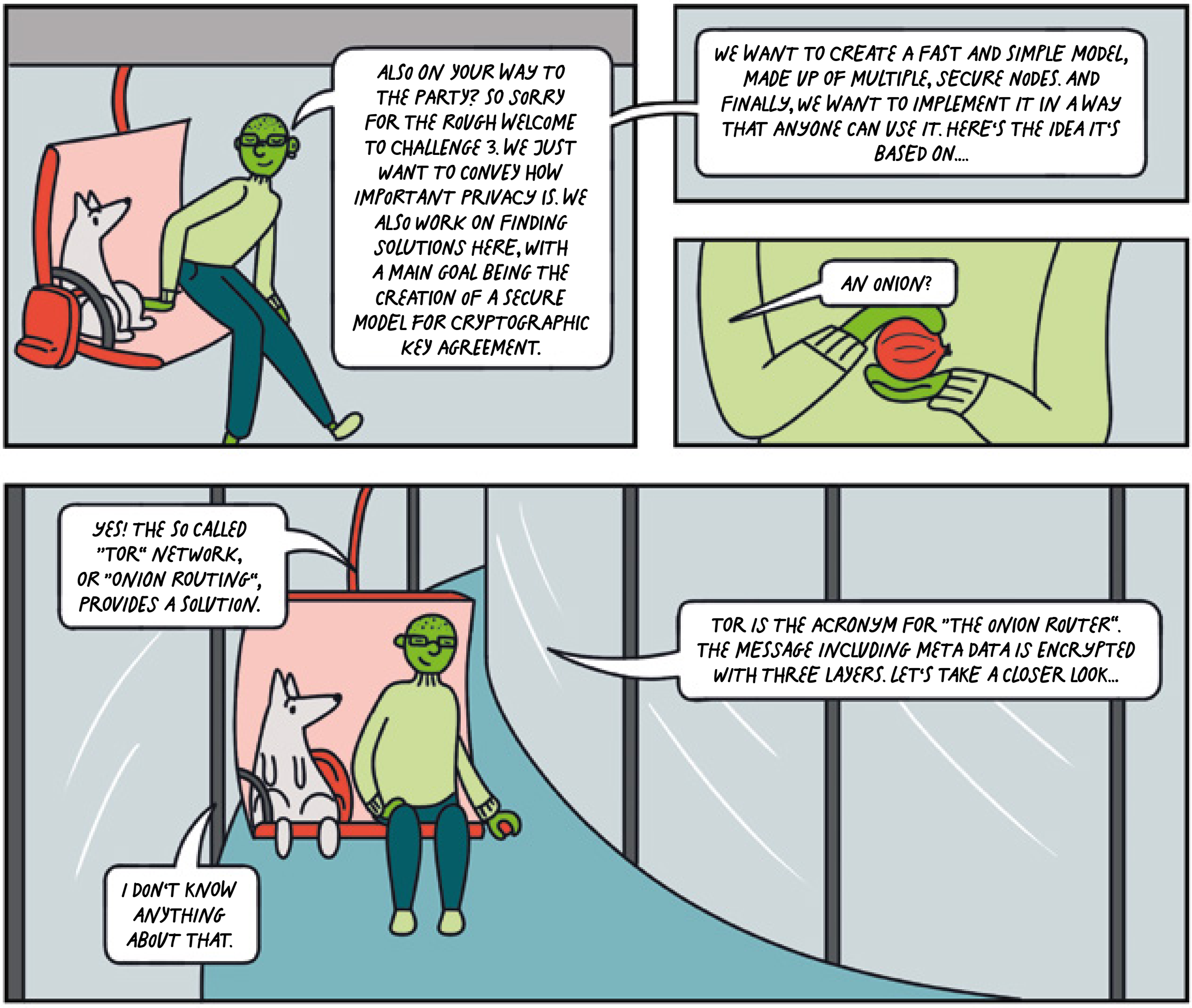


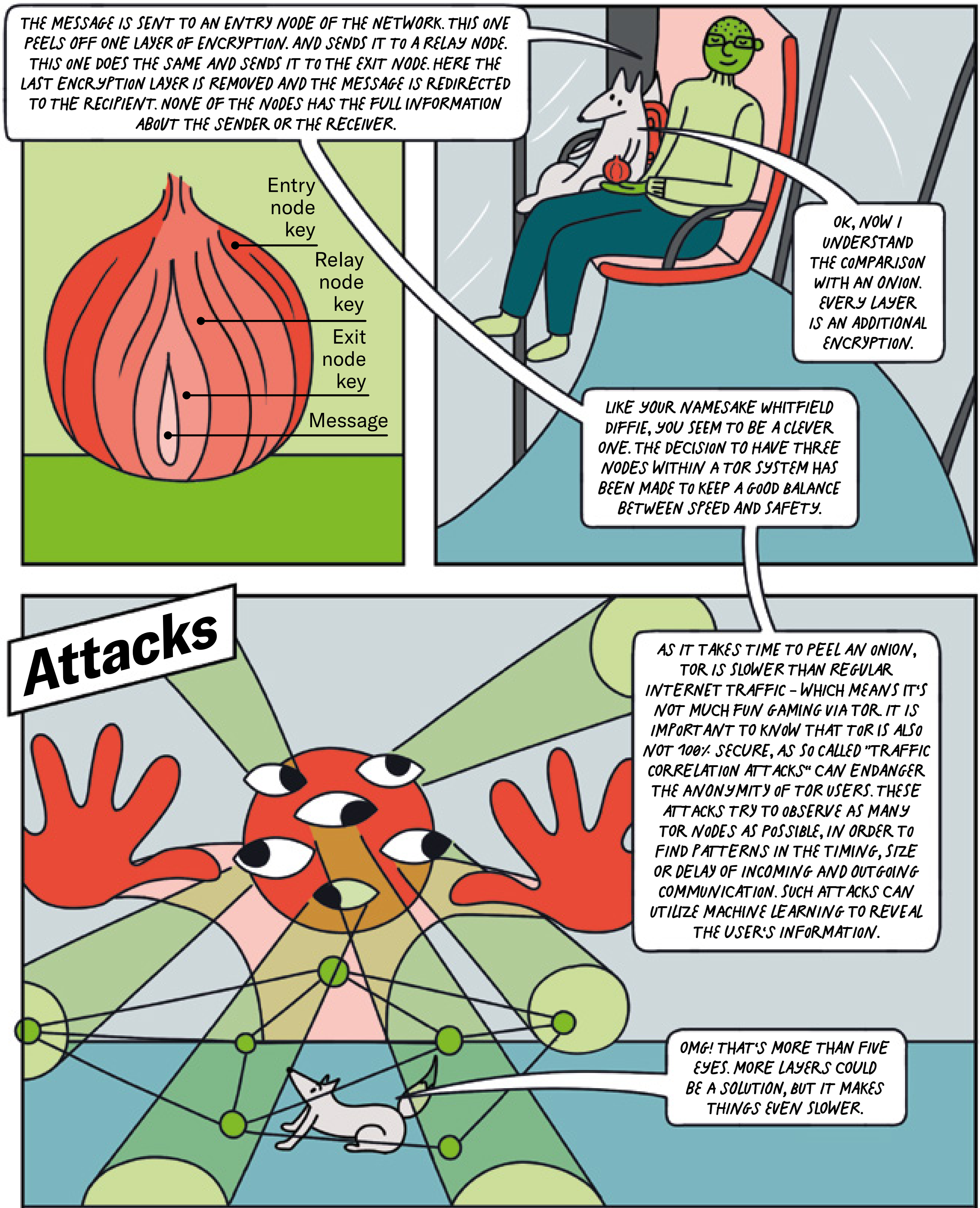


REAL LIFE STORY

In 2016, Paul Farrell researched detention camps for refugees on the island Nauru, where the poor, inhumane conditions have been harshly criticized. Based on the government's Data Retention Act laws, the Australian Police were legally allowed to obtain and study all of his communication; under the grounds of identifying his sources and procuring information about potential whistle blowers. They also collected the meta data from Farrell's mobile phone and analyzed data from his e-mail account.

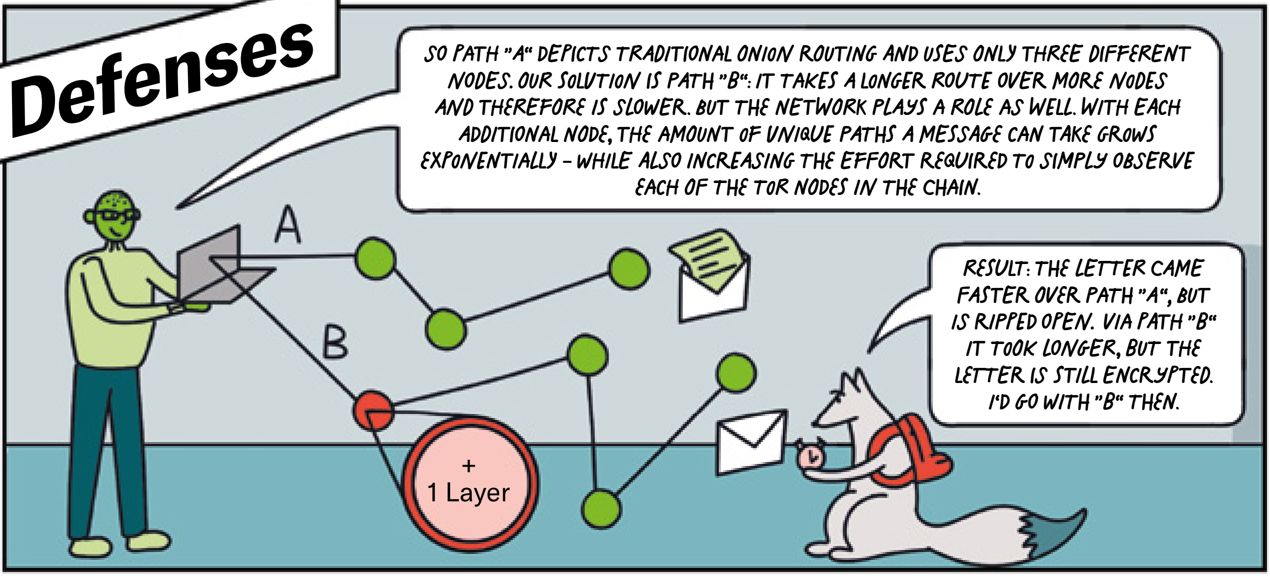
If such an invasion of private space is allowed in democracies, what kind of things are happening in authoritarian regimes?

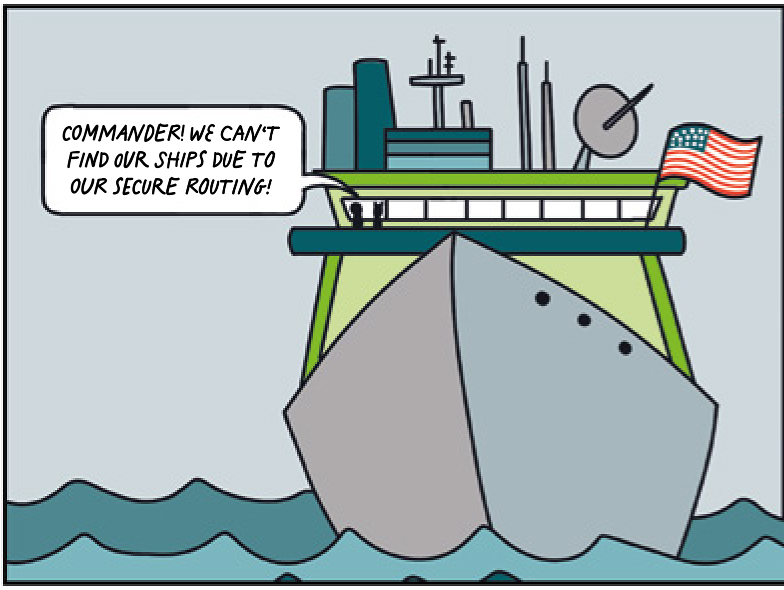




Even hidden nodes can be detected. Some Tor-specific code can be recognized using deep package inspection if a message is sent. Once the hidden node is known, it can be blocked. For example, China blocks all attempts to access entry nodes from within the country.

Defenses





FUN FACT

Despite its apparent enmity with Tor, the U.S. government played a pivotal role in its creation. Onion Routing, in it's most basic form, was developed by the U.S. Navy in the 1990s to protect intelligence communications. Also, the U.S. Department of State Bureau of Democracy, Human Rights and Labor is among Tor's financial backers.


CHEERS TO YOU! YOU HAVE DONE A GREAT JOB WITH LISTENING AND UNDERSTANDING OUR WORK!
WELL, I GUESS IT'S PROBABLY JUST THE TIP OF THE ICEBERG, ISN'T IT?
OH, AND BY THE WAY: I GOT THIS LETTER FROM MY AUNTY. SHE IS ASKING FOR SOME ADVICE.
LET ME SEE...
HMM. I THINK YOUR COUSIN ALREADY MADE THE FIRST STEP BY USING ENCRYPTED E-MAIL. HE SHOULD USE A TOR BROWSER AND SECURE MESSENGER AS WELL. EVEN NOW, CERTAIN SECURITY AND PRIVACY MECHANISMS CAN BE VERY INCONVENIENT TO USE – BUT OUR COLLEAGUES AT HUB D ARE WORKING ON THAT! MAYBE YOU SHOULD VISIT THEM SOMETIME TOO.
HEY, YOU TWO! STOP TALKING AND JOIN OUR BREAK-DANCE BATTLE!
IT SOUNDS REALLY TEMPTING, BUT I'LL HAVE TO PASS. MY AUNTY IS PROBABLY STARTING TO GET REALLY WORRIED.
SO, NOW I HAVE A BAG FULL OF COOKIES, MY HEAD FULL OF KNOWLEDGE AND EVEN SOME ANSWERS AND ADVICE FOR AUNTY. SHE WILL BE PROUD. AFTER ALL, I HAVE LEARNED THAT SECURITY IS NOT A STATE BUT A CONTINUOUS PROCESS. YOU HAVE TO TAKE FUTURE POSSIBILITIES INTO ACCOUNT. IT'S GOOD THAT THE PEOPLE AT CASA ARE TAKING CARE OF IT.

CASA: Cyber Security in the Age of Large-Scale Adversaries was established in 2019. It is the only Cluster of Excellence in the field of computer security in Germany. CASA is funded by a grant from the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) worth about 30 million Euros, which ensures excellent research conditions.

CASA brings together a core group of principal investigators, chosen with a strong focus on security and privacy, with selected top-level researchers from highly relevant neighboring disciplines. The team covers the full scope needed to tackle the challenging research problems in modern computer security; namely computer science, mathematics, electrical engineering, and psychology.

CASA is hosted by the Horst Görtz Institute for IT Security (hgi.rub.de/en), a pioneering research center in Germany. Furthermore, CASA collaborates strongly with the Max Planck Institute for Security and Privacy in Bochum (mpi-sp.org) and several other institutes and universities.

What is a "Cluster of Excellence"?
With the funding line "Clusters of Excellence", internationally competitive research centers at universities or university alliances in Germany are provided with project-based funding for a period of 7 years. Within the clusters, scientists from different disciplines and institutions work together on a research project. The funding gives them the opportunity to concentrate intensively on their research goal, to train young scientists and to recruit international top researchers.

casa.rub.de

TECHNICAL BACKGROUND

The concepts and methods presented in this comic were developed by researchers involved in the Cluster of Excellence CASA. If you are interested in more details, you can find the original publications online. These scientific papers explain the results in more detail. For many publications we also publish the source code and other research artifacts. Please reach out to us, if you have questions: info@casa.rub.de

PUBLICATIONS

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

2nd edition 2023

Editorial team
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
Illustrations: Lucia Cordero,
Hannah Schrage, David Ramirez Fernandez
Project Management: Martin Steffens

Cover image
Hannah Schrage

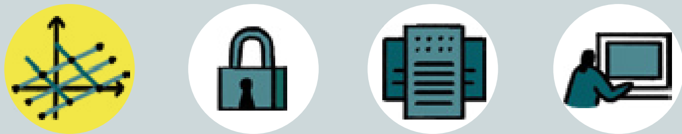
Printed at
Schmidt, Ley + Wiegandt GmbH + Co. KG,
Lünen, www.slw-medien.de

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

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

Scan to access the digital version of our comic:

CASA
Cyber Security in the Age of Large-Scale Adversaries
Gefördert durch
DFG Deutsche Forschungsgemeinschaft
Ruhr Universität Bochum
RUB
ellery studio



HUB A HUB B HUB C HUB D

WHAT IS SAFE TODAY MAY BE AN OPEN SECRET TOMORROW. THIS IS ESPECIALLY TRUE IN THE DIGITAL SPHERE: FROM MASS SURVEILLANCE AND POST-QUANTUM CRYPTOGRAPHY TO SAFE ROUTING AND ENCRYPTION.

FOLLOW THE CURIOUS LITTLE FOX WHITFIELD ON HIS CHASE THROUGH HUB A. WILL HE MANAGE ALL THE TWISTS AND TURNS ALONG THE WAY?

FIND OUT MORE!