Kid Krypto: Public Key Verschlüsselung

Materialien

Die Schülerinnen und Schüler (SuS) werden in Gruppen von ungefähr 4 SuS aufgeteilt und in diesen Gruppen in jeweils 2 Untergruppen. Jede Untergruppe erhält eine Kopie der Vorlage S. 5.

Für jede Gruppe wird benötigt:

- 2 Kopien der Vorlage S. 5
- 1 Kopie der Vorlage S. 6
- eine Möglichkeit zur Annotation

Aufgabe:

Amy möchte Bill eine geheime Nachricht senden. Normalerweise denken wir bei einer geheimen Nachricht an einen Satz oder einen Abschnitt, aber in der folgenden Übung möchte Amy nur ein Zeichen senden – tatsächlich wird sie eine Nummer senden, die ein Zeichen repräsentiert. Obwohl das wie eine sehr vereinfachte Nachricht erscheint, muss man bedenken, dass Amy eine ganze Kette solcher Nachrichten senden kann, um einen Satz zu produzieren.

Wir werden sehen, wie Amys Nummer durch die Nutzung von Bills öffentlichem Schloss so verschlüsselt wird, dass - falls irgendjemand diese Nachricht auffängt - es für einen Fremden nicht möglich sein wird, sie zu entschlüsseln. Nur Bill kann das, weil nur er den Schlüssel zu diesem Schloss hat.

Vorüberlegungen

Wir werden Nachrichten dadurch verschlüsseln, indem wir Karten nutzen; Straßenkarten wo Linien Straßen repräsentieren und Punkte Straßenecken. Jede Karte hat eine öffentliche Version: das Schloss und eine private Version: den Schlüssel. Bill legt seine öffentliche Version der Karte auf einen Tisch oder eine Webpage, sichtbar für jedermann oder – ebenso gut – gibt sie jedem, der ihm eine Nachricht senden möchte. Amy hat wie alle anderen eine Kopie. Bild 1 zeigt Bills private Karte. Es ist die gleiche wie seine öffentliche Karte mit der Ausnahme, dass einige Straßenecken durch Vergrößerungen hervorgehoben sind. Diese Version der Karte hält er geheim.

Diese Aktivität muss exakt ausgeführt werden; Fehler verursachen viele Folgeprobleme. Ebenso ist es wichtig, dass die SuS erkennen, dass diese Art der Verschlüsselung überall vorgenommen werden kann. Motivierend für Schülerinnen und Schüler ist, dass sie diese Methode nutzen können, um geheime Nachrichten in der Klasse zu versenden und dass sogar, wenn der Lehrer versteht, wie die Mitteilung verschlüsselt ist, diese nicht in der Lage sein wird, sie zu entschlüsseln.

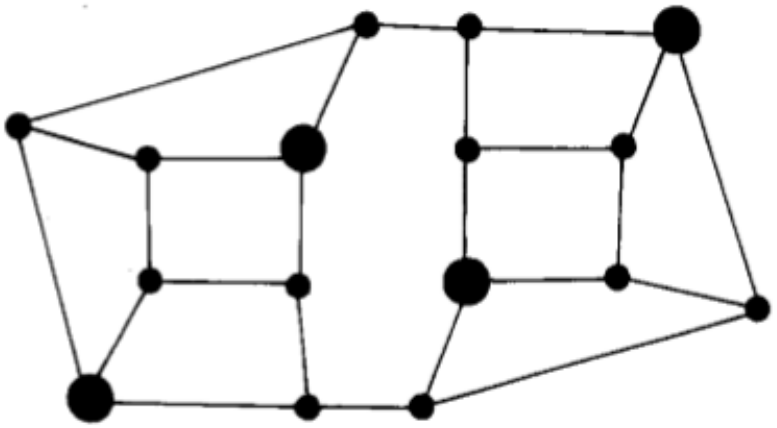


Bild 1: Bills private Karte

Vorgehen:

1. Händige Bills öffentliche Karte aus (S. 7). Entscheide, welche Zahl Amy versenden wird. Nun platziere zufällige Zahlen an jeder Kreuzung der Karte, so dass diese addiert werden können zu der Zahl, die Amy senden möchte. Bild 2 gibt ein Beispiel für solche Zufallszahlen - neben jeder Kreuzung (die obere, nicht geklammert Zahl). Hier hat Amy entschieden, die Zahl 66 zu senden, so dass die Zufallszahlen später zu 66 addiert werden können.

2. Jetzt muss Amy berechnen, was sie Bill senden möchte. Wenn sie die Karte mit den Zahlen darauf sendet, wäre es nicht gut, denn falls sie in die falschen Hände fällt, kann man sie addieren und bekommt die Nachricht. Stattdessen wird jede Kreuzung genutzt und auf diese und deren 3 Nachbarn geguckt – also auf 4 Kreuzungen und die zu ergänzenden Zahlen. Schreibe diese Zahlen an die Kreuzung in Klammern oder nutze verschiedene Farben.

Ein Beispiel: die Kreuzung ganz rechts in Bild 2 (bezeichnet mit 6) ist mit 3 anderen Kreuzungen verbunden, bezeichnet mit 1, 4, 11. Man kommt auf eine Gesamtsumme ist 22. Jetzt wiederhole dieses für alle anderen Kreuzungen in der Karte. So kommst Du zu den Zahlen in Klammern (Bild 2).

3. Amy möchte Bill diese Karte senden, nur mit den Zahlen in Klammern darauf. Lösche die Originalzahlen oder fertige eine neue Karte an mit nur diesen Zahlen darauf. Schau, ob jemand von den Kindern einen Weg finden kann, um hieraus sagen zu können, was wohl die Originalnachricht war. Sie werden dazu nicht in der Lage sein.

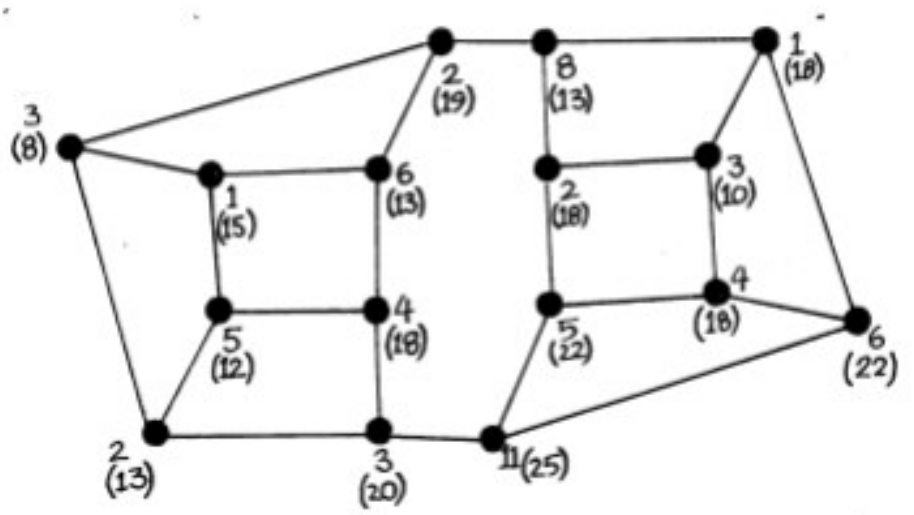


Bild 2: Amys Berechnungen auf Grundlage von Bills öffentlicher Karte

4. Nur jemand mit Bills privaten Schlüssel kann die Nachricht entschlüsseln, um die Nachricht zu finden, die Amy ursprünglich senden wollte. In der verschlüsselten Nachricht markiere die vergrößerten Knoten in Bills privaten Karte.

Um die Nachricht zu entschlüsseln, guckt Bill auf die geheimen markierten Kreuzungen und addiert die entsprechenden Zahlen. Im Beispiel heißen diese Kreuzungen 13, 13, 22, 18, welche addiert werden zu 66 – Amys Originalnachricht.

5. Wie funktioniert das? Diese Karte ist besonders. Angenommen Bill hat eine der markierten Kreuzungen gewählt und malt dann um die Kreuzungen, die jeweils eine Straße davon entfernt sind, herum und wiederholt den Vorgang für jede markierte Kreuzung. Dieses wäre dann eine Zerteilung der Karte in nicht überlappende Bereiche wie in Bild 3 illustriert. Zeige diese Bereiche den Kindern durch das Zeichnen der Grenzen auf der Karte. Die Gruppe der Kreuzungen in jedem Bereich ist genau diejenige, die zusammen die übertragenen Zahlen für die markierten Kreuzungen ergeben, so dass die Summe von 4 übertragenen Zahlen dieser Kreuzungen die Summe aller originalen Zahlen in der originalen Karte ist. Und fertig – das wird die originale Nachricht sein.

Puh! Das scheint eine Menge Arbeit zu sein, einen Brief zu senden. Und es ist tatsächlich so – Verschlüsselung ist keine einfache Sache. Aber schau was erreicht wurde: Die totale Geheimhaltung durch Nutzung eines öffentlichen Schlüssels, was keine Vorabsprachen zwischen zwei Teilnehmern benötigt. Du kannst Deinen Schlüssel veröffentlichen an einer Pinnwand und jeder kann Dir eine geheime Nachricht senden, doch niemand kann sie entschlüsseln ohne den privaten Schlüssel.

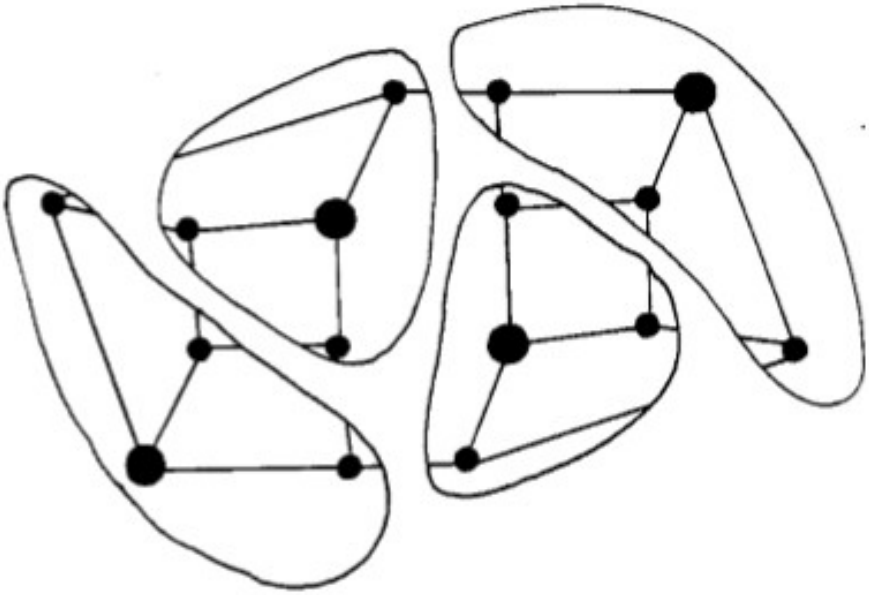
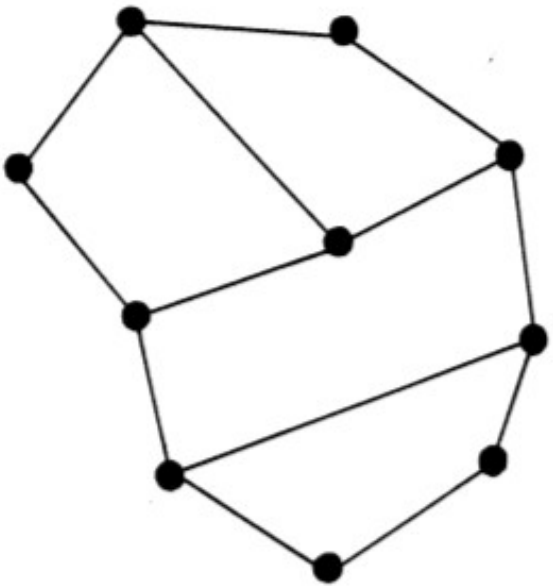


Bild 3: Die Regionen, die Bills private Karte umfassen

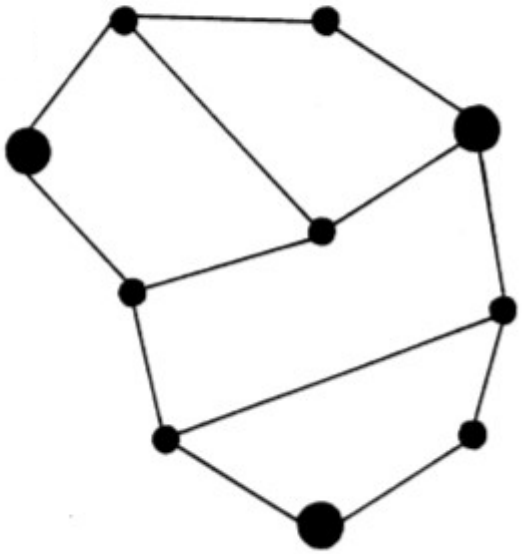
6. Wenn man jetzt das Beispiel mit der ganzen Klasse behandelt hat, teile die SuS in 4 Gruppen ein. Gib jeder Gruppe die öffentliche Karte S. 5. Jede Gruppe sollte eine Nachricht wählen (eine ganze Zahl), verschlüsseln mit dem öffentlichen Schlüssel und die Ergebniskarte einer anderen Gruppe geben. Die andere Gruppe kann versuchen, diese zu entschlüsseln, aber sie werden nicht erfolgreich sein, bis ihnen die private Karte gegeben (oder von ihnen ausgearbeitet!) wurde. Dann gib die private Karte aus und schau, ob sie korrekt entschlüsseln.

7. Jetzt kann jede Gruppe ihre eigene Karte gestalten, die private Karte jeweils geheim halten und die öffentliche Karte an eine andere Gruppe geben – oder diese an einem Klassenboard veröffentlichen. Bei der Kartengestaltung können extra Straßen hinzugefügt werden, um die Lösung zu verschleiern. Aber achte darauf, dass keine extra Straßen bei den speziellen Punkten hinzugefügt werden.

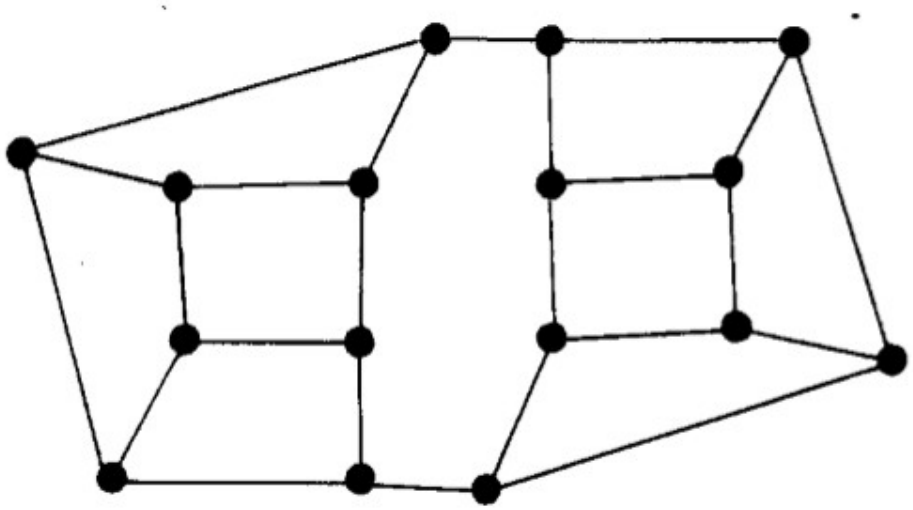
Öffentliche Karte



Private Karte



Anwendung: Nutze diese Karten, wie im Text beschrieben, zur Verschlüsselung und Entschlüsselung von Nachrichten.



Anwendung: Demonstriere anhand dieser Vorlage – bestenfalls transparent darstellen – die Verschlüsselung von Nachrichten.