Übungen zur Vorlesung Kryptographie

Blatt 13

Aufgabe 49: (Secret Sharing)
Für manche Zwecke möchte man, dass n Personen $A_1, A_2, \ldots, A_n$ nur gemeinsam ein Dokument lesen/ein Tresorfach öffnen/... können. Kryptographisch kann man das so erreichen: Sei

$$p : \mathbb{R} \to \mathbb{R},\ p(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$$

Die geheime Zahlenkombination für den Tresor sei a_0. Die Person A_i kennt den Wert $p(i)$ von p an der Stelle i.

(a) Wie ermitteln alle n Personen den Wert a_0?

(b) Wieso können weniger als n Personen nicht den Wert a_0 ermitteln?

(c) Angenommen es sei $n = 4$. A_1 kennt $p(1) = 76$, A_2 kennt $p(2) = 49$, A_3 kennt $p(3) = 0$ und A_4 kennt $p(4) = -113$. Was ist der Wert von a_0?

Aufgabe 50: (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?

Aufgabe 51: (Blinde Signatur)
(a) Zeigen Sie, dass das Verfahren zur blinden Signatur in Kap 9.4 der Vorlesung bzw des Skripts korrekt ist.
(b) Begründen Sie auch kurz, warum das Verfahren sicher ist; insbesondere, warum Bob nicht das m ermitteln kann.

Aufgabe 52 (ElGamal-Signatur) Interessanterweise liefert ElGamal auch eine Signaturmethode ohne Hashfunktionen. Wieder sei G eine geeignete Gruppe und g ein Erzeuger von G. Die Schritte 1, 2 und 4 sind dieselben wie beim ElGamal-Verschlüsseln. Hier muss der Parameter g^r eine ganze Zahl sein, daher schildern wir das Verfahren zunächst für $G = Z_p^*$.

ElGamal-Verschlüsselung mit Signatur:

Vorab: Alice wählt zufällig $a \in \{2, 3, \ldots, p-1\}$ (geheimer Schlüssel) und veröffentlicht p, g und g^a. Auch Bob wählt zufällig ein $b \in \{2, 3, \ldots, p-1\}$ (geheimer Schlüssel) und veröffentlicht p, g und g^b.
Verschlüsseln: Bob wählt zufällig $r \in \{2, 3, \ldots, p-2\}$ mit $\text{ggt}(r, p-1) = 1$ und berechnet den Einmalschlüssel $k \equiv (g^a)^r \bmod p$. Er verschlüsselt m als $c \equiv mk \bmod p$.
Signieren: Bob berechnet r^{-1} in Z_{p-1}^* sowie $s \equiv (m - bg^r)r^{-1} \bmod p-1$. Er sendet (c, g^r, s) an Alice.
Entschlüsseln: Alice berechnet $k \equiv (g^r)^a \bmod p$, dann k^{-1} in Z_p^*, und damit $m \equiv ck^{-1} \bmod p$.
Verifizieren: Alice prüft, ob $g^m \equiv (g^b)^{g^r} \cdot (g^r)^s \bmod p$. Sie akzeptiert die Signatur, falls die Gleichung stimmt.

(a) Begründen Sie kurz, warum das Verfahren effizient und sicher ist.

(b) Zeigen Sie, dass das Verfahren korrekt ist.

Abgabe bis Mittwoch 15.7.2026 bis 12:00 Uhr per Email an die Tutorin.

Lisa Henetmayr Mi 12 Uhr in S0-115 lhenetmayr+krypto@techfak.de
Lisa Henetmayr Mi 16 Uhr in U2-147 lhenetmayr+krypto@techfak.de