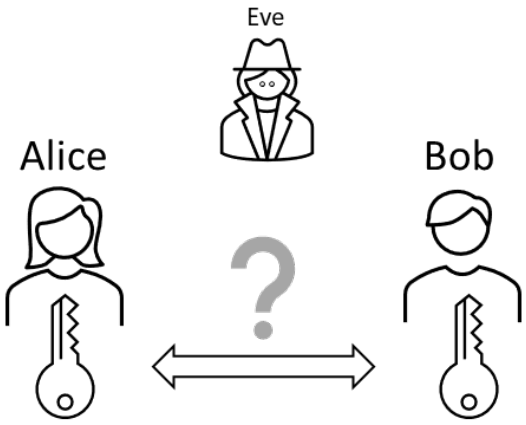
Der Diffie-Hellman-Schlüsselaustausch

Die Schülerinnen und Schüler sollen dieses Skript selbstständig durcharbeiten. Die Aufgaben werden anschliessend gemeinsam besprochen.

Voraussetzungen

- Die SuS kennen die Prinzipien der symmetrischen und der asymmetrischen Verschlüsselung.
- Die SuS kennen die Rechenoperation Modulo.
- Die SuS kennen die RGB-Farbcodierung.

Einstieg



In den letzten Lektionen haben wir das symmetrische Verschlüsselungsverfahren kennengelernt und haben festgestellt, dass die Ver- und Entschlüsselung sehr effizient abläuft. Die grosse Schwachstelle der symmetrischen Verschlüsselung ist jedoch der Schlüsselaustausch. Im Kapitel zum asymmetrischen Verschlüsselungsverfahren haben wir gelernt, dass der problematische Schlüsselaustausch umgangen werden kann, indem mit einem öffentlichen Schlüssel eine Nachricht in einen «Briefkasten» geworfen wird. Nur der Eigentümer des privaten Schlüssels hat somit die Möglichkeit, diese Nachricht zu lesen. Der Nachteil dieses Verfahrens ist jedoch, dass die asymmetrische Verschlüsselung viel langsamer ist als die symmetrische. Ist es möglich diese beiden Verfahren zu kombinieren, bei beiden deren Vorteile zu nutzen und gleichzeitig die Nachteile zu eliminieren? Das werden wir in dieser Lektion herausfinden.

Lernziele

- Du kannst schematisch zeigen, wie der Schlüsselaustausch nach dem Diffie-Hellman-Protokoll abläuft.
- Du weisst, welche Rechnungen beim Diffie-Hellman-Protokoll angewendet werden und bist vertraut mit den Voraussetzungen, die einen hohen Sicherheitsgrad garantieren.
- Du kennst die Vor- und Nachteile des Diffie-Hellman-Protokolls.
- Du kannst die Begriffe Kommutativität und Irreversibilität in Bezug auf das Diffie-Hellman-Protokoll erklären.

Aufgabenbeispiel: Der Farbscanner

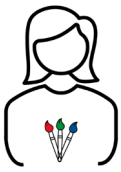
Du bist Hüterin oder Hüter über eine Geheimkammer, deren Zutritt von einem einzigartigen Farbscanner kontrolliert wird. Der Zutritt wird freigegeben, wenn dieser die exakt richtige Farbe scannt und daraus die einzelnen RGB-Farbwerte herauslesen kann.

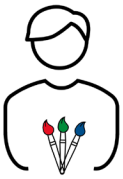
Auftrag 1
Als Erstes willst du überprüfen, ob dem Farbscanner der Geheimkammer vertraut werden kann, für den Fall, dass jemandem ein Blick auf die Geheimfarbe gelingt. Stelle dir dafür eine RGB-Farbe[1] zusammen, die den Schlüssel zur Geheimkammer darstellt. Nun schickst du einen Screenshot der Farbe an deinen Banknachbarn, der versuchen wird, genau diese Farbe zusammenzustellen. Können die Farb-Werte innerhalb einer Minute gefunden werden?

Du hast bereits zwei wichtige Eigenschaften des Farbmischens kennengelernt, die ganz bewusst für die Verschlüsselung und den Schlüsselaustausch genutzt werden können. Die **Kommutativität** besagt, dass die neu gemischte Farbe unabhängig von der Mischreihenfolge der Ursprungsfarben ist. Dies sehen wir beim RGB-Farbmischer daran, dass die Rot-, Grün- und Blau-Werte unabhängig voneinander gewählt bzw. nachträglich verändert werden können. Das gleiche Prinzip gilt auch, wenn z.B. fünf unterschiedliche Lebensmittelfarben gemischt werden. Die **Irreversibilität** macht es äusserst aufwändig, die Ursprungsfarben herauszufinden. Dies ist nur durch Ausprobieren möglich und wird mit der zunehmenden Anzahl von Unbekannten immer schwieriger.

Auftrag 2
Hast du noch andere Ideen für irreversible Mischungen?

Auftrag 3
Du willst nun den Zutritt zur Geheimkammer mit einer Freundin teilen, ohne ihr die einzelnen Farbwerte mitzuteilen, da diese abgefangen werden könnten. Hast du eine Idee, wie das möglich ist?
Skizziert einen denkbaren Austausch von Informationen!
Tipps: Ihr entwerft zum Schluss zusammen eine neue gemeinsame geheime Farbe, indem ihr zuvor das asymmetrische Verschlüsselungsprinzip anwendet. (Stichwort: Kommutativität)

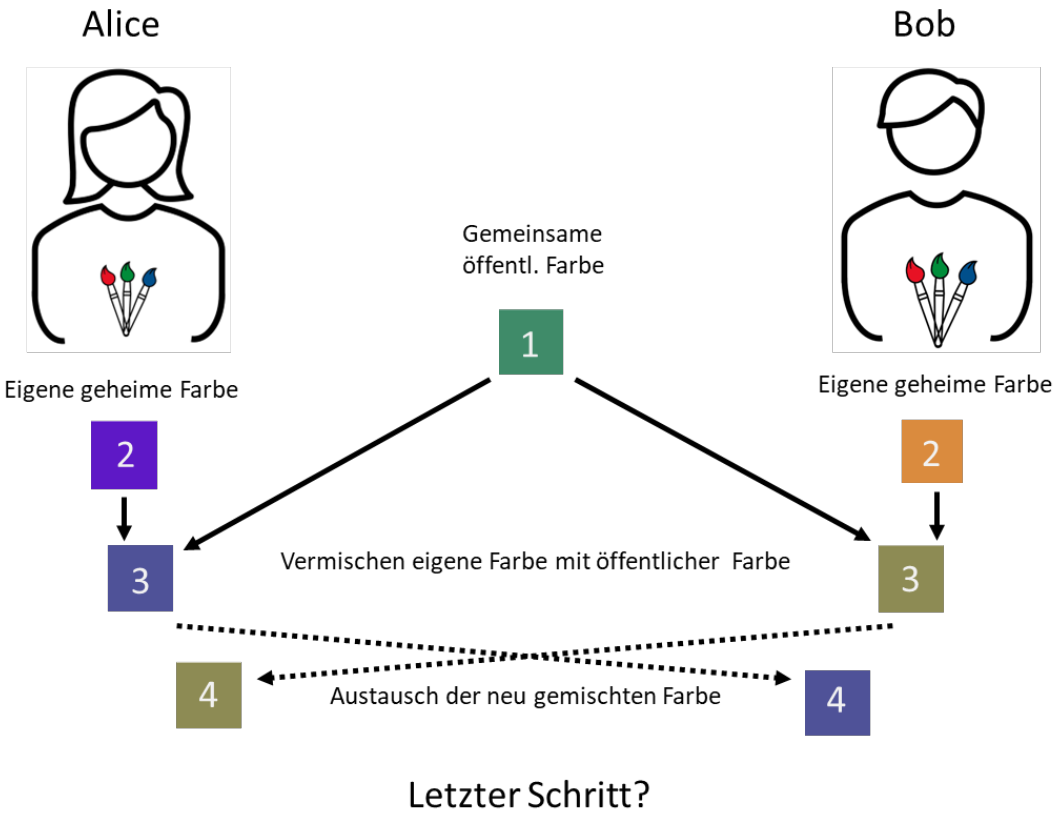




[1] https://www.w3schools.com/colors/colors_rgb.asp

Das Diffie-Hellman-Protokoll

Wenn ihr in Auftrag 3 das richtige Kommunikationsprotokoll bereits herausgefunden habt, ist das fantastisch!
Whitfield Diffie und Martin Hellman haben das Problem der sicheren Schlüsselvereinbarung im Jahr 1976 gelöst, indem sie die Kommunikation zwischen zwei Personen festgelegt haben.
Das folgende Schaubild erklärt den Ablauf anhand unseres Farben-Beispiels einschliesslich des vorletzten Schrittes:



1. Schritt: Alice und Bob einigen sich auf eine gemeinsame öffentliche Farbe.
2. Schritt: Alice und Bob bestimmen eine eigene geheime Farbe.
3. Schritt: Vermischen der eigenen mit der öffentlichen Farbe.
4. Schritt: Die gemischten Farben schicken sie sich gegenseitig zu.
5. Schritt:

Auftrag 4
Finde den letzten Schritt heraus, damit das Ziel von Alice und Bob erfüllt ist. Was ist die Bedeutung des Endprodukts und wie können Alice und Bob dieses Produkt nutzen?

_____

_____

_____

Auftrag 5

Probiert das Diffie-Hellman-Protokoll zu zweit aus. Um die Farben zu mischen, könnt ihr den Code aus dem Anhang kopieren und in eure Programmierumgebung kopieren. Erhaltet ihr denselben geheimen Schlüssel?

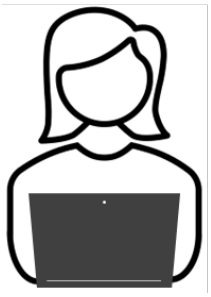
_____

Bei der Anwendung dieses Protokolls wird in der Realität nicht mit Farben gearbeitet, sondern mit Zahlen. Die Prinzipien der Kommutativität und Irreversibilität bleiben zentral und beruhen auf dem modularen Potenzieren. Die Rechenoperation Modulo habt ihr bereits kennengelernt.

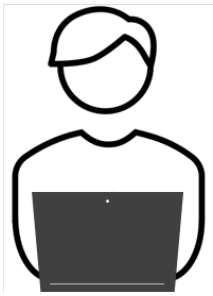
Auftrag 6

Versucht herauszufinden, wie das Farbbeispiel auf das mathematische Verfahren angewendet wird.
Als Hilfe wird die Rolle von Alice vorgegeben:
Alice und Bob einigen sich auf zwei öffentliche natürliche Zahlen: $p = 13$ und $g = 9$.
Alice wählt eine zufällige geheime Zahl $a = 7$.
Alice rechnet: $x = g^a \bmod p$
Alice schickt x an Bob.
Alice erhält eine Zahl y von Bob und rechnet: $z = y^a \bmod p$
Ergänzt die Vorgehensweise von Bob und skizziert den Ablauf. (Falls Bob Zahlen wählt, dürft ihr diese selbst bestimmen.)

Alice



Bob



Auftrag 7

Führt diesen Ablauf mit anderen Zahlen zu zweit durch, wobei folgende Voraussetzungen für die zwei natürlichen Zahlen *p* und *g* gelten:

- p ist eine Primzahl.
- g ist kleiner als p.

Die Kommunikation soll dafür nur über Microsoft Teams geschehen. Zu Übungszwecken sollt ihr davon ausgehen, dass es ein öffentlicher Chat ist.

Auftrag 8

Berechne den gemeinsamen Schlüssel nach dem Diffie-Hellman-Protokoll für die folgenden Parameter: $p = 19$, $g = 3$, $a = 7$, $b = 5$

S_{AB}: _____

Auftrag 9

Die Sicherheit in dem Beispiel mit den Farbwerten basiert darauf, dass die Zusammensetzung einer Mischfarbe schwer herauszufinden ist. Was macht das Knacken des mathematischen Verfahrens irreversibel?

Hinweis: Was weiss eine Spionin namens Eve, die den öffentlichen Schlüssel und die ausgetauschten Nachrichten sieht? Was kann sie damit herausfinden?

_____

_____

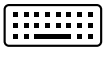
_____

Auftrag 10

Der Schlüsselaustausch nach dem Diffie-Hellman-Protokoll gilt gegenüber einem passiven Kryptoanalytiker als sicher. Mit passiv ist dabei gemeint, dass nur beobachtet wird bzw. Nachrichten abgefangen und gelesen werden. Hast du eine Idee, wie Eve das Protokoll austricksen kann, indem sie zu einer «aktiven Gegnerin» wird?

_____

_____



Auftrag 11 (optional)

Schreibt einen Algorithmus, der euch beim Diffie-Hellman-Protokoll mit Zahlen assistiert. Beachtet dabei die Voraussetzungen für *p* und *g* und stellt sicher, dass sie richtig gewählt werden müssen.

Zusammenfassung / Fazit

Wir haben gelernt, dass die Vorteile der asymmetrischen Verschlüsselung genutzt werden können, um einen symmetrischen Schlüssel auszutauschen. Somit fällt die ineffiziente Verschlüsselung des asymmetrischen Verfahrens nicht ins Gewicht und das Risiko beim Schlüsselaustausch ist gering. Dabei wird zuerst gemeinsam ein öffentlicher Schlüssel gewählt und von beiden Parteien mit dem eigenen privaten Schlüssel verarbeitet. Das Zwischenprodukt wird ausgetauscht und das Erhaltene mit dem eigenen Schlüssel zu einem gemeinsamen geheimen Schlüssel ergänzt. Die Sicherheit des Diffie-Hellman-Protokolls beruht darauf, dass wenn die Zahlen p, a und b sehr gross gewählt werden, eine Kryptoanalyse zu aufwändig ist, um in einer realistischen Zeit auf das richtige Ergebnis zu kommen. Die grösste Schwäche des Protokolls ist, dass keine Identifizierung stattfindet. Dieses Problem kann man jedoch mit digitalen Unterschriften beheben.

Bemerkung zu diesen Unterlagen

Dieses Skript ist für ca. drei Lektionen vorgesehen. Wenn das Thema noch eingehender behandelt werden soll, kann genauer auf die mathematischen Verfahren eingegangen und z.B. die zyklische Gruppe besprochen werden. (Siehe Kapitel 7.4 im Buch «Einführung in die Kryptologie» von Karin Freiermuth, Juraj Hromkovič, Lucia Keller und Björn Steffen.)
Ebenfalls könnte das Thema der digitalen Unterschriften detailliert behandelt werden.

Anhang: Farbmischer

Führe das Skript aus und folge den Anweisungen in der Kommandozeile.

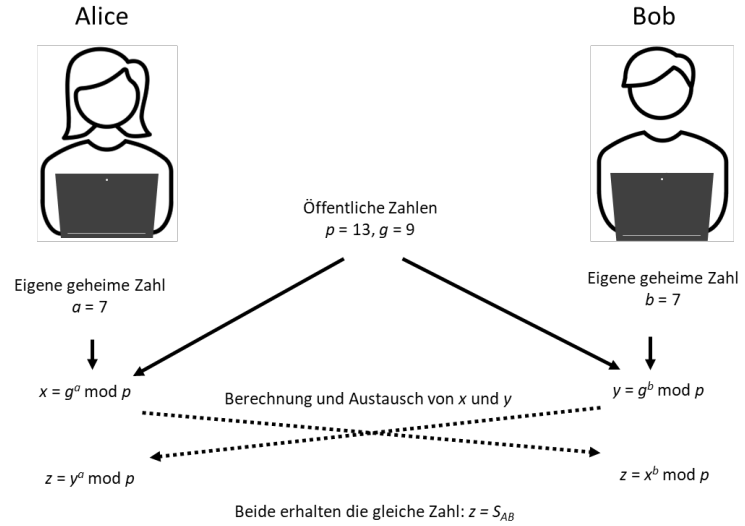
```
class Color:

    def __init__(self, red, green, blue):
        self.red = red
        self.green = green
        self.blue = blue

def farbanteil():
    print("Füge Werte zwischen 0 und 255 für rot, grün und blau ein!")
    r1 = float(input("Rot-Anteil:"))
    g1 = float(input("Grün-Anteil:"))
    b1 = float(input("Blau-Anteil: "))

    return Color(r1,g1,b1)

print("Bestimmung der gemeinsamen öffentlichen Farbe:")

pubCo = farbanteil()  # public Color

print("Eure gemeinsamen öffentlichen Farbwerte lauten:", pubCo.red,
pubCo.green, pubCo.blue)
print()

print("Bestimmung der eigenen geheimen Farbe:")

privCo = farbanteil()  # private Color A

print("Deine persönlichen geheimen Farbwerte lauten: ", privCo.red,
privCo.green, privCo.blue)
print()

mix1 = ((pubCo.red+privCo.red)//2, (pubCo.green+privCo.green)//2,
(pubCo.blue+privCo.blue)//2)
print("Sende diese gemischten Farbwerte an den Empfänger: ", mix1)
print()
print("Welche Farbwerte hast du zugeschickt bekommen?")

bCo = farbanteil()  # private Color B

privKey = Color((privCo.red +2*bCo.red)//3, (privCo.green +2*bCo.green)//3,
(privCo.blue +2*bCo.blue)//3)

print("Eure gemeinsame Geheimfarbe lautet:", privKey.red, privKey.blue,
privKey.green)
```

Lösungen

Auftrag 2
Irreversible Mischungen liegen zum Beispiel vor in Fruchtsaftgetränken und auch in vielen weiteren farbigen Flüssigkeiten.

Auftrag 3
Siehe Auftrag 4!

Auftrag 4
Schritt 5: Die vom Kommunikationspartner erhaltene Farbe mischen beide mit ihrer eigenen geheimen Farbe und bekommen damit beide genau die gleiche Farbe. Diese besteht aus der öffentlichen Farbe und den beiden privaten Farben. Die finale Farbe stellt ab diesem Zeitpunkt den gemeinsamen geheimen Schlüssel (S_{AB}) dar, den sie für symmetrische Kryptosysteme verwenden können.

Auftrag 6


Auftrag 8
$S_{AB} = 13$

Auftrag 9
Wenn Eve die zwei ausgetauschten Nachrichten sieht, weiss sie, dass:
- $p = 13$, $g = 9$
- $x = g^a \bmod p$
- $y = g^b \bmod p$

Eve ist nun daran interessiert, a und b herauszufinden. Wenn p, a und b sehr klein sind, kann Eve die Werte nur durch Ausprobieren finden (Irreversibilität). Anschliessend kann sie $S_{AB} = g^{ab} \bmod p$ bestimmen.
Wenn diese drei Zahlen aber sehr gross gewählt werden, dauert es extrem lange, sie zu berechnen.

Auftrag 10

Als aktive Gegnerin kann sich Eve als Bob ausgeben und mit Alice das Diffie-Hellman-Protokoll durchführen. Dabei fängt sie die erste Kontaktaufnahme von Alice an Bob ab und antwortet in dessen Namen. Schlussendlich erhält Eve den gleichen symmetrischen Schlüssel wie Alice, die davon ausgeht, mit Bob kommuniziert zu haben. Dieser wiederum ist ahnungslos, da er vom Schlüsselaustausch nichts mitbekommen hat.

Damit Alice und Bob sicherstellen können, dass sie mit der richtigen Person kommunizieren, macht es Sinn, digitale Signaturen einzuführen. Dabei wird der Nachweis der Identität mit einem privaten Schlüssel verschlüsselt, und jeder kann mit dem passenden öffentlichen Schlüssel den Absender der Nachricht identifizieren.