

Aufgabe 20: (6 Punkte)

Im Bereich des Onlinebankings wird von den meisten Banken zur Authentifizierung und Autorisierung von Benutzern ein PIN/TAN-System verwendet, wobei für jede Transaktion ein Einmalpasswort (TAN, **T**ransaktions**n**ummer) benutzt wird.

Verschaffen Sie sich einen Überblick über aktuelle Verfahren zum Einsatz von TANs und vergleichen Sie diese im Hinblick auf Sicherheit (mögliche Angriffe) und Benutzerfreundlichkeit.

Aufgabe 21: (6 Punkte)

Wir betrachten das folgende *Zero-Knowledge-Protokoll*. Dabei möchte Alice gegenüber Bob beweisen, dass sie den diskreten Logarithmus von $\beta = \alpha^a \bmod p$ kennt, ohne dabei $a \in \mathbb{Z}_{p-1}^*$ selbst zu verraten. Die Werte α , β und p (p prim) seien dabei öffentlich bekannt, wobei wir annehmen, dass a allein aus der Kenntnis dieser Werte nicht mit vertretbarem Aufwand berechnet werden kann.

Beweisprotokoll

1. Bob wählt $e \in \mathbb{Z}_{p-1}$ zufällig und sendet $c := \beta^e \bmod p$ an Alice.
2. Alice sendet $r := c^{a^{-1} \bmod (p-1)} \bmod p$ an Bob.
3. Bob akzeptiert, falls $r = \alpha^e \bmod p$ ist.

- (a) Zeigen Sie, warum Bob akzeptiert, falls Alice korrekt antwortet.
- (b) Warum lernt Bob bei der Durchführung des Protokolls nichts über a ? Warum kann Bob anhand des Protokolls keinen Dritten davon überzeugen, dass Alice den diskreten Logarithmus von β kennt?

Programmieraufgabe P7: (12 Punkte)

Implementieren Sie das Fiat-Shamir-Protokoll

- mit einer Person Alice, die das Geheimnis kennt, und
- mit einer Person Carol, die das Geheimnis nicht kennt und bei den Tests durch Bob stets eine Antwort errät.

Bestimmen Sie experimentell die Erfolgsquote für Carol bei k Wiederholungen des Tests (verschiedene Werte für k).