Secret-Sharing

Einleitung

Die folgenden Materialen dienen als Einblick in Secret Sharing Methoden. Bei Secret Sharing handelt es sich um Verschlüsselungen mit einer Vielzahl zugehöriger Schlüssel. Je nach Methode benötigt man für die Entschlüsselung alle erstellten Schlüssel (Addition von Zufallszahlen/graphische Verschlüsselung) oder eine bestimmte minimale Anzahl Schlüssel (Shamir's Secret-Sharing-Methode), um den Geheimtext/die Geheimzahl zu entschlüsseln. Dieses Thema eignet sich als Anschlussthema zur Kryptologie, kann aber auch mit dem Ziel der Vertiefung bzw. Festigung behandelt werden, sei es im Grundlagenfach oder Ergänzungsfach Informatik. Gerade die Secret-Sharing-Methode von Adi Shamir lässt sich gut graphisch darstellen und eignet sich zur Veranschaulichung eines sehr eleganten Algorithmus, der erst 1979 erstellt wurde und in der Informatik (z.B. bei crypto wallets) heute angewendet wird.

Lernziele

- Die Lernenden verstehen den Aufbau einfacher Secret-Sharing-Methoden und wenden sie an.
- Die Lernenden erarbeiten die Grundkonzepte der Secret-Sharing-Methode von Adi Shamir.

Jahrgangsstufe

Ergänzungs- oder Grundlagenfach 11. Klasse

Vorwissen

aus dem Grundlagenfach Informatik

- Grundlagen Kryptologie (Klartext / Geheimtext / Schlüssel)
- Caesar-Verschlüsselung / monoalphabetische Substitution
- Vigenère-Verschlüsselung / polyalphabetische Substitution
- Modulo-Operation

aus dem Mathematikunterricht

- Erstellen von linearen Funktionen

Ablauf

- Einstieg: Repetition bekannter Chiffriermechanismen
- Hauptteil Theorie: Einführung Secret-Sharing mit Beispielen
- Wissenssicherung: Lösen und Besprechen der Aufgaben

  Bemerkung: Die Wissenssicherung kann jeweils direkt nach den zugehörigen Theorieblöcken erfolgen.

Zeitaufwand

Repetition:	ca. 1 Lektion (inkl. Übungen)
Secret-Sharing:	ca. 2 Lektionen Theorie
	ca. 1 Lektion Übungen und Besprechung

Webseite zum Erstellen von visuellen Verschlüsselungen

https://kryptografie.de/kryptografie/chiffre/visuelle-kryptografie.htm

Verschlüsselung mit mehreren Schlüsselträgern: Secret-Sharing

Im ersten Teil möchten wir die bereits bekannten Caesar- und Vigenère-Chiffriermechanismen repetieren. Im zweiten Teil betrachten wir Möglichkeiten, wie man mehrere Schlüssel generieren kann, die auf mehrere Individuen aufteilbar sind. Dies wird auch Secret-Sharing genannt.

1. Einstiegsaufgabe: bekannte Chiffriermechanismen

Bevor wir mit den Secret-Sharing-Methoden starten, wiederholen wir die wichtigsten Konzepte der uns bereits bekannten Chiffriermechanismen. Tausche dazu eine Geheimbotschaft mit dem nebensitzenden Klassenmitglied gemäss der untenstehenden Anleitung aus und fülle danach die Lücken der Kurzbeschreibung zu den jeweiligen Verschlüsselungen mit den korrekten Begriffen.

a) Austauschen einer Geheimbotschaft

i. Wähle deinen Namen als Schlüsselwort für die Vigenère-Verschlüsselung.
ii. Führe zuerst eine Verschlüsselung deines Schlüsselwortes mit der gegebenen Caesar-Scheibe (S. 2) durch.
iii. Führe mit dem verschlüsselten Schlüsselwort eine Vigenère-Verschlüsselung eines Geheimtextes deiner Wahl durch.
iv. Tausche mit deinem benachbarten Klassenmitglied den Geheimtext aus und dechiffriere ihn. Er*Sie hat für die Verschlüsselung die gleiche Caesar-Scheibe benutzt.

Wieso funktioniert diese Dechiffrierung, obwohl kein Schlüsselwort direkt ausgetauscht wurde?

Sie funktioniert, da das Schlüsselwort (der Name) indirekt bekannt ist und dieselbe Caesar-Verschiebung benutzt wird.

b) Caesar-Verschlüsselung

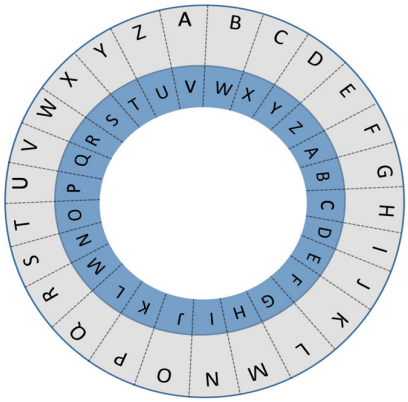
Bei der Caesar-Chiffrierung handelt es sich um eine _____monoalphabetische_____ Substitution.

Diese Eigenschaft kann zum ____Entschlüsseln_____ des Geheimtextes ausgenutzt werden. Dazu wird die _____Häufigkeitsverteilung_____ der verschiedenen Buchstaben in der Ursprungssprache des _____Klartextes_____ betrachtet. Somit werden solche Chiffrierverfahren nicht einzeln angewandt.

c) Vigenère-Verschlüsselung

Bei der Vigenère-Verschlüsselung handelt es sich um eine ___ polyalphabetische _____ Substitution. Der Geheimtext kann nur entschlüsselt werden, wenn das Schlüsselwort ___mehrfach für verschiedene Verschlüsselungen verwendet wird_____.

Caesar-Scheibe mit
Verschiebung = 21



	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

2. Secret Sharing

Die Einstiegsaufgabe zeigt, dass wir relativ einfach eine Verschlüsselung mit mehreren Schlüsseln erzeugen können (Anzahl der Caesar-Verschiebungen sowie Vigenère-Schlüssel). Zwei Personen erhalten nun je einen Schlüssel. Damit ist klar, dass sie zusammenfinden müssen, um den Geheimtext zu dechiffrieren. Da die Caesar-Verschlüsselung über einen kleinen Schlüsselraum verfügt, wäre die Person, die das Schlüsselwort zugeteilt bekommt, im Einstiegsbeispiel jedoch stark im Vorteil.

Es gibt Situationen, in welchen eine solche Schlüsselaufteilung erwünscht ist und eingesetzt wird. Zum Beispiel sind gewisse Waffensysteme so gesichert, dass mehrere Schlüssel für die Entsicherung notwendig sind. Im Bankensystem muss beispielsweise die Überweisung grosser Geldsummen oft von mehreren Stellen bewilligt werden. Um bei solch wichtigen Verschlüsselungen eine grössere Sicherheit zu gewährleisten als es im Einstiegsbeispiel der Fall ist, benötigt man andere Verschlüsselungsverfahren. Wir werden nun drei mögliche Varianten genauer kennenlernen, wobei jedoch zuerst geklärt wird, was *Sicherheit* bei Verschlüsselungssystemen mit mehreren Schlüsseln bedeutet.

a) Was bedeutet „Sicherheit“ bei Secret-Sharing-Methoden?

Betrachten wir nochmals die Vigenère-Verschlüsselung; um aus dem Schlüsselwort mehrere Schlüssel zu generieren, könnten wir es prinzipiell einfach in Stücke schneiden.

Beispiel:

Nehmen wir an, unser Schlüsselwort besteht aus 15 Zeichen. (Hier: **NidwaldenRules!)**

Dies wird nun in sieben Stücke à je 3 Buchstaben aufgeteilt. Diese sieben Stücke können nun als Schlüssel verteilt werden und nur durch das Zusammenführen aller Stücke wird das Schlüsselwort bekannt.

Anwendungsversuch:

Aufteilung des Schlüsselwortes:

Nid _ _ _ _ _ _ _ _ _ _ _ _ _ _ _wal _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ den _ _ _ _ _ _
_ _ _ _ _ _ _ _ _ Rul_ _ _ _ _ _ _ _ _ _ _ _ _ _ es!

Als Lehrer kann man die sieben Teilstücke Nid, wal, den, Rul, es! gemäss dem Zufälligkeitsprinzip an die Klassenmitglieder verteilen. Zudem kann man vorgeben, dass das Lösungswort aus 15 Zeichen besteht.
Danach sollen sie in Vierergruppen mit unterschiedlichen Teilstücken eingeteilt werden und versuchen, das Lösungswort zu erraten. Als Kontrollgruppe können auch Zweier- und Dreier-Gruppen oder sogar Einzelpersonen versuchen, das Lösungswort zu erraten. Dies soll zeigen, dass der Anteil der partiellen Information mit der Gruppengrösse wächst.
Hinweis: Das !-Zeichen macht es für Gruppen ohne es! schwierig, das Schlüsselwort zu knacken. Dies zeigt, dass für gewählte Passwörter eine zufällige Zeichenwahl besser ist. (https://www.tagblatt.ch/leben/cybersicherheit-eine-studie-zeigt-es-schwarz-auf-weiss-unsere-passwoerter-sind-geistlos-ld.2216525)

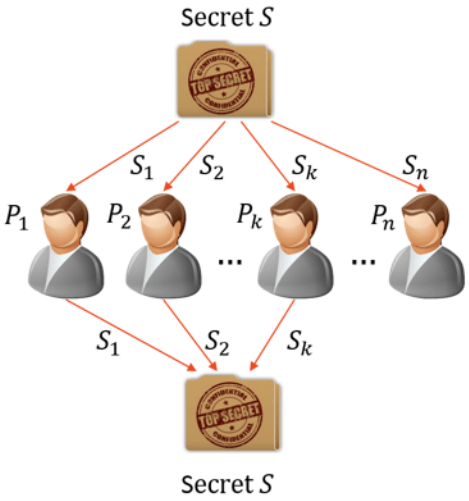
Wir sehen, dass mit dieser Methode jede Person über eine *partielle Information* des Schlüssels verfügt. Die nötige Anzahl Versuche den Schlüssel via Brute-Force-Methode zu knacken, ist für diejenigen Personen mit einem Teilschlüssel kleiner als für Personen, die keine Informationen über den Schlüssel besitzen. Zusätzlich wird die Wahrscheinlichkeit das Schlüsselwort zu knacken immer grösser, je mehr Schlüsselträger sich zusammenschliessen.

Eine sichere Secret-Sharing-Methode sollte jedoch gewährleisten, dass Personen oder Gruppen mit einem Teilschlüssel oder mehreren Teilschlüsseln keine kleinere Anzahl nötiger Versuche benötigen, um den Gesamt-Schlüssel zu erraten. Damit entfallen alle Methoden, bei welchen ein Passwort in Stücke aufgeteilt wird, und es werden Methoden verlangt, bei denen der verteilte Schlüssel keine *partiellen Informationen* über den Schlüssel preisgibt.

Hinweis: An dieser Stelle kann als Übung die Aufgabe 3.i gelöst werden.

Sicheres Secret-Sharing

Sichere Secret-Sharing-Verfahren fügen ihren Schlüsseln Zufälligkeit hinzu. Bei numerischen Schlüsseln werden dafür zwei Zufallszahlen modular addiert und jedem Schlüsselträger wird eine der Zufallszahlen mitgeteilt. Keiner der beiden Schlüsselträger kann mit seiner Zahl das Secret schneller knacken, er hält mit dem Teilschlüssel keine partielle Information des Schlüssels in Händen.

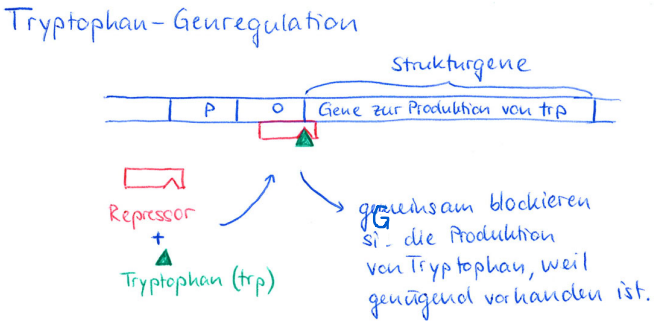


Dieses Verfahren wird auch als One-Time-Pad (Einmalverschlüsselung) bezeichnet und wurde von Claude Shannon[1] als hochsicher bewiesen. Charakteristisches Merkmal des One-Time-Pads ist, dass der Schlüssel und die Zufallszahlen (Teilschlüssel) gleich lang sind.

Zwei Schlüsselträger müssen sich treffen, die Schlüssel zusammenlegen, um den Schlüssel für die Entschlüsselung der Geheimnachricht zu erhalten.
Dies kann beliebig ausgeweitet werden, indem n Schlüssel verteilt werden (siehe Bild rechts).

Beispiel:

Auch biochemische Rückkoppelungsprozesse bedienen sich der sicheren Methodik: Eine Wirkung wird nur erzielt, wenn zwei Komponenten (z.B. Coenzym und Enzym) vorhanden sind und eine Bindung eingehen.



Im Bild links siehst du die Genregulation am Beispiel von Tryptophan (Aminosäuren).

Weder der Repressor noch die Aminosäure selber können die Produktion stoppen.

b) Addition von Zufallszahlen

Die addierten Zufallszahlen bestehen aus beliebig vielen Ziffern, müssen aber beide gleich lang sein. Die Addition ist eine modulare, das heisst, es gibt keinen Übertrag.

Beispiel im Binärsystem:

110100011	*Schlüssel S_1*
+ 100010101	*Schlüssel S_2*
010110110	*Schlüssel zur Entschlüsselung der Geheimnachricht*

Um den Schlüssel zu generieren, müssen beide Schlüssel S_1 und S_2 bekannt sein. Ein einzelner Schlüssel enthält keine partielle Information und somit ist es eine sichere Secret-Sharing-Methode.

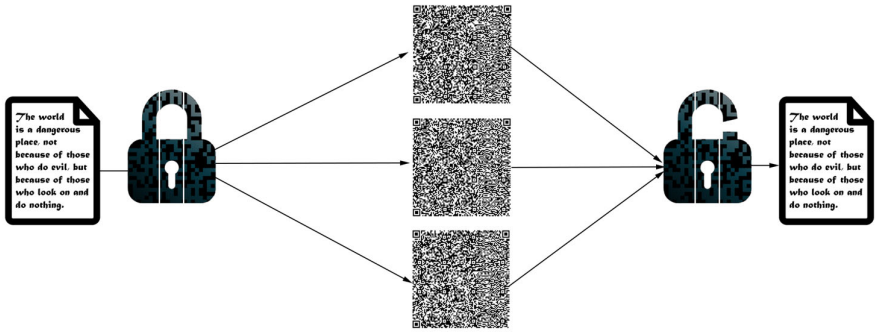
Hinweis: Du kannst nun die Aufgaben 3.ii und 3.iii lösen.

[1] Claude Shannon war ein amerikanischer Mathematiker, welcher als Begründer der Informationstheorie gilt. Er leistete einen grossen Beitrag bei der Erarbeitung der Grundlagen der Kryptologie.

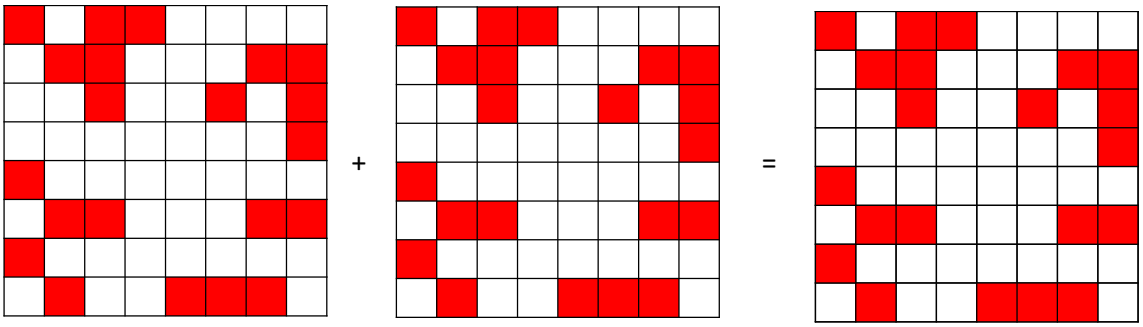
c) Graphische Verschlüsselung

Seit dem 1. Oktober 2022 gehören orange und rote Einzahlungsscheine der Vergangenheit an. Die Rechnungen werden neu über Einzahlungsscheine mit dem «Swiss QR-Code» bezahlt, der alle nötigen Rechnungsinformationen in graphischer Art enthält.

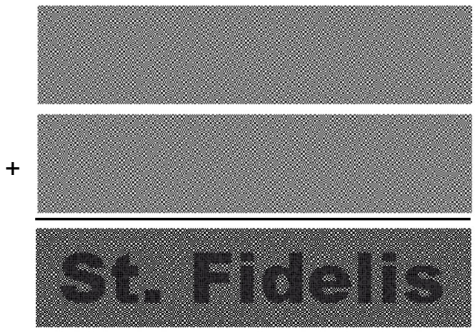
Informationen können somit ebenfalls graphisch verschlüsselt werden. Dazu werden graphische Informationen zufällig aufgesplittet. Ein Pixel (kleines Quadrat) ist ein Teil des Ganzen, das alleine keine Nachricht oder Information trägt. Überlagert man die Pixelbilder (Teilschlüssel) unten, kann man die Information entnehmen.



Dieses Beispiel zeigt, wie die Schweizer-Flagge graphisch verschlüsselt wurde:



Ebenso entstand das Wort «St.Fidelis» aus zwei verpixelten Bildern (den beiden Teilschlüsseln), die überlagert wurden.



Hinweis: Löse Aufgabe 3.iv und 3.v.

d) Shamir's Secret-Sharing - Polynomverschlüsselung

Bei den oben genannten Methoden (abgesehen von dem Caesar- und dem Vigenère-Verfahren) werden zwingend alle erstellten Schlüssel für die Entschlüsselung benötigt. Dies bedeutet, dass die Entschlüsselung unmöglich ist, sobald ein Schlüsselhalter nicht kooperieren möchte oder ungünstigerweise ein Schlüssel verloren geht. Um dieses Problem zu lösen, betrachten wir nun den Algorithmus von Adi Shamir[2] zum Secret-Sharing-Verfahren, mit welchem eine *unendliche Vielzahl* an Schlüsseln, welche keine partielle Informationen liefern, erstellt werden kann und der zusätzlich *eine Einschränkung* der minimal benötigten Anzahl Schlüssel für eine erfolgreiche Entschlüsselung erlaubt.

Minimal zwei benötigte Schlüssel – Lineare Funktionen

Nehmen wir an, wir möchten 10 Agenten, die eine wertvolle private Sammlung bewachen, mit je einem Schlüssel ausstatten. Dabei soll der Eingang zur Sammlung nur von mindestens zwei Schlüsselträgern zusammen geöffnet werden können. Dadurch wollen wir sicherstellen, dass nie ein einzelner Schlüsselträger die Sammlung bewacht und unbemerkt (vorausgesetzt die installierten Videokameras haben einen anderen Beobachtungswinkel eingenommen) einen Gegenstand entfernen kann.

Übertragen wir das Problem auf eine lineare Funktion, die eine Gerade beschreibt, dann sind alle Punkte auf dem Funktionsgraphen mögliche Schlüssel. Mit zwei bekannten Punkten kann der Funktionsgraph der allgemeinen Art $f(x) = y = ax + b$ erstellt werden. Der y-Achsenabschnitt, Punkt (0, y), steht dabei für die Geheimzahl.

Beispiel:

Nehmen wir an, unser Eingangscode wäre 2 (natürlich wäre eine mehrstellige Zahl besser, dies dient nur als Beispiel). Somit lautet eine mögliche lineare Funktion mit f(x = 0) = 2:

$$f(x) = y = x + 2$$

Nun können 10 mögliche Lösungen der Funktion berechnet werden und die jeweiligen x,y-Wertepaare den Agenten zugeteilt werden.

Zum Beispiel:

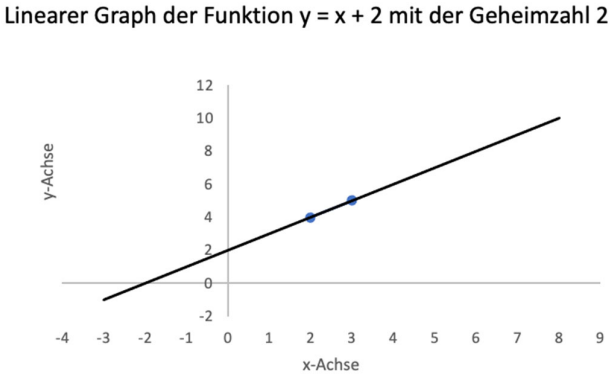
Wertepaar	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
x	*3*	*2*	*-2*	*5*	*9*	*-5*	*13*	*16*	*-12*	*1*
y	*5*	*4*	*0*	*7*	*11*	*-3*	*15*	*18*	*-10*	*3*

Die dazugehörige lineare Funktion kann nun mit zwei beliebigen Wertepaaren bestimmt werden und danach x_0 als Geheimzahl aufgelöst werden. Ein Wertepaar besitzt keine partielle Information zur Geheimzahl.

Graphisch betrachtet sind die Wertepaare Punkte auf dem Funktionsgraphen. Es werden zwei Punkte benötigt, um eine Gerade zu zeichnen und den y-Achsenschnittpunkt der beschriebenen Gerade zu bestimmen.

[2] Adi Shamir ist ein israelischer Kryptologie Experte, welcher unteranderem an der Entwicklung des heutzutage häufig angewendeten RSA-Verfahrens (das S steht dabei für Shamir) beteiligt war.

Nehmen wir an, die Punkte A(3,5) und B(2,4) sind bekannt. Die dazugehörige Gerade sieht dann wie folgt aus:

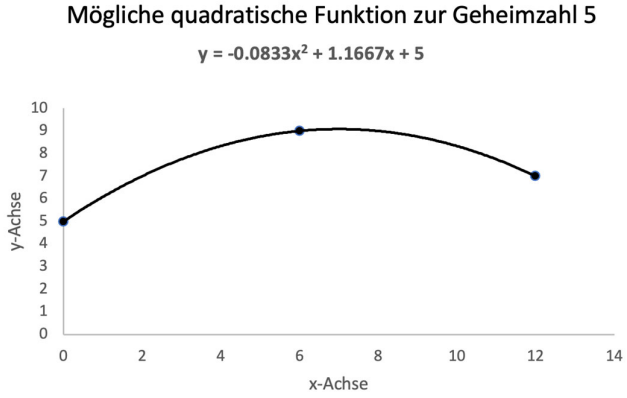


Daraus lässt sich der y-Achsenschnittpunkt (x = 0) herauslesen und somit die Geheimzahl 2 bestimmen. Mit nur einem Punkt ist es jedoch nicht möglich, die Gerade zu zeichnen und man besitzt keine zusätzlichen Informationen zum y-Achsenschnittpunkt. Somit ist dies eine sichere Secret-Sharing-Methode.

Löse die Aufgabe 3.vi.

Minimal drei benötigte Schlüssel – Quadratische Funktionen

Wir vermuten, dass sich zwei der Schlüsselträger verbündet haben, um eines bestimmten Objekts der Sammlung habhaft zu werden. Um dies zu verhindern, generieren wir neue Schlüssel, die gewährleisten, dass mindestens 3 Schlüssel benötigt werden, um in die private Sammlung zu gelangen. Dazu können wir die mathematische Bedingung, dass 3 Punkte benötigt werden, um einen Funktionsgraphen einer quadratischen Funktion zu zeichnen, ausnutzen.



Für eine quadratische Funktion $ax^2 + bx + c = f(x)$ kann man also je einen Punkt $(x_i, f(x_i))$ an n Personen verteilen. Jedoch müssen nur drei von ihnen kooperieren, um die Funktion (Koeffizienten a, b und c) eindeutig zu bestimmen.

Löse, um dies zu zeigen, das lineare Gleichungssystem unter 3.vii.

Verallgemeinerung – Polynomfunktionen n-ten Grades

Die folgende mathematische Aussage kann dazu verwendet werden, die Menge an benötigten Schlüsseln zu definieren.

Es werden jeweils *n* unterschiedliche Punkte $(x, f(x))$ benötigt, um einen Graphen des Polynoms $(n-1)$*ten* Grades zu zeichnen.

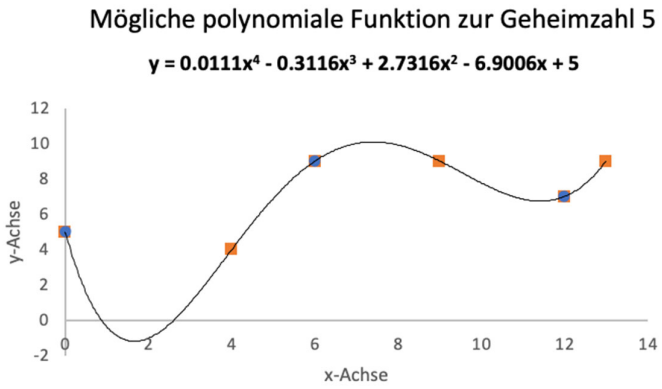
Oder in anderen Worten ausgedrückt:

Bei einer Polynomfunktion n-ten Grades müssen somit n+1 Schlüsselträger zusammenfinden, um das Secret herauszufinden.

Beispiel:

Man möchte 10 Schlüssel für einen Safe generieren. Falls die Mehrheit der Schlüsselträger anwesend ist (≥ 5), soll der Safe mit den vorhandenen Schlüsseln geöffnet werden können.

Welche Voraussetzungen müssen gegeben sein? Definiere n, den Funktionsgrad und erkläre mit Hilfe des untenstehenden Graphen, welchen Punkt du nicht als Schlüssel verteilen darfst.



Verschlüsselung einer Geheimzahl, die nicht auf der y-Achse liegt

Bis jetzt befand sich die Geheimzahl immer auf der y-Achse. Somit musste man den Wert der aus den Punkten berechneten polynomialen Funktion für x = 0 berechnen oder den y-Achsenschnittpunkt des gezeichneten Graphen bestimmen. Diese Einschränkung ist jedoch nicht zwingend. So kann der Schlüsselersteller, ohne dass das Vorgehen an Sicherheit einbüsst, eine beliebige x-Koordinate vorgeben, an deren y-Koordinate des Graphs sich die Geheimzahl verbirgt. Diese x-Koordinate wird als öffentlicher Schlüssel für alle bekannt gegeben.

Löse nun die Aufgaben 4.i-iii, welche alle besprochenen Secret-Sharing-Methoden nochmals behandeln.

3. Aufgaben

Die folgenden 6 Aufgaben sind in Einzelarbeit zu lösen.

i. *Ist es möglich, mit mehreren aneinander folgenden Caesar-Verschiebungen eine Vielzahl an Schlüssel zu generieren und somit eine „sinnvolle" Secret-Sharing-Methode zu erstellen? Begründe deine Aussage.*

Das ist nicht möglich, da Mehrfachverschiebungen die Caesar-Verschlüsselung nicht sicherer machen; zum Beispiel ist die Verschiebung von zuerst 3 und danach 5 gleichwertig zu einer Verschiebung von 8. Es besitzen somit alle Schlüsselträger eine partielle Information, welche es allen erlaubt den Geheimtext zu entschlüsseln.

ii. *Bestimme zwei Schlüssel (S1 und S_2), die die Geheimzahl 327493 verschlüsseln mit den Ziffern des Dezimalsystems.*

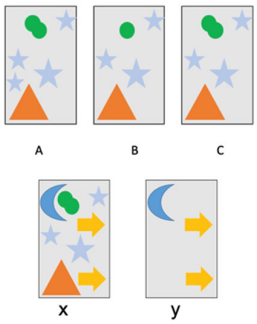
Individuelle Lösungen
Z.B.

$$\begin{array}{r} 712853 \\ +\,615640 \\ \hline 327493 \end{array}$$

iii. *Du findest bei zwei verschiedenen Agenten die Zahlen 11001010001 und 01110110100. Wie lautet die verschlüsselte Geheimzahl?*

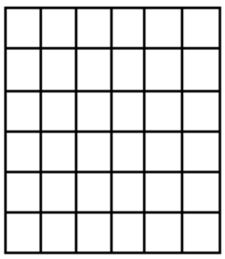
$$\begin{array}{rl} 11001010001 & \textit{random secret} \\ +\,01110110100 & \textit{random number} \\ \hline 10111100101 & \textit{secret number} \end{array}$$

iv. *Zu welchem Bild (A, B oder C) gehören die beiden visuellen Schlüssel (x und y)?*

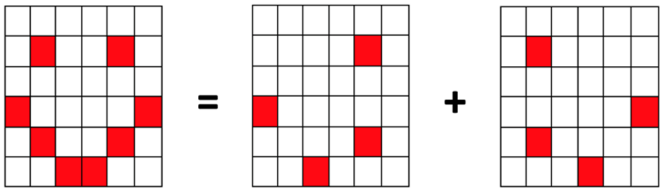


Lösung: c

v. *Verschlüssle eine selbst erstellte Graphik im gegebenen Pixelraster:*



Lösung Beispiel:



vi. *Folgende Schlüssel sind verteilt worden: A (6, 8), B (-6, 2), C (10, 10), D (-2, 4). Du weisst vom Ersteller der Schlüssel, dass sich zwei Schlüsselträger treffen müssen. Finde die Geheimzahl heraus.*

$$\text{I:}\quad f(x_1) = 10 = 10a + b$$
$$\text{II:}\quad f(x_2) = 2 = -6a + b$$

II von I subtrahieren und nach a auflösen

$$a = \frac{1}{2}$$

a in I einsetzen und nach b auflösen

$$b = 5$$
$$f(x_1) = \frac{1}{2}x + 5$$

Mit dem y-Achsenabschnitt ist die Geheimzahl gegeben: 5

vii. *Gegeben sei eine allgemeine quadratische Funktion f(x) = ax^2 + bx + c. Die Punkte R(1/2), Q(−1/3) und S(0/1) liegen auf dem Graphen der Funktion f.*
Bestimme mit Hilfe dieser Informationen die Parameter a, b und c und notiere die quadratische Funktion.

$$\text{I:}\quad f(x_1 = 1) = 2 = a + b + c$$
$$\text{II:}\quad f(x_2 = -1) = 3 = a - b + c$$
$$\text{III:}\quad f(x_3 = 0) = 1 = c$$

c einsetzen in I und II

$$\text{IV:}\quad f(x_1) = 2 = a + b + 1$$
$$\text{V:}\quad f(x_2) = 3 = a - b + 1$$

IV + V

$$\text{VI:}\quad f(x) = 5 = 2a + 2$$

umformen

$$a = \frac{3}{2}$$

a in IV einsetzen und nach b auflösen

$$b = 2 - \frac{3}{2} - 1 = -\frac{1}{2}$$

$$f(x) = \frac{3}{2}x^2 - \frac{1}{2}x + 1$$

4. Die folgenden drei Aufgaben sollten in Gruppen (mind. zu dritt) gelöst werden.

i. Verschlüssele eine Zahl, von welcher du die x-Koordinate der Geheimzahl als öffentlichen Schlüssel bekannt gibst, mit der Shamir-Secret-Sharing-Methode, sodass zwei Schlüssel für die Entschlüsselung benötigt werden. Tausche die Schlüssel und die x-Koordinate mit zwei Personen der Klasse aus und lass sie deine Geheimzahl bestimmen.

Beispiel: Vorgehensweise:

Gewählte Geheimzahl = 5; gewählter bekannter Schlüssel x = 3

Bestimme eine lineare Funktion, die eine Gerade mit einem zufälligen Punkt, zum Beispiel A(2, 1) und dem Punkt der Geheimzahl G(3, 5) beschreibt:

y = 4x – 7 (analoges Vorgehen zu 3.vi)

Als Nächstes bestimmst du einen weiteren zufälligen Punkt auf der Gerade – zum Beispiel für x = -6:

*B(-6, -31) (y = 4 *(-6) – 7 = -31)*

Nun werden die beiden Punkte A(2,1) und B(-6, -31) sowie der öffentliche Schlüssel x = 3 übergeben.

Zum Entschlüsseln wird mit den beiden Punkten die lineare Funktion, die die Gerade beschreibt, berechnet und für x = 3 aufgelöst.

ii. Verschlüssele eine 4-stellige Zahl im Dezimalsystem mit der Methode der Zufallszahladdition. Verteile die beiden Schlüssel S_1 und S_2 an Klassenmitglieder und lass sie deine Geheimzahl bestimmen.

Individuelle Lösungen, in Anlehnung an die Aufgabe 3.ii und 3.iii.

iii. Zeichne ein Bild und verschlüssele es mit der visuellen Verschlüsselung. Tausche die erstellten Bild-Schlüssel mit anderen aus und lass sie dein originales Bild zeichnen.

Individuelle Lösungen, in Anlehnung an die Aufgabe 3.iv und 3.v.