Vertiefung Rechnertechnik und -netzwerke
Übungsaufgaben – 26. April 2013

Aufgabe 1: RSA-Signatur

Beim RSA-Verschlüsselungsverfahren verwendet man den öffentlichen Schlüssel zum Verschlüsseln einer Nachricht und den geheimen Schlüssel zum Entschlüsseln. Macht man es umgekehrt, ergibt sich das RSA-Signaturverfahren:

- Alice wählt zwei Primzahlen p und q sowie eine weitere Zahl e, die zu p und q teilerfremd ist.
  Das Produkt pq der Primzahlen und die Zahl e sind der öffentliche Schlüssel von Alice.
- Der geheime Schlüssel von Alice ist das multiplikative Inverse d von e modulo $(p-1)(q-1)$:

  $$d = e^{-1} \left(\mathrm{mod}\,(p-1)(q-1)\right)$$

  (Um d aus e zu berechnen, ist die Kenntnis der einzelnen Primzahlen p und q notwendig.
  Insofern kann man auch die Primzahlen p und q als den geheimen Schlüssel bezeichnen.)
- Die Signatur s der Nachricht m ist gegeben durch $s = m^d (\mathrm{mod}\, pq)$.
- Um die Signatur zu überprüfen, berechnet Bob $s^e (\mathrm{mod}\, pq)$.
  Wenn dabei m herauskommt, stammt die Signatur wirklich von Alice.

(a) Demonstrieren Sie das RSA-Signaturverfahren am Beispiel $p = 7$, $q = 11$, $e = 43$, $m = 2$.

(b) Was ist hinsichtlich der Übertragung von pq und e von Alice an Bob zu beachten?
Genügt es insbesondere, wenn Alice diese zusammen mit der Nachricht m und der Signatur s an Bob versendet? Begründen Sie Ihre Antwort.

(c) Da die Berechnung einer RSA-Signatur sehr aufwendig ist, vereinbaren Alice und Bob, bei längeren Nachrichten nicht die Nachricht selbst, sondern ihren CRC-32-Prüfwert zu signieren. Wie wirkt sich dies auf die Fälschungssicherheit der Signatur aus?

Aufgabe 2: E-Mail-Verschlüsselung in der Praxis

Senden Sie eine verschlüsselte E-Mail an `peter.gerwinski@hs-bochum.de`.

Die Aufgabe ist gelöst, sobald Sie eine verschlüsselte Antwort empfangen und entschlüsselt haben.

Aufgabe 3: ElGamal-Verschlüsselung

Dieses Public-Key-Verschlüsselungsverfahren arbeitet ähnlich wie der Diffie-Hellman-Schlüselaustausch. Wie bei allen Public-Key-Verschlüsselungsverfahren gilt:

- Alice erzeugt einen öffentlichen und einen geheimen Schlüssel.
- Bob verwendet den öffentlichen Schlüssel von Alice, um einen Klartext m zu verschlüsseln.
- Alice verwendet ihren geheimen Schlüssel, um den verschlüsselten Text wieder zu entschlüsseln.

Beim ElGamal-Verfahren gilt:

- Alice und Bob einigen sich auf einen gemeinsamen Modulus p und eine gemeinsame Basiszahl g.
- Der geheime Schlüssel von Alice ist eine Zahl a; der zugehörige öffentliche Schlüssel ist $g^a (\mathrm{mod}\, p)$.
- Um eine Nachricht m zu verschlüsseln, wählt Bob eine zufällige Zahl b.
  Zur Verschlüsselung wird m mit $(g^a)^b$ multipliziert (alles mod p).
  Zusätzlich zur verschlüsselten Nachricht überträgt Bob den Wert g^b an Alice.
- Da Alice die Zahl a kennt, kann sie $(g^a)^b = (g^b)^a$ berechnen,
  die verschlüsselte Nachricht dadurch dividieren (alles mod p)
  und auf diese Weise entschlüsseln.

(a) Demonstrieren Sie die ElGamal-Verschlüsselung am Beispiel $p = 17$, $g = 3$, $a = 6$, $m = 9$, $b = 5$.
(Musterlösung: Wikipedia)

(b) Erklären Sie den Zusammenhang mit dem Diffie-Hellman-Schlüsselaustausch.

(c) Warum darf Bob nicht b an Alice übertragen, sondern nur g^b?