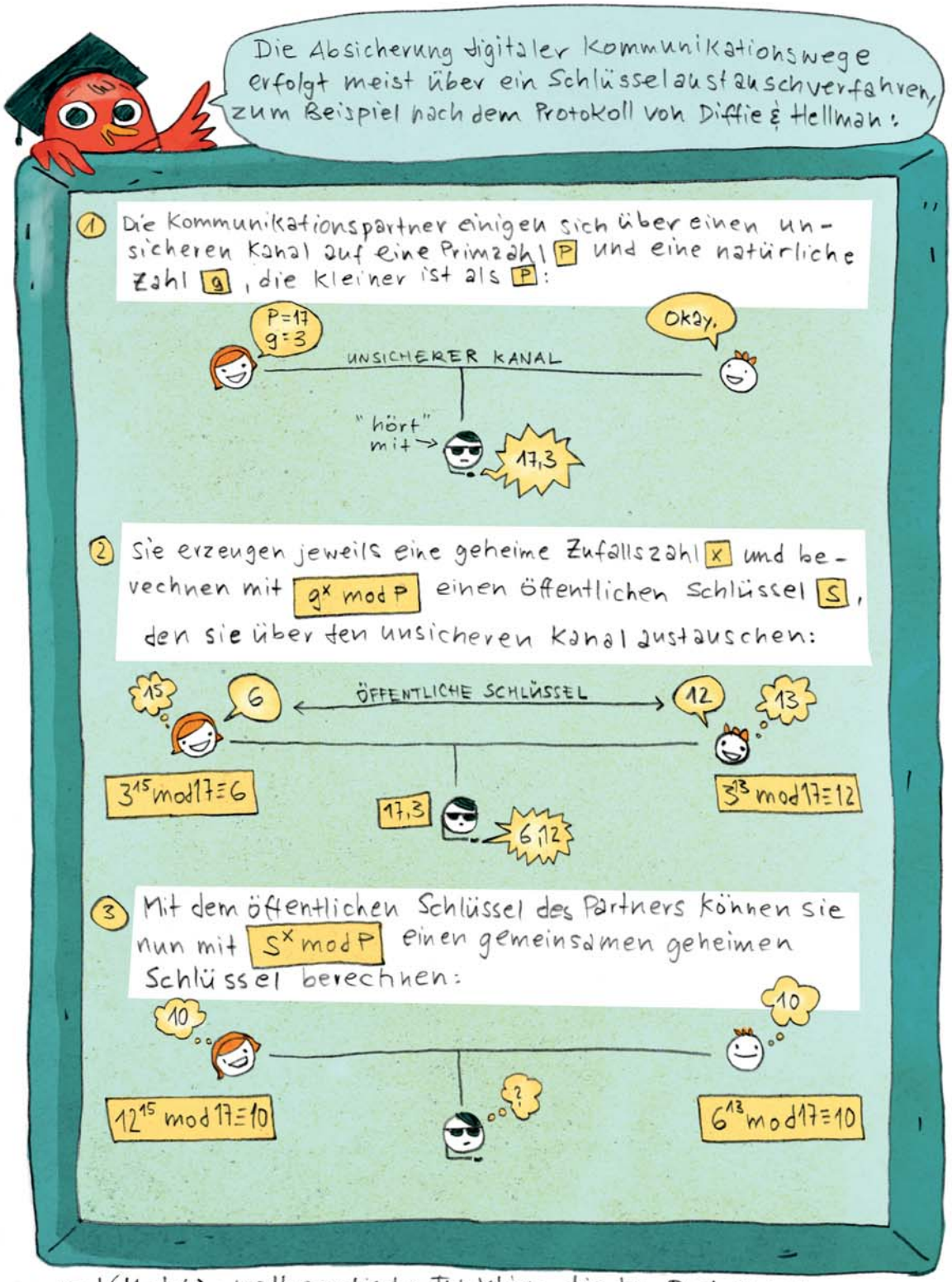
KLAR SOWEIT? No.8

Sicher ist sicher

Das Bedürfnis Nachrichten sicher auszutauschen treibt uns Menschen schon seit tausenden von Jahren um:

 DOI 10.1515/dmvm-2016-0011


Offline ist das klar geregelt. Durch das Briefgeheimnis zum Beispiel.
Späh.
Schwirr ab.
WAAAAAAH...
ARTIKEL 10, 2 GG
§ 202 StGB
Und Online?
Unverschlüsselt verschickte Daten fallen nicht in den gesetzlichen Schutzbereich...
send
verteil
HEY, WHATSAPP?
Speicher
funk
...und können an vielen Punkten mitgelesen werden.
Oho!
Sehr interessant.
Hm...
Pfft. Steht doch in den AGBs.
Wenn's dich stört, musst du halt Geräte eines anderen Herstellers nutzen. Uncool.
Well, Nationale Sicherheit - you know?
HEY!
Seufz
Okay, okay - schon kapiert. Wenn ich sicher kommunizieren will, muss ich meine Daten also verschlüsseln. Und wie funktioniert das?



mod (Modulo) = mathematische Funktion, die den Rest aus einer Division ganzer Zahlen benennt.


Man spricht von einer Einweg-Funktion: leicht zu berechnen – aber schwierig umzukehren. Klar Soweit?
Ähm
Okay. Versuchen wir es mal mit Farben anstelle der Zahlen:
1 Die Kommunikationspartner einigen sich über den unsicheren Kanal auf eine Farbe. Sie erzeugen außerdem jeweils eine geheime Farbe:
UNSICHERER KANAL
OKAY.
2 Sie mischen nun ihre geheime Farbe mit der gemeinsamen und tauschen die Mixturen aus:
ÖFFENTLICHE SCHLÜSSEL
3 Jetzt mischt jeder seine geheime Farbe in die erhaltene Mixtur. Dadurch entsteht eine gemeinsame geheime Farbe!
Orrr...
Farben mischen ist leicht. Von einer Mixtur auf die exakten Ausgangsfarben zu schließen ist nahezu unmöglich.
Clever!

Klar soweit? ist ein Wissenschaftscomic, den Veronika Mischitz alias Frau Kirschvogel monatlich für den Blog der Helmholtz-Gemeinschaft (http://tinyurl.com/o5m95qh) und das Magazin *Helmholtz Perspektiven* zeichnet. *Klar soweit?* wurde am am 19. November in Berlin mit dem Journalistenpreis der Deutschen Mathematiker-Vereinigung ausgezeichnet.
(Abdruck mit freundlicher Genehmigung der Helmholtz-Gemeinschaft)