Wissensfabrik
Mehr Wissen. Mehr Können. Mehr Zukunft.

IT2SCHOOL – GEMEINSAM IT ENTDECKEN

MODERNE KRYPTOLOGIE

VORWORT

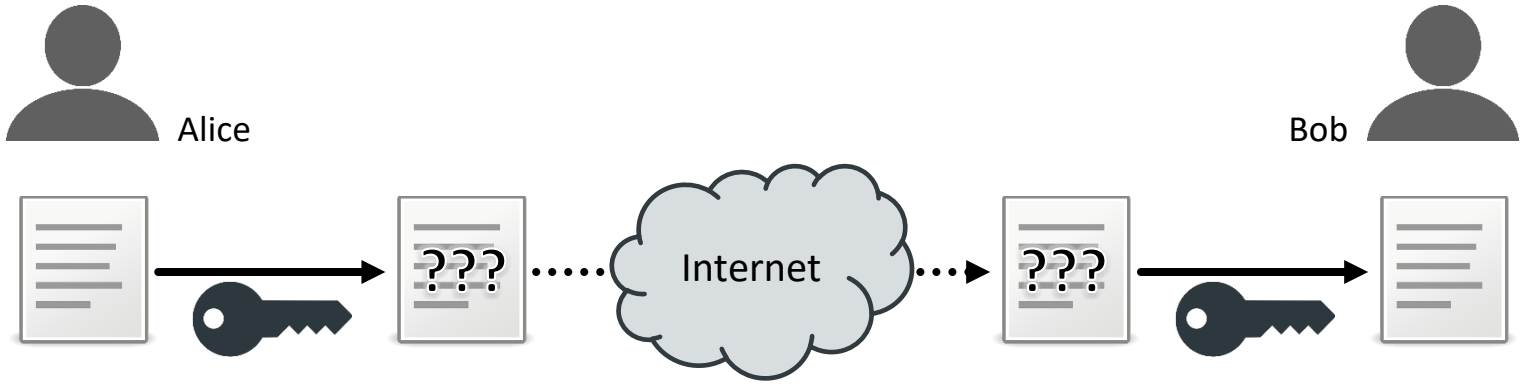
Die Mathematik ermöglicht es die uns bekannte Kryptologie zu modernisieren und komplexere Verfahren zu entwickeln!

Wie dies genauer funktioniert wird euch auf den folgenden Folien gezeigt. Wichtige Grundlagen dafür sind:

- symmetrische und asymmetrische Verschlüsselung
- Public- und Private-Keys
- RSA
- PGP

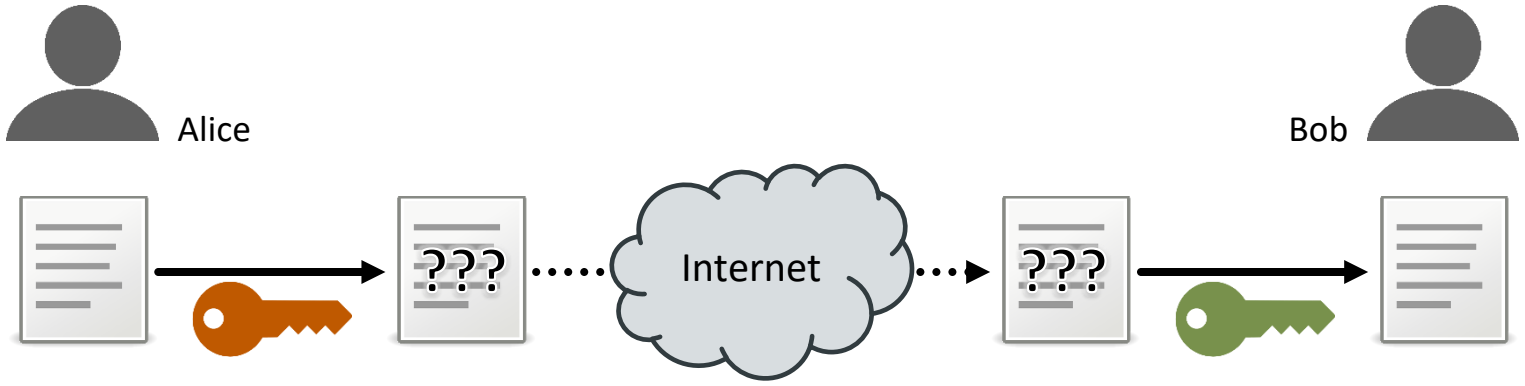
SYMMETRISCHE VERSCHLÜSSELUNG

Alice schickt Bob eine verschlüsselte Nachricht über das Internet.
Zum Ver- und Entschlüsselt wird der selbe Schlüssel bzw. das selbe Verfahren verwendet.



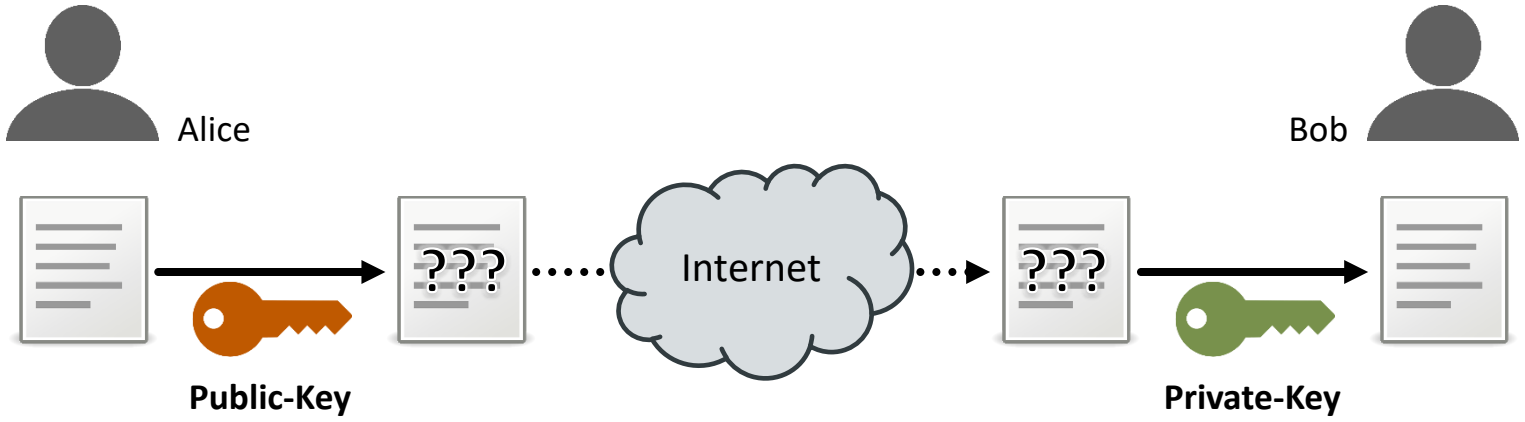
ASYMMETRISCHE VERSCHLÜSSELUNG

Alice schickt Bob eine verschlüsselte Nachricht über das Internet.
Zum Ver- und Entschlüsselt wird nicht der selbe Schlüssel bzw. das selbe Verfahren verwendet.



PUBLIC- UND PRIVAT-KEY

Bei der asymmetrischen Verschlüsselung wird ein Schlüssel bekannt gegeben, um die Nachrichten an eine Person zu verschlüsseln und einer wird geheim gehalten, um die verschlüsselten Nachrichten zu entschlüsseln.



PUBLIC- UND PRIVAT-KEY

Wichtig ist, dass der Public- und Private-Key ein Schlüsselpaar sind und immer zusammen gehören bzw. zusammen erstellt werden. Bildlich gesprochen, sind beide für das gleiche Sicherheitsschloss zuständig, nur einer dient zum zuschließen und der andere zum öffnen.

UND WAS HAT DAS MIT DEN BISHERIGEN VERFAHREN ZU TUN?

- Bisher hatten wir im Unterricht nur symmetrische Verfahren, meist auch nur mit Substitution
  - Zum Ver- und Entschlüsseln (bei Caesar, Vigenére etc.) wurde immer das gleiche Schlüsselwort oder Verfahren verwendet
  - Buchstaben werden nur durch andere Buchstaben ausgetauscht
- Bisher noch keine besondere Mathematik oder Logik in den Verfahren
  - Erlaubt uns Buchstaben zu codieren und dann zu verschlüsseln
  - Erlaubt uns Schlüsselpaare zu erzeugen
  - Ein Beispiel dafür ist RSA

RSA

- Benannt ist das Verfahren nach seinen drei Entwicklern:
  - Rivest
  - Shamir
  - Adleman
- Es gibt mehrere Phasen des Verfahrens:
  - Schlüsselpaar erzeugen
  - Nachricht verschlüsseln
  - Nachricht entschlüsseln

RSA – SCHLÜSSELPAAR ERZEUGEN

- Wir brauchen zwei sehr große Primzahlen p und q
- Es wird das Produkt $pq = F$ berechnet
  - Wichtig ist, dass man anhand des Produkt nicht so leicht erkennen kann, welche Primzahlen verwendet wurden! (Wichtig für die Sicherheit)
- Mit mathematischen Hilfsmitteln werden nun die Zahlen e und d ermittelt
  - (F, e) bilden den Public-Key
  - (F, d)bilden den Private-Key

RSA – NACHRICHT VERSCHLÜSSELN

- Die Nachricht wird so codiert, dass sie aus Zahlen besteht
  - Die Codierung kann z. B. mit dem ASCII Code erfolgen
  - Wir bezeichnen die codierte Nachricht als N
- Zum Verschlüsseln brauchen wir den Public-Key
  - Die Verschlüsselte Nachricht M errechnet sich durch

$$M \equiv N^e \pmod{F}$$

RSA – NACHRICHT ENTSCHLÜSSELN

- Zum Entschlüsseln brauchen wir den Private-Key und die verschlüsselte Nachricht M
  - Die codierte Nachricht N errechnet sich durch

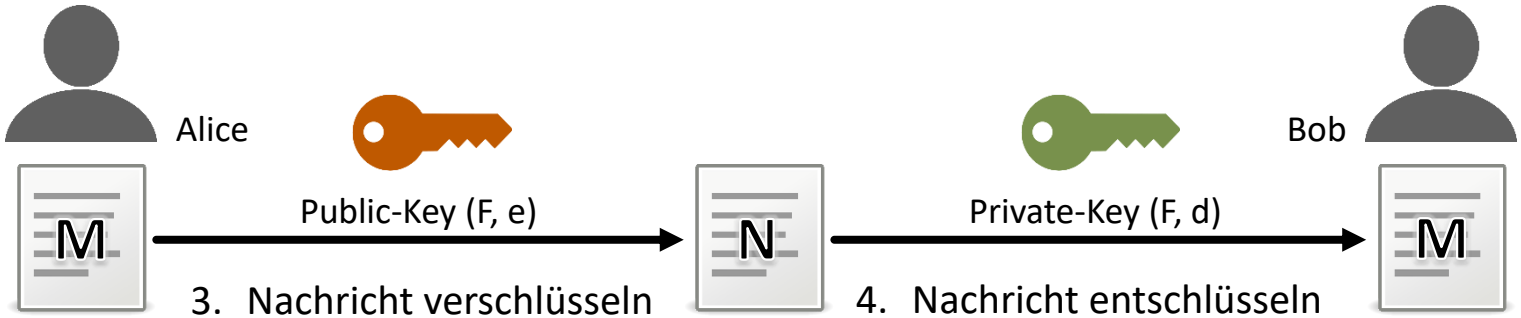
$$N \equiv M^d \pmod{F}$$

- Die Nachricht N kann nun so codiert werden, dass die ursprüngliche Nachricht lesbar ist
  - Wie die Nachricht codiert wurde, kann sowohl Sender als Empfänger bekannt sein

RSA – SCHAUBILD

1. Große Primzahlen p und q wählen
2. Berechnung von F, e und d

Wichtig ist hier natürlich, dass Bob seinen Public-Key für Alice bereitstellt, damit sie für ihm auch eine Nachricht verschlüsseln kann.



3. Nachricht verschlüsseln
$M \equiv N^e \pmod{F}$

4. Nachricht entschlüsseln
$\mathrm{N} \equiv M^{\mathrm{d}} \pmod{F}$

PGP

- PGP steht für Pretty Good Privacy
- Programm zum Verschlüsseln und Unterschreiben von Daten
- Verwendet hybrides Verfahren aus symmetrischer und asymmetrischer Verschlüsselung
- Verwendete in der ersten Version RSA zum Verschlüsseln (später Elgamal)
- Häufig verwendet zur Verschlüsselung von E-Mails

PGP – SCHAUBILD