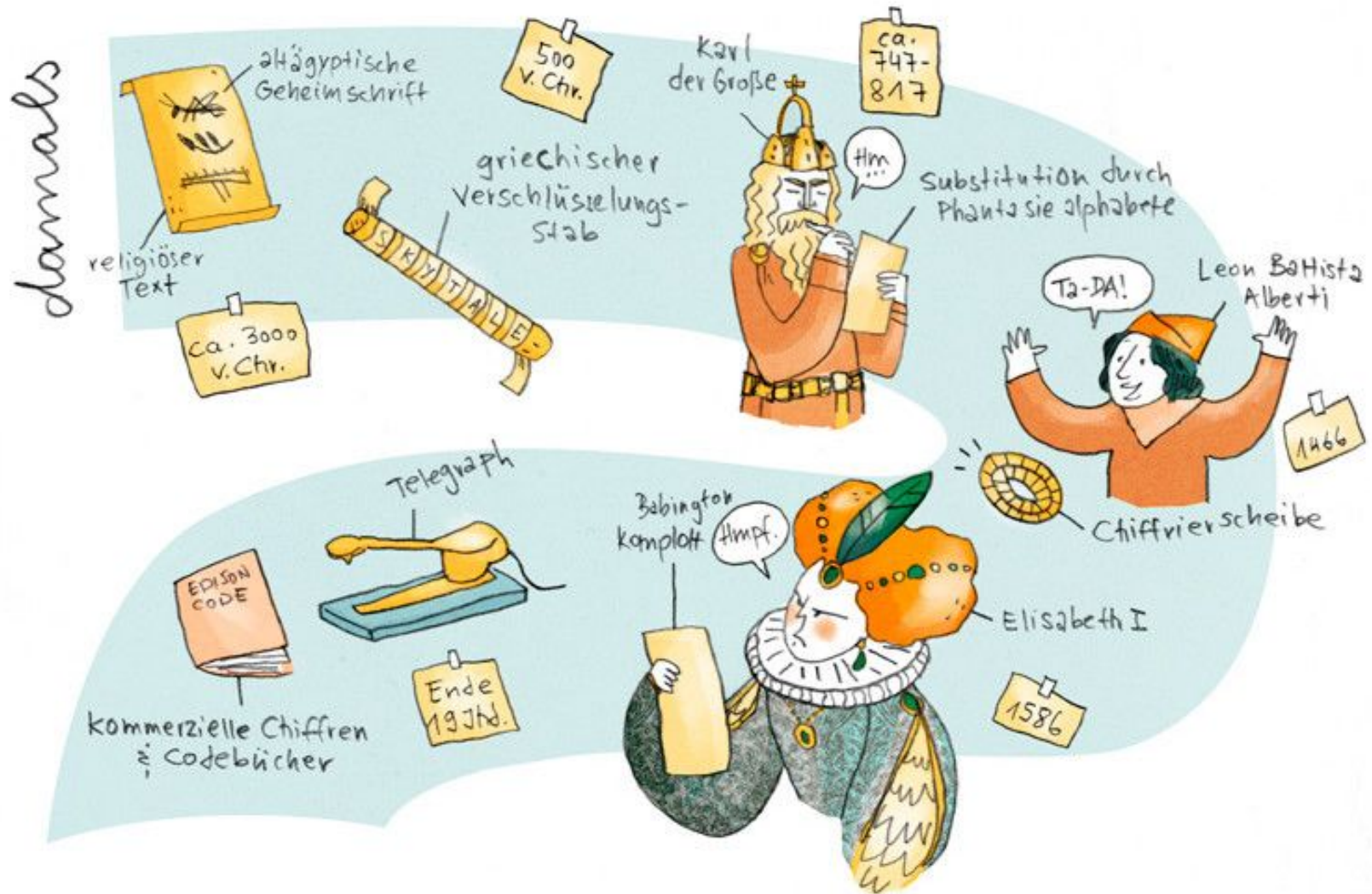


Sicher ist sicher

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





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

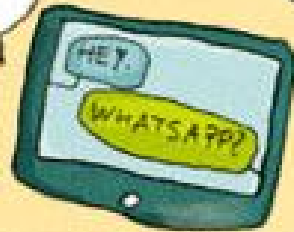


Unverschlüsselt verschickte Daten fallen nicht in den gesetzlichen Schutzbereich...

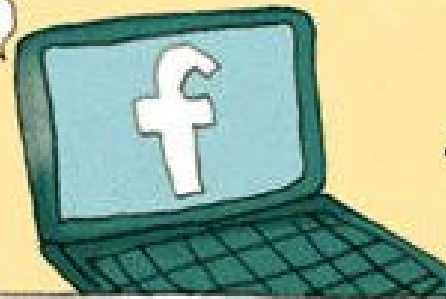
Send



verteilt



Speicher

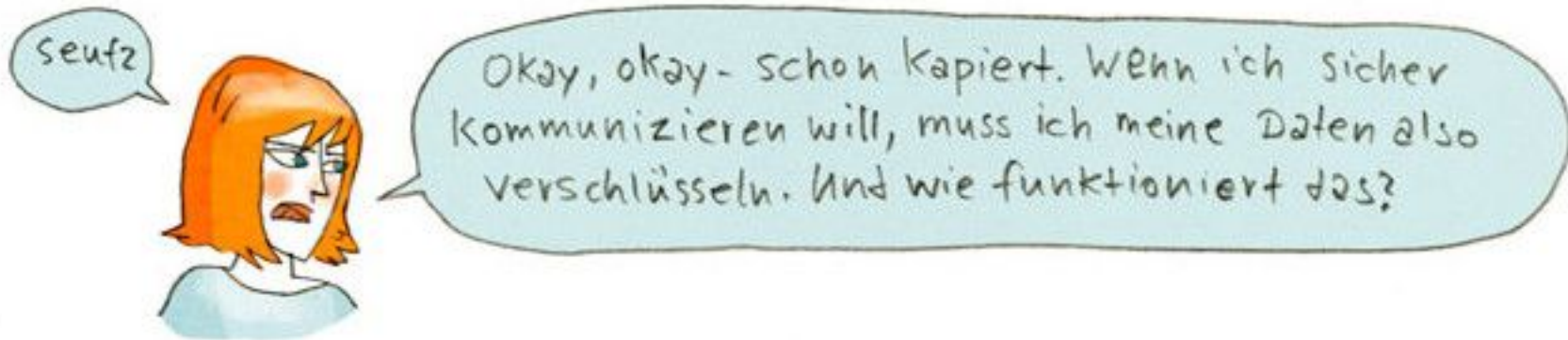


funk

...und können an vielen Punkten mitgelesen werden.

...und können an vielen Punkten mitgelesen werden.





[Allgemein](#)
[Medien](#)
[Berechtigungen](#)
[Sicherheit](#)

Website-Identität

Website: moodle.qg-moessingen.de

Besitzer: Diese Website stellt keine Informationen über den Besitzer zur Verfügung.

Validiert von: Let's Encrypt

Gültig bis: 13. Juli 2020

Datenschutz & Chronik

Habe ich diese Website früher schon einmal besucht? Ja, 5.438 Mal

Speichert diese Website Daten auf meinem Computer? Ja, Cookies

Habe ich Passwörter für diese Website gespeichert? Ja

Technische Details

Verbindung verschlüsselt (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128-Bit-Schlüssel, TLS 1.2)

Die Seite, die Sie ansehen, wurde verschlüsselt, bevor sie über das Internet übermittelt wurde.

Verschlüsselung macht es für unberechtigte Personen schwierig, zwischen Computern übertragene Informationen anzusehen. Daher ist es unwahrscheinlich, dass jemand diese Seite gelesen hat, als sie über das Internet übertragen wurde.

[Allgemein](#)
[Medien](#)
[Berechtigungen](#)
[Sicherheit](#)

Website-Identität

Website: static-rsa.badssl.com

Besitzer: Diese Website stellt keine Informationen über den Besitzer zur Verfügung.

Validiert von: DigiCert Inc

Gültig bis: 17. Mai 2022

[Zertifikat anzeigen](#)

Datenschutz & Chronik

Habe ich diese Website früher schon einmal besucht? Nein

Speichert diese Website Daten auf meinem Computer? Nein [Cookies und Website-Daten löschen](#)

Habe ich Passwörter für diese Website gespeichert? Nein [Gespeicherte Passwörter anzeigen](#)

Technische Details

Verbindung verschlüsselt (TLS_RSA_WITH_AES_256_CBC_SHA, 256-Bit-Schlüssel, TLS 1.2)

Die Seite, die Sie ansehen, wurde verschlüsselt, bevor sie über das Internet übermittelt wurde.

Verschlüsselung macht es für unberechtigte Personen schwierig, zwischen Computern übertragene Informationen anzusehen. Daher ist es unwahrscheinlich, dass jemand diese Seite gelesen hat, als sie über das Internet übertragen wurde.

[Hilfe](#)

[Allgemein](#)
[Medien](#)
[Berechtigungen](#)
[Sicherheit](#)

Website-Identität

Website: app.diagrams.net

Besitzer: Diese Website stellt keine Informationen über den Besitzer zur Verfügung.

Validiert von: CloudFlare, Inc.

Gültig bis: 9. Oktober 2020

[Zertifikat anzeigen](#)

Datenschutz & Chronik

Habe ich diese Website früher schon einmal besucht? Ja, 6 Mal

Speichert diese Website Daten auf meinem Computer? Ja, Cookies und 144 KB Website-Daten [Cookies und Website-Daten löschen](#)

Habe ich Passwörter für diese Website gespeichert? Nein [Gespeicherte Passwörter anzeigen](#)

Technische Details

Verbindung verschlüsselt (TLS_AES_128_GCM_SHA256, 128-Bit-Schlüssel, TLS 1.3)

Die Seite, die Sie ansehen, wurde verschlüsselt, bevor sie über das Internet übermittelt wurde.

Verschlüsselung macht es für unberechtigte Personen schwierig, zwischen Computern übertragene Informationen anzusehen. Daher ist es unwahrscheinlich, dass jemand diese Seite gelesen hat, als sie über das Internet übertragen wurde.

[Hilfe](#)

<https://badssl.com/>



Die Absicherung digitaler Kommunikationswege erfolgt meist über ein Schlüsselaustauschverfahren, zum Beispiel nach dem Protokoll von Diffie & Hellman:

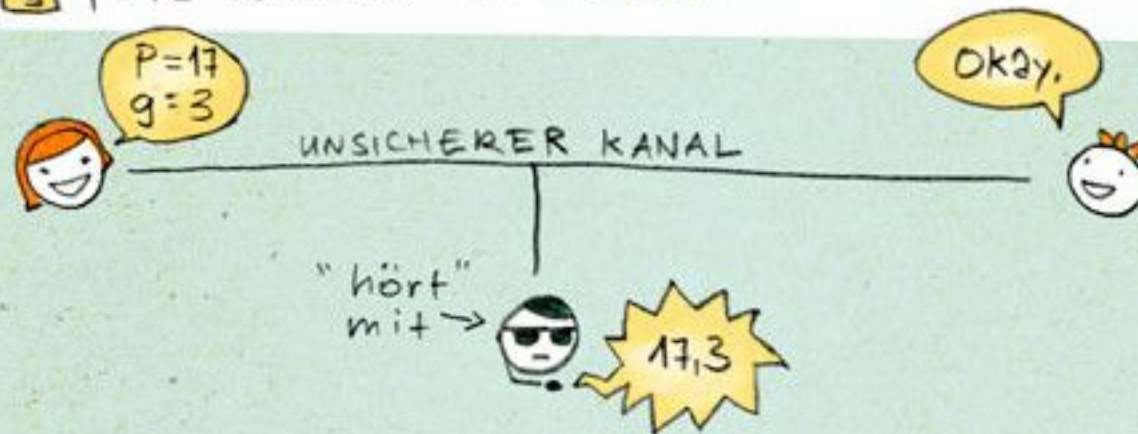
Diffie/Hellman ist ab TLS 1.3 Standard. →

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

„PFS“
Perfect Forward Secrecy

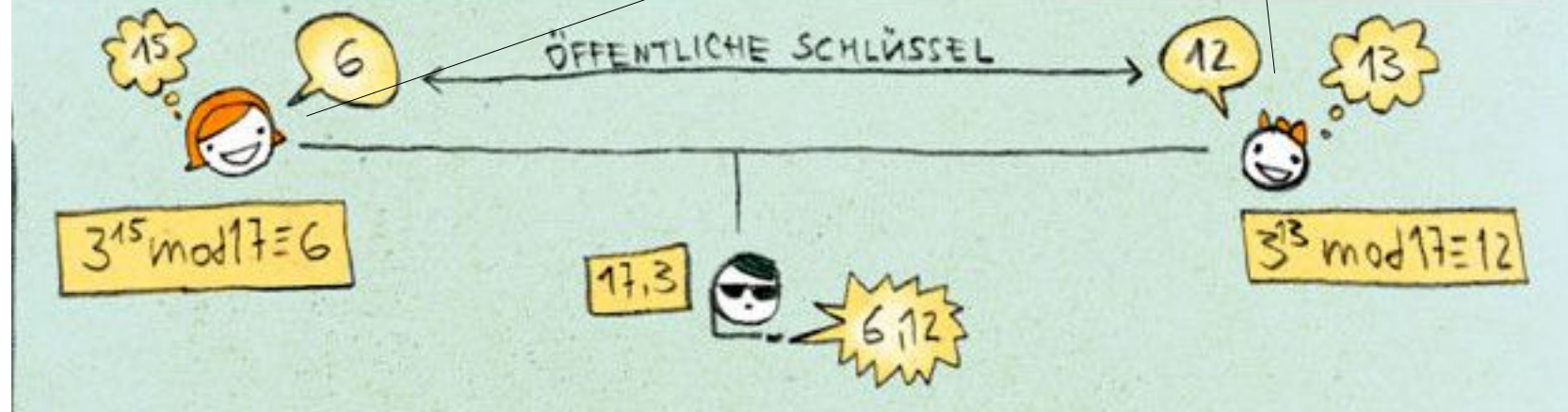
Forward im Sinne von
„in die Zukunft“

- 1 Die Kommunikationspartner einigen sich über einen unsicheren Kanal auf eine Primzahl P und eine natürliche Zahl g , die kleiner ist als P :

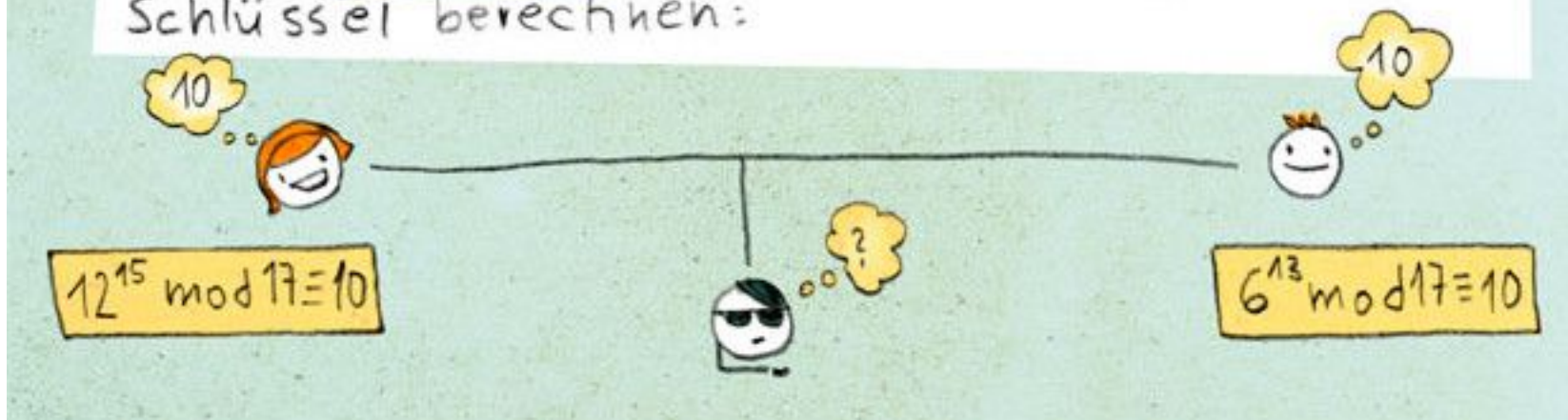


Jeder erzeugt sein eigenes x !
(Geheimer Schlüssel!)

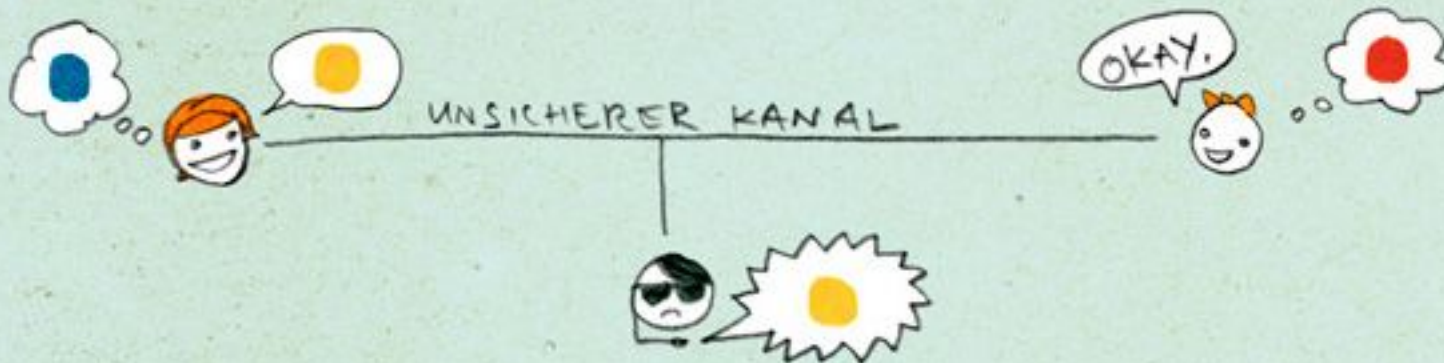
② Sie erzeugen jeweils eine geheime Zufallszahl x und berechnen mit $g^x \bmod p$ einen öffentlichen Schlüssel S , den sie über den unsicheren Kanal austauschen:



3 Mit dem öffentlichen Schlüssel des Partners können sie nun mit $S^x \bmod P$ einen gemeinsamen geheimen Schlüssel berechnen:

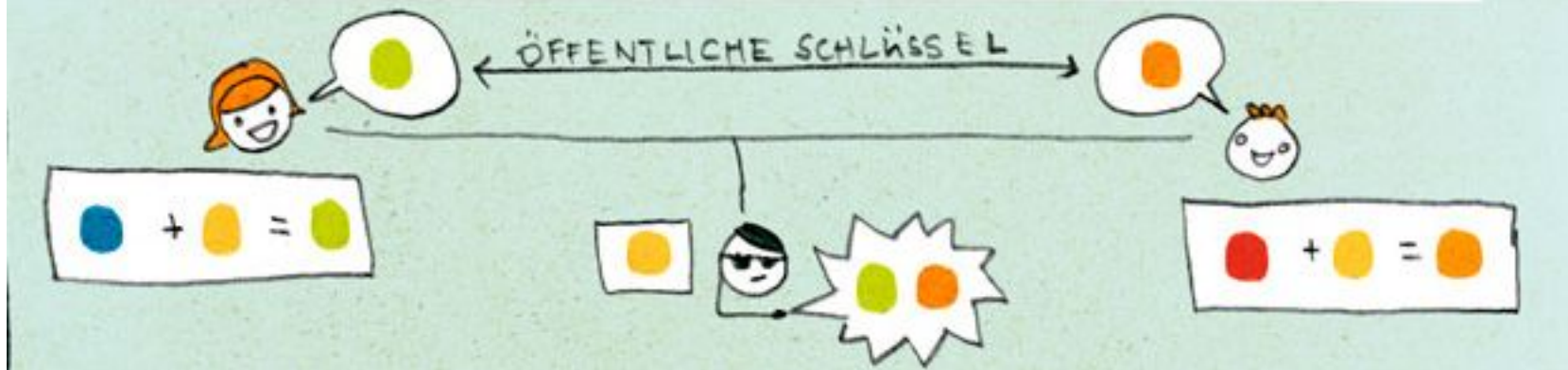


① Die Kommunikationspartner einigen sich über den unsicheren Kanal auf eine Farbe. Sie erzeugen außerdem jeweils eine geheime Farbe:



②

Sie mischen nun ihre geheime Farbe mit der gemeinsamen und tauschen die Mixturen aus:



③ Jetzt mischt jeder seine geheime Farbe in die erhaltene Mixtur. Dadurch entsteht eine gemeinsame geheime Farbe!







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.