Dr. Dirk Frettlöh 28.6.2023

Übungen zur Vorlesung Kryptographie

Blatt 13

Aufgabe 49: (AES-Fixpunkte)
Für jede der vier Operationen AddRoundKey, ShiftRows, SubBytes und MixColumns: Bestimmen Sie, wieviele Eingaben m es jeweils gibt, so dass die Ausgabe auch m ist. Begründen Sie Ihre Antworten. Geben Sie jeweils auch an, wieviel Prozent das sind im Vergleich mit allen möglichen Eingaben (auf drei Nachkommastellen gerundet).

(Bei AddRoundKey *dürfen Sie annehmen, dass der Rundenschlüssel nicht ausschließlich Nullen enthält. Bei* SubBytes *dürfen Sie sich erinnern, dass das per table-lookup gemacht werden kann, und die Antwort im Internet recherchieren.)*

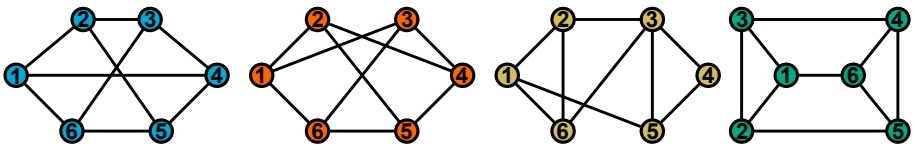
Aufgabe 50: (Wozu?)
Betrachten Sie folgendes Verfahren:

1. Alice wählt zwei große Primzahlen p, q so, dass entweder $p \equiv q \equiv 1 \bmod 4$ gilt, oder $p \equiv q \equiv 3 \bmod 4$. Dann sendet Alice $N = p \cdot q$ an Bob.
2. Bob rät, ob $p \equiv q \equiv 1 \bmod 4$ oder $p \equiv q \equiv 3 \bmod 4$ und schickt seinen Tipp an Alice.
3. Alice sendet p und q an Bob.

Wenn Bob richtig geraten hat, gewinnt Bob, ansonsten gewinnt Alice.

Welche Funktion erfüllt dieses Verfahren? Welche Funktionen erfüllen die einzelnen Schritte? Auf welchem Problem basiert das Verfahren? Warum ist das Verfahren korrekt? Warum ist das Verfahren effizient? Warum ist das Verfahren sicher?

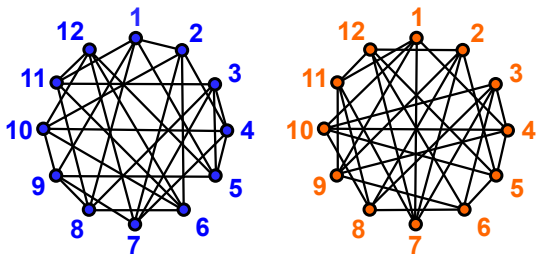
Aufgabe 51: (Commitment mit Graphisomorphie)
Eine andere Möglichkeit für Commitment-Verfahren benutzt Graphen. Ein *Graph* G ist ein Paar (V, E), wobei V die Menge der *Knoten* ist und $E \subset \big\{\{i, j\} \mid i, j \in V\big\}$ die Menge der *Kanten*. Beispiele für Graphen sind in der folgenden Abbildung dargestellt. (Z.B. ist für den Graphen $G = (V, E)$ ganz links $V = \{1, 2, 3, 4, 5, 6\}$ und $E = \big\{\{1, 2\}, \{1, 4\}, \{1, 6\}, \{2, 3\}, \{2, 5\}, \{3, 4\}, \{3, 6\}, \{4, 5\}, \{5, 6\}\big\}$).



Zwei Graphen G_1 und G_2 heißen *isomorph* zueinander, falls es eine Umnummerierung (*Permutation*) der Knoten gibt, so dass $G_1 = G_2$. (Anschaulich darf man dass auch so sehen: wenn ich die Knoten von G_1 so umnummerieren und verschieben kann, dass G_2 rauskommt, dann sind die Graphen isomorph.)

(...und jetzt die Aufgabe:) Bestimmen Sie, welche der vier Graphen im Bild isomorph zueinander sind und welche nicht. Für jedes Paar begründen Sie entweder, warum sie nicht isomorph zueinander sind, oder geben Sie eine Umnummerierung der Knoten an, die die Isomorphie zeigt.

Zusatzinformation: Eine Bit-Commitment-Anwendung geht nun so: Alice und Bob einigen sich auf zwei große nichtisomorphe Graphen G_1 und G_2. Alice wählt ein $i \in \{1, 2\}$ und schickt Bob eine umnummerierte Version von G_i. Da das Isomorphieproblem für (geeignete) Graphen schwierig ist, sieht Bob nicht, ob $i = 1$ oder $i = 2$. Später kann Alice die Umnummerierung offenlegen: mittels dieser ist es einfach, zu sehen, ob $i = 1$ oder $i = 2$. Ein immer noch zu kleines Beispiel, das aber erahnen lässt, warum das Problem schnell schwierig wird, wäre zu entscheiden, ob die beiden folgenden Graphen isomorph sind (das ist hier aber nicht gefragt).



Aufgabe 52: (Gehaltsvergleich)
In vielen Unternehmen weiß fast niemand in den gehobenen Positionen, was die Kollegen verdienen, und niemand möchte sein Gehalt verraten. Alice, Bob und Carol möchten wissen, ob sie "genug" verdienen in dem Sinne, ob sie jeweils mehr oder weniger als das Durchschnittsgehalt der drei verdienen. Dazu nutzen sie folgendes Verfahren:

1. Alice wählt eine geheime Zufallszahl r, addiert ihr Gehalt a und gibt $a + r$ an Bob weiter.
2. Bob addiert sein Gehalt b und gibt $a + b + r$ an Carol weiter.
3. Carol addiert ihr Gehalt c und gibt $a + b + c + r$ an Alice weiter.
4. Alice subtrahiert r und gibt $\frac{1}{3}(a + b + c)$ bekannt.

(a) Begründen Sie, warum das Verfahren sicher ist, d.h.: Warum kann Alice nicht b oder c ermitteln, warum Bob nicht a oder c, und warum Carol nicht a oder b?

(b) Analog zum oben geschilderten anonymen Berechnen des Durchschnittsgehalts von drei Leuten, finden Sie eine Methode zum anonymen Berechnen des Durchschnittsgehalts von n Leuten ($n \geq 3$).

(c) Wie viele Leute müssen sich oben bzw bei Ihrer Methode mindestens verabreden, um alle Gehälter ermitteln zu können? (Sie teilen untereinander alle Informationen, die sie haben; sie verraten damit natürlich auch Ihre eigenen Gehälter, zumindest untereinander.) Angenommen, alle Beteiligten sitzen an einem runden Tisch, wie genau muss diese Minimalzahl von verabredeten Leuten sitzen, um alle Gehälter zu erfahren?

Abgabe bis Dienstag 4.7.2023 bis 23:59 Uhr per Email an den Tutor.
Bitte auf jeder Abgabe das Tutorium angeben!

Jakob Niermann janiermann+krypto@techfak.de
Tim Lakämper tlakaemper+krypto@techfak.de