

Blatt 10

Aufgabe 10.1.

Nehmen Sie an, Sie hätten einen schnellen Algorithmus für das Diskrete Logarithmus Problem. Brechen Sie damit Diffie-Hellman.

Aufgabe 10.2.

Geben Sie zwei Varianten für ein Challenge/Response Authentisierungs-Verfahren mit einem public-key Verfahren an: Einmal verschlüsselt der public-key (beim Server), einmal der private-key (auf dem Faktor Haben). Welche Vor-/Nachteile haben die zwei Varianten?

Aufgabe 10.3.

Verfolgen Sie, was die SHA1 Hashfunktion aus dem Passwort "123456" macht (Platz 1 der Passwort-Charts – das ist keine positive Auszeichnung!). Einmal die erste Hauptschleife von SHA1 durchgehen reicht für einen Eindruck. Der endgültige SHA1-Hashwert von "123456" ist übrigens 7c4a8d09ca3762af61e59520943dc26494f8941b.

Aufgabe 10.4

Beim neuen PushTAN Online Banking Verfahren der Sparkassen (seit Nov. 2013) loggt sich der Kunde per Passwort im Browser auf dem PC ein, gibt eine Überweisung ein und schickt sie zum Bankserver. Der Bankserver schickt an die PushTAN-App auf dem Handy des Kunden per Handy-Internet die Überweisungsdaten. Nach deren Bestätigung durch den Kunden gibt der Kunde ein zweites Passwort auf dem Handy ein, mit dessen Hilfe und eines weiteren, auf dem Handy bei der App-Initialisierung gespeicherten Schlüssels a ein auf dem Handy verschlüsselt gespeicherter Schlüssel $e(b)$ zu einem Schlüssel b entschlüsselt wird, der zusammen mit den Überweisungsdaten den Input für eine Hashfunktion bildet. Der so berechnete Hashwert (TAN) wird von der PushTAN-App angezeigt, vom Kunden in den PC eingegeben und von dort an den Bankserver geschickt.

Wieviele und welche Authentisierungs-Faktoren sind in die Signierung der Transaktion involviert? Wieviele sind es, wenn der Kunde ein iPhone 5s hat, das vorher den Fingerabdruck prüft?

Wie sieht die Situation aus, wenn der Kunde sich nicht auf dem PC einloggt, sondern auf der Sparkassen-App (eine andere als die PushTAN App) auf dem Handy? Das wird von den Sparkassen nicht nur erlaubt, sondern für Mobile Banking empfohlen.