

Übung zur Vorlesung Kryptokomplexität II

Bearbeitungszeit: 14. Mai bis 24. Mai
Verantwortlich: Roman Zorn

Begründen Sie Ihre Antworten und bereiten Sie sie so vor, dass Sie sie in der Übung präsentieren können.

Aufgabe 1: ElGamal – Known-Message-Angriff I

Betrachten Sie den in der Vorlesung beschriebenen Known-Message-Angriff auf das ElGamal-Protokoll für digitale Signaturen. Zeigen Sie, dass die dabei definierten Werte σ , ρ und m die Verifikationsbedingung

$$\gamma^m \equiv \beta^\sigma \cdot \sigma^\rho \pmod{p}$$

tatsächlich erfüllen.

Aufgabe 2: ElGamal – Known-Message-Angriff II

Betrachten Sie erneut den in der Vorlesung beschriebenen Known-Message-Angriff auf das ElGamal-Protokoll für digitale Signaturen. Seien $p = 401$ und $\gamma = 13$ bekannt. Angenommen, Erich kennt die Werte $\langle \hat{m}, \beta, (\hat{\sigma}, \hat{\rho}) \rangle = \langle 197, 37, (75, 344) \rangle$. Führen Sie einen Known-Message-Angriff auf das ElGamal Protokoll für digitale Signaturen mit den Werten $x = 221$, $y = 80$ und $z = 23$ aus.

- (a) ► Zeigen Sie dazu zunächst, dass die Werte x , y und z gültig sind.
- (b) ► Führen Sie anschließend Erichs Angriff durch und geben Sie die gefälschte Signatur an.

Aufgabe 3: Kryptographische Hash-Funktionen

Kryptographische Hash-Funktionen finden viele Anwendungen. Unter anderem wurden sie in der Vorlesung als mögliche Gegenmaßnahmen zum Fälschen einer Signatur vorgestellt.

- (a) Betrachten Sie die folgende Hash-Funktion: $h(x) = x \bmod 33$.
- Wie in Blatt 5 Aufgabe 3 seien die Parameter $p = 383, \gamma = 5, s = 29, b = 15$ für ElGamals Signatur-Schema gegeben. Signieren Sie $m = 54$ unter Verwendung der Hash-Funktion h .
 - Geben Sie eine andere Nachricht m' an, für die diese Signatur ebenfalls gültig ist.
 - Bewerten Sie, ob h eine geeignete Hash-Funktion für die Anwendung ist.
- (b) Heutzutage verwendet man oft den *secure hash algorithm (SHA)*. Je nach Version bildet er Daten auf eine Zahl fester Länge von 160, 224, 256 bis hin zu 512 Bit ab.¹
- Angenommen Sie verwenden zur Absicherung von Signaturen den *SHA-1* mit 160 Bit. Erich kann 10000 Nachrichten inklusive Hash pro Sekunde erzeugen. Wie lange wird Erich (näherungsweise) brauchen, bis er mit 50% Sicherheit eine zweite Nachricht m' mit gleichem Hash wie m gefunden hat? Gehen Sie davon aus, dass alle Hashes etwa gleich oft vorkommen.

Aufgabe 4: Rabins Public-Key-Kryptosystem

Betrachten Sie das Kryptosystem von Rabin mit $p = 83$ und $q = 103$.

- (a) ► Verschlüsseln Sie die Nachricht $m = 177$. Was sind der öffentliche und private Schlüssel?
- (b) ► Berechnen Sie für den in Aufgabenteil (a) erhaltenen Ciphertext alle möglichen Klartexte.

¹SHA-1 (mit 160 Bit) wird nicht mehr als Sicher eingestuft. SHA-256 ist heutzutage ein Mindeststandard.