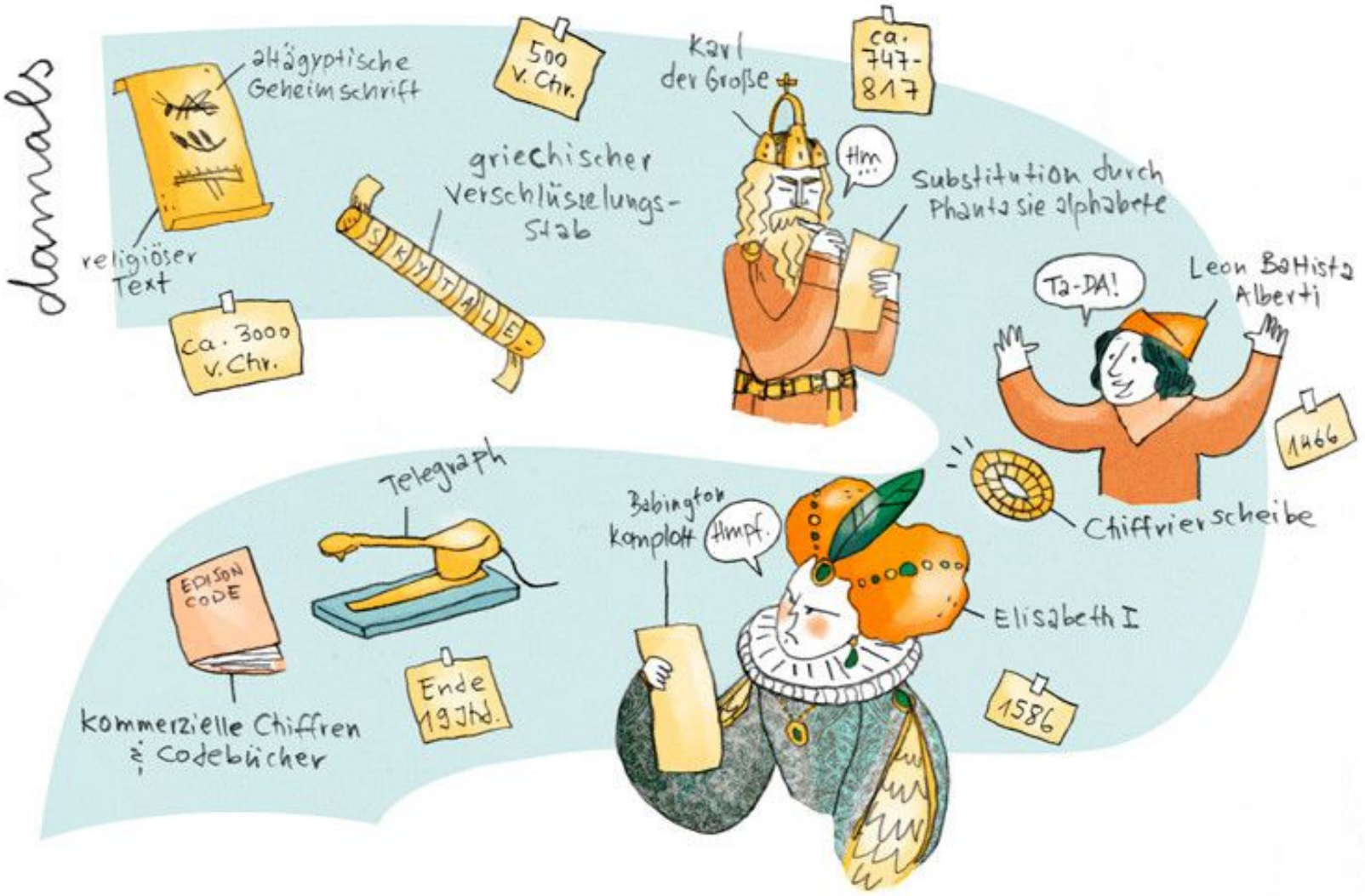
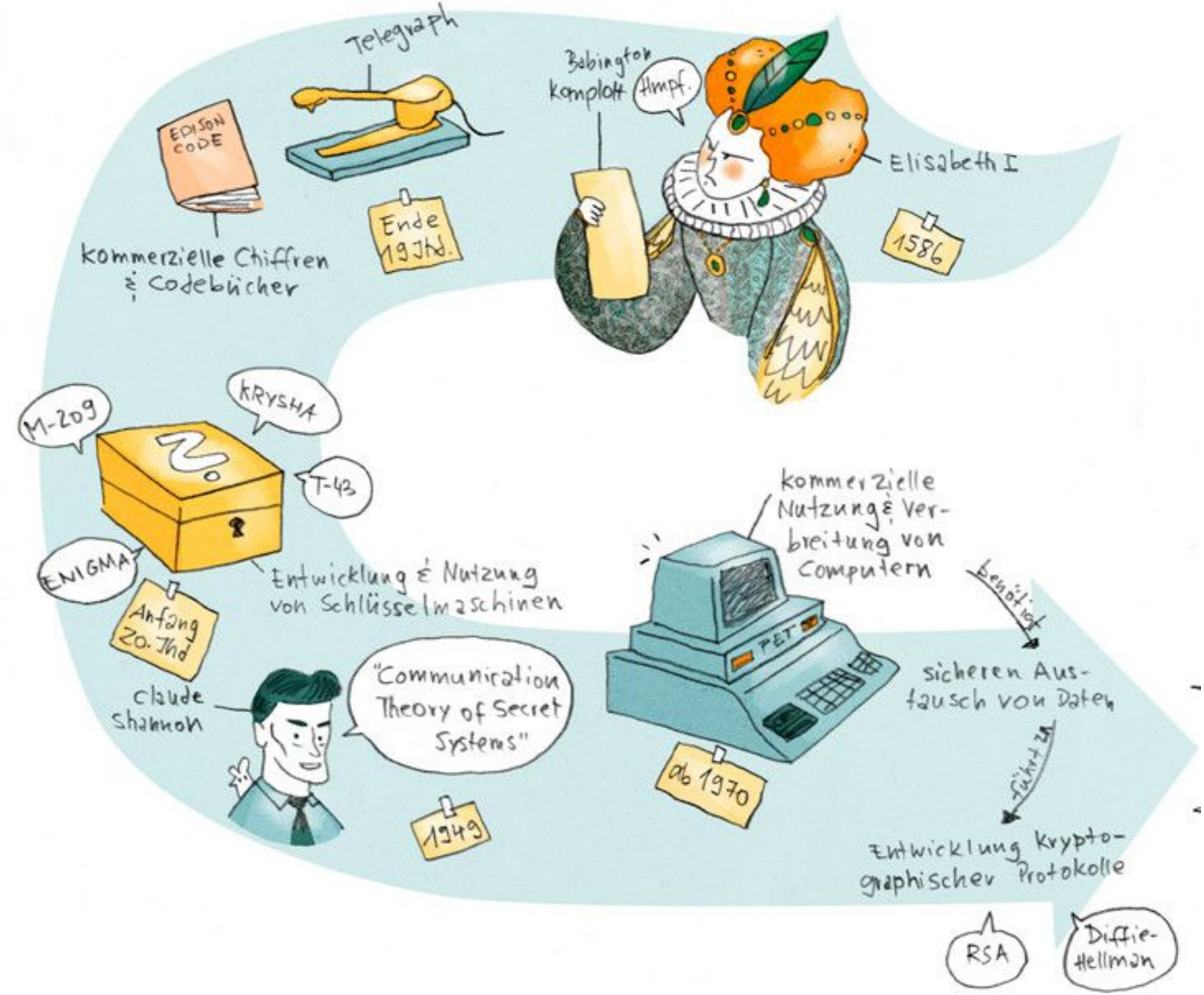
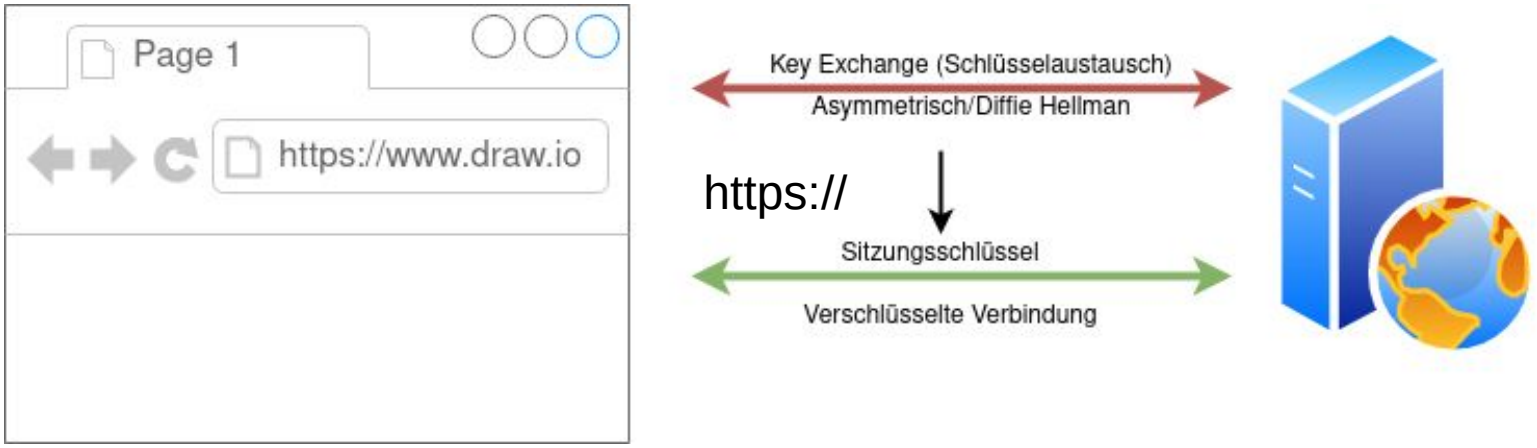
# Sicher ist sicher

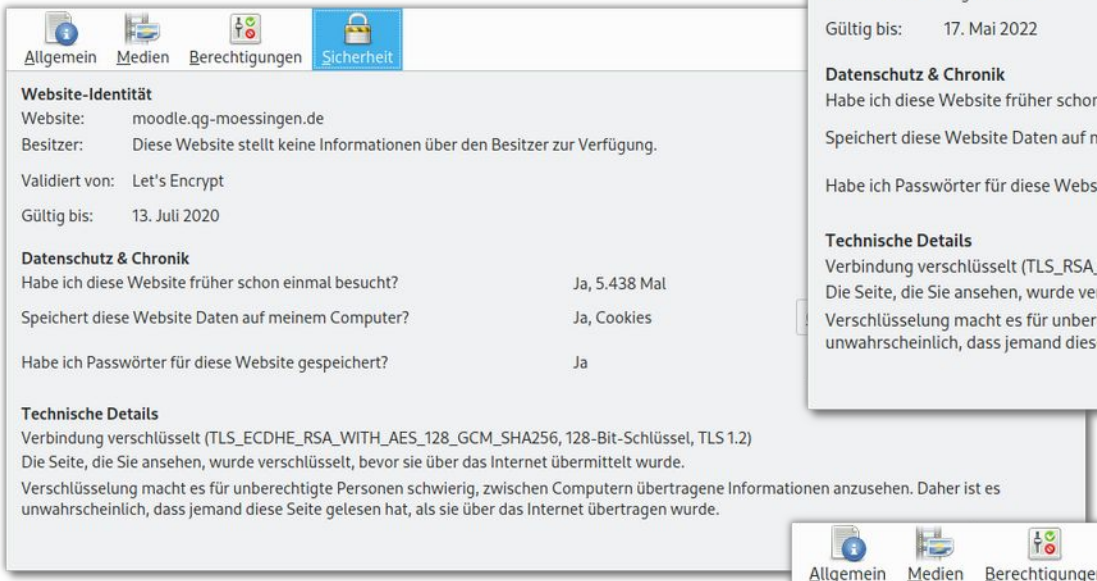
Das Bedürfnis Nachrichten sicher auszutauschen treibt uns Menschen schon seit tausenden von Jahren um:

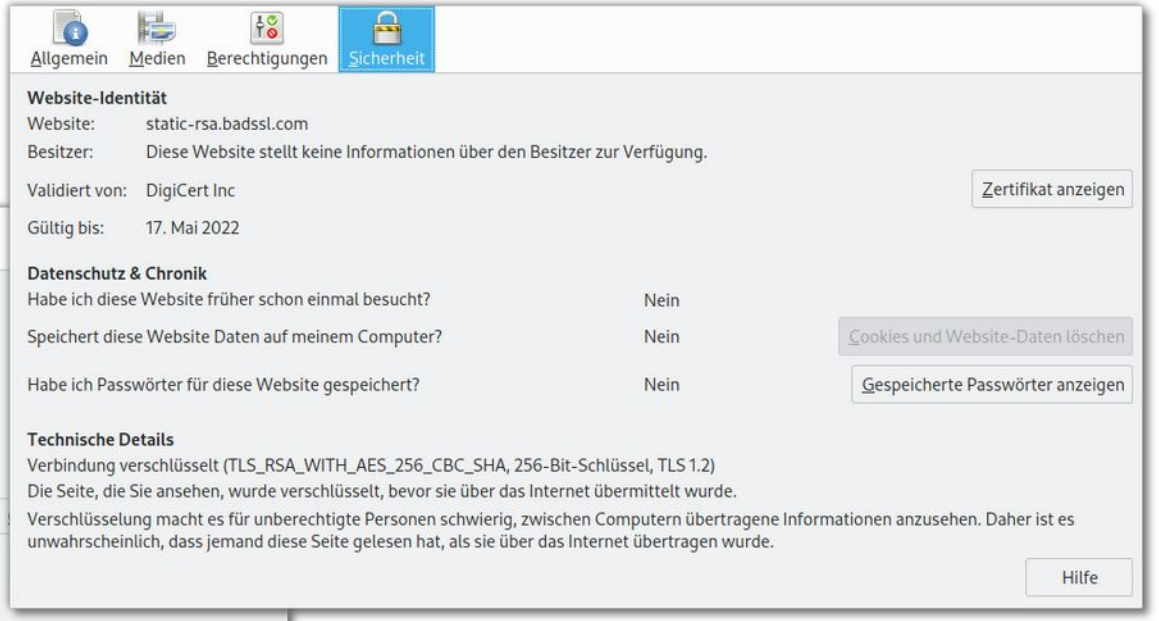


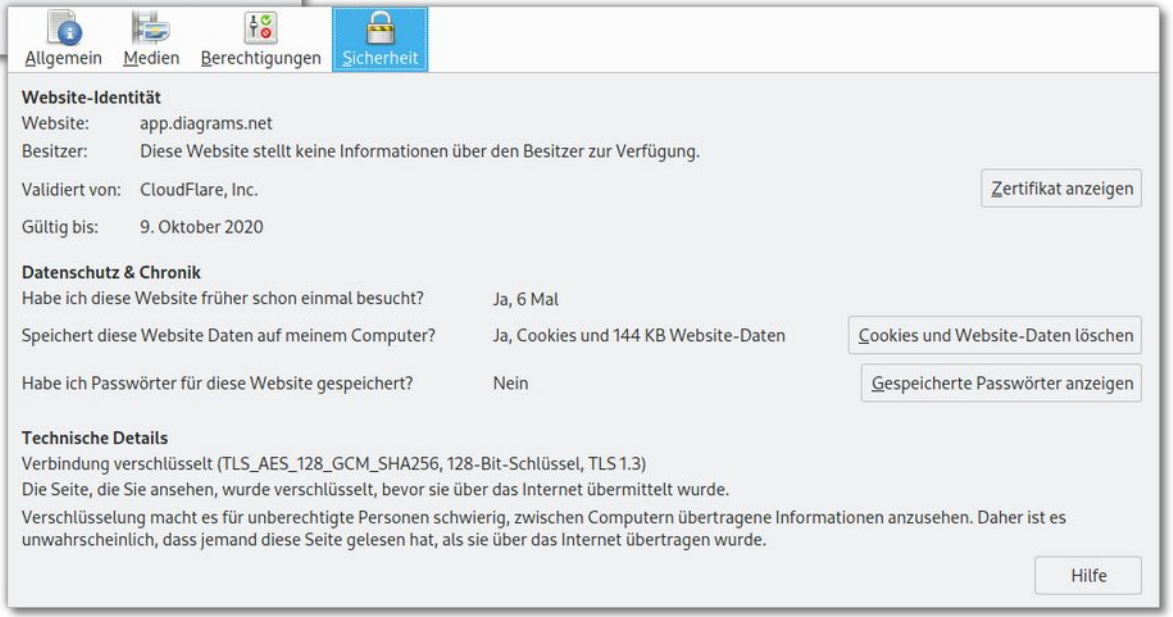


Offline ist das klar geregelt. Durch das Briefgeheimnis zum Beispiel.



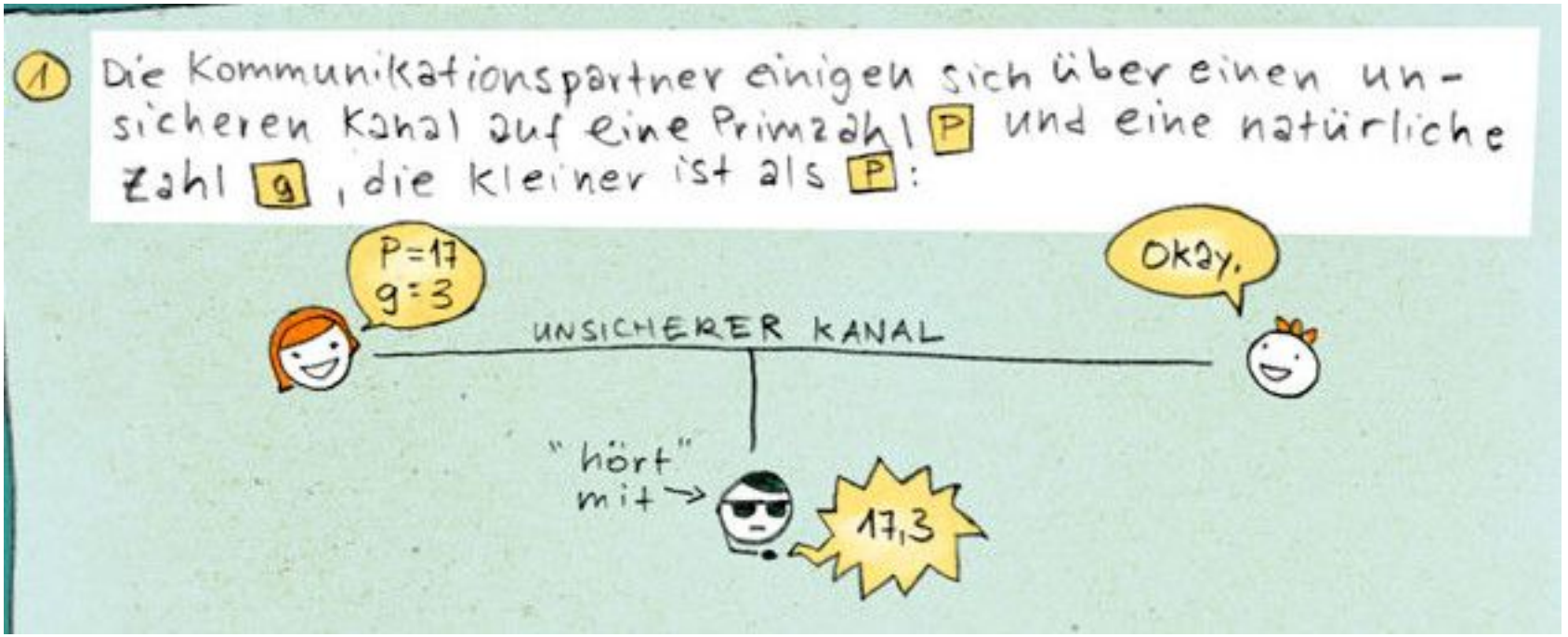

https://badssl.com/


**Diffie/Hellman ist ab TLS 1.3 Standard.** ⟶

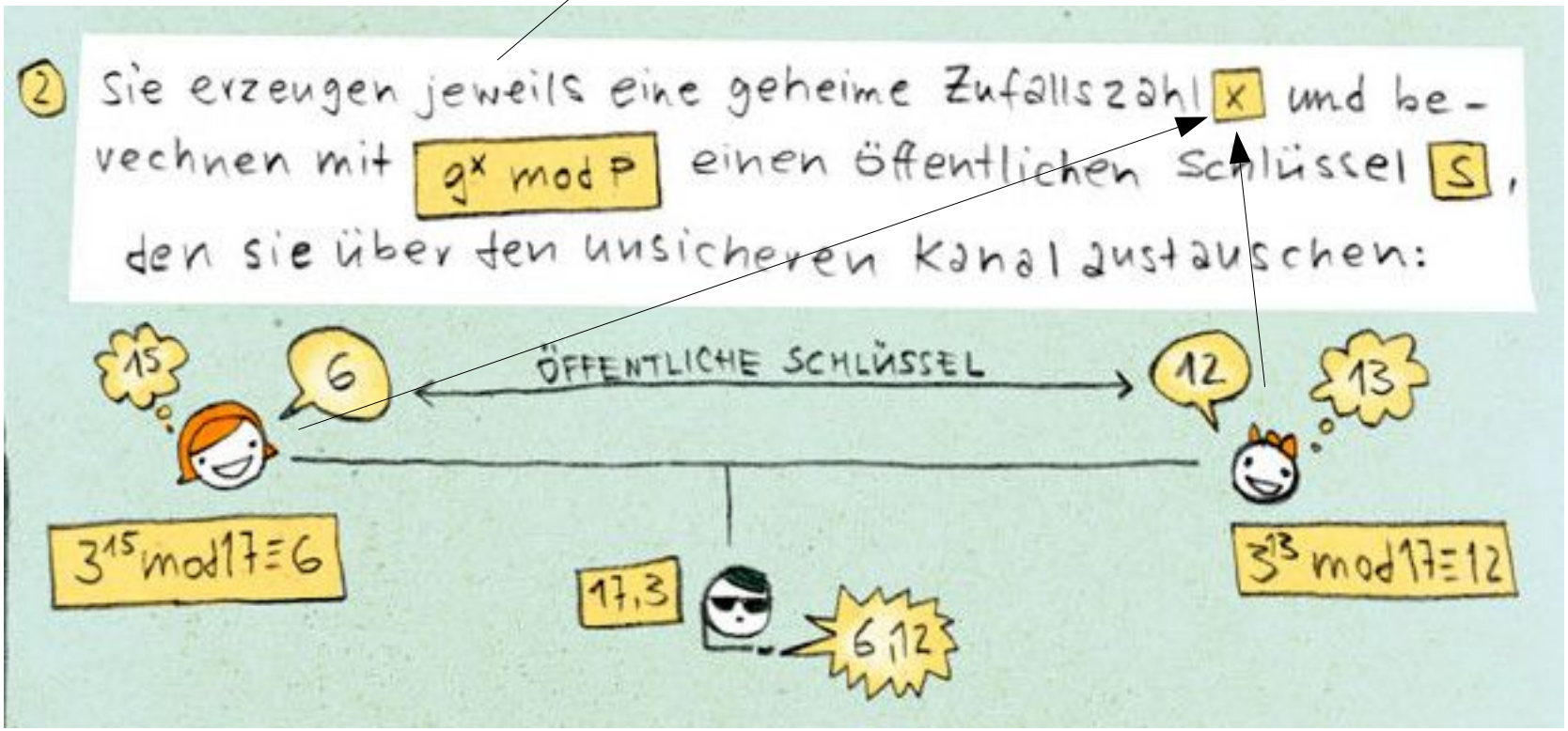
„PFS“
Perfect Forward Secrecy

*Forward* im Sinne von „in die Zukunft“

Statische RSA Verfahren zum Schlüsselaustausch **sind überholt**, da hierbei der Sitzungsschlüssel übertragen werden muss. RSA später „geknackt“ → Gesamte Sitzung entschlüsselbar!



Jeder erzeugt sein eigenes x!
(Geheimer Schlüssel!)



Die Abbildungen dieser Präsentation sind alle dem Comic

# Klar Soweit No.8 – sicher ist sicher

entnommen.

https://blogs.helmholtz.de/augenspiegel/2014/09/klar-soweit-no-8-sicher-ist-sicher/

Der Helmholtz-Wissenschaftscomics “Klar soweit?” erscheint einmal im Monat in den Helmholtz Blogs. Die Zeichnungen von Veronika Mischitz, aka Frau Kirschvogel, stellen Themen des aktuellen Diskurses um die Wissenschaft und Forschung dar – mal kommentierend, mal witzig – mal erzählend, mal erklärend.