Sommersemester 2005

Hasso- Plattner- Institut, Universität Potsdam

Übung zur Vorlesung

Fachgebiet Internet- Technologien und - Systeme

Meinel / Kutzner

Aufgabenblatt 11
(NUR FÜR ULI-STUDENTEN)

(URL: http://www.hpi.uni- potsdam.de/index.php?id=411)

Abgabe: Mo, 04.07.2005, bis 12 Uhr MEZ (per E-Mail an mathias.kutzner@hpi.uni- potsdam.de)

Thema: Authentifikation, Digitale Signaturen

Erreichbare Punkte: 15

Aufgabe 1: 3 Punkte

Mit Hilfe von Zero- Knowledge- Protokollen überzeugt ein Teilnehmer einen anderen davon, dass er ein Geheimnis kennt, ohne es preisgeben zu müssen. Das Fiat-Shamir- Verfahren ist ein Beispiel dafür: Alice wählt zwei große Primzahlen p und q und berechnet $n = p \cdot q$. Nun wählt Sie zufällig und gleichverteilt eine Zahl $s \in Z_n^*$ und berechnet $v = s^2 \bmod n$. Somit ergibt sich Alice' öffentlicher Schlüssel (v, n) und ihr privater Schlüssel s.

Alice beweist nun Bob auf folgenden Weg, dass sie eine Quadratwurzel s von $v \bmod n$ kennt:

- Alice wählt zufällig und gleichverteilt eine Zahl $r \in Z_n^*$ und berechnet $x = r^2 \bmod n$. Die Zahl x sendet sie an Bob
- Bob wählt nun ein Zufallsbit $e \in \{0,1\}$ und sendet es an Alice.
- Wenn Alice den Wert $e = 0$ erhält, schickt sie die Zufallszahl r an Bob. Bob verifiziert, dass $r^2 \equiv x \bmod n$ ist.
- Wenn Alice den Wert $e = 1$ erhält, schickt sie die Zahl $y = r \cdot s \bmod n$ an Bob. Bob verifiziert, dass $y^2 \equiv x \cdot v \bmod n$ ist.

Sei $n = 143$, $v = 82$, $x = 53$ und $e = 1$. Bestimmen Sie eine gültige Antwort, die die Kenntnis einer Quadratwurzel von $v \bmod n$ beweist.

Aufgabe 2: 12 Punkte

Der Digital Signature Algorithm (DSA) wird im Digital Signature Standard (DSS) zum Signieren von Nachrichten verwendet. Machen Sie sich mit diesem Algorithmus vertraut.

Sei $p = 2237$ und $g = 1984$. Der geheime Schlüssel von Alice ist $a = 1234$. Der Hashwert einer Nachricht m sei $h(m) = 111$. Alice benutzt DSA, wobei q der größte Primteiler von $p - 1$ ist. Sie verwendet $k = 25$. Wie lautet die entsprechende DSA-Signatur? Verrifizieren Sie diese Signatur. Geben Sie Ihren kompletten Lösungsweg an.

Hinweise:

Schlüsselerzeugung:

- Alice erzeugt eine Primzahl q mit $2^{159} < q < 2^{160}$
- Alice wählt eine große Primzahl p mit folgenden Eigenschaften:
  - $2^{511+64 \cdot t} < p < 2^{512+64 \cdot t}$ für ein $t \in \{0,1,\ldots,8\}$
  - Primzahl q ist ein Teiler von $p-1$
- Alice wählt eine Primitivwurzel $x \bmod p$ und berechnet $g = x^{(p-1)/q} \bmod p$
- Alice wählt eine Zahl a zufällig in der Menge $\{1,2,\ldots,q-1\}$ und berechnet $A = g^a \bmod p$

Öffentlicher Schlüssel von Alice ist (p,q,g,A) und ihr geheimer Schlüssel ist a.

Erzeugung der Signatur:

- Alice wählt Zufallszahl $k \in \{1,2,\ldots,q-1\}$
- Alice berechnet $r = (g^k \bmod p) \bmod q$
- Alice setzt $s = k^{-1}(h(m) + ar) \bmod q$ (k^{-1} ist das Inverse von k modulo q)
- Die Signatur ist (r, s)

Verifikation:

- Bob beschafft sich den öffentlichen Schlüssel von Alice und die bekannte Hashfunktion.
- Bob verifiziert, dass $1 \le r \le q-1$ und $1 \le s \le q-1$ gilt.
- Bob verifiziert, dass $r = \left(\left(g^{(s^{-1} \cdot h(x)) \bmod q} \cdot A^{(r \cdot s^{-1}) \bmod q}\right) \bmod p\right) \bmod q$