Eerste Herdeeltoets Security

Woensdag 19 augustus 2015, 13.30–15.30, BBG169.

Motiveer je antwoorden *kort*! Zet je mobiel uit. Stel geen vragen over deze toets; als je een vraag niet duidelijk vindt, schrijf dan op hoe je de vraag interpreteert en beantwoord de vraag zoals je hem begrijpt.
Cijfer: Maak vraag 1 en 2 op pagina 1, vraag 3 en 4 op pagina 2 en vraag 5 en 6 op pagina 3. Vraag 3 en 5 zijn 3pt, de andere 2pt. Te halen 14pt, cijfer is totaal plus 1 gedeeld door 1,5.

1. **Entropie van Cijferreeks:** Alice stuurt Bob in een ASCII bestand (een Byte per letter) een lange cijferreeks, bestaande uit alleen 0, 1, 2, 3, 4, 5, 6, 7, 8 en 9. Zij versleutelt haar bericht met AES.
   (a) Wat is de entropie van de berichten?
   (b) Wat is de relatie tussen entropie, sleutellengte en kritieke lengte?
   (c) Hoe groot is de kritieke lengte voor deze berichten?
2. **Bescherming van DES:** Je wilt data op een website versleutelen met beschermingsnivo 48 bits; dwz., je wilt dat een CipherText Only aanval minstens 2^{48} stappen werk is.
   (a) Welk van de varianten: DES, 2DES of 3DES kan hier worden gebruikt? Motiveer!
   (b) Welke variant kun je gebruiken voor 96 bits veiligheid?
3. **Stroomversleuteling:** GSM telefonie gebruikt stroomversleuteling.
   (a) Wat is de sleutellengte en hoe heet dit algoritme?
   (b) Welke (drie) voordelen van stroomversleuteling zijn belangrijk bij mobiele telefonie?
   (c) Hoe is berichtmanipulatie mogelijk bij stroomversleuteling?
4. **Diffie-Hellman Key Exchange:** Een Key Exchange protocol zorgt ervoor dat partijen Alice en Bob over dezelfde key k kunnen beschikken, zonder dat een afluisteraar die key ook te weten komt. In het protocol van Diffie en Hellman hebben de partijen elk een *geheim* getal x en een *publiek* getal y.
   (a) Wat is de relatie tussen x en y, en hoe bepalen Alice en Bob k?
   (b) Bewijs dat zij dezelfde waarde vinden.
5. **Precomputation bij Rainbow Table:** Bertus Boef heeft gemerkt dat op Simons Site elke gebruiker een wachtwoord van 10 letters heeft uit `[a-z]`, zoals `jsibepmzii`, waarvan de MD5-hash wordt opgeslagen. Bertus besluit deze tabel te gaan stelen, maar eerst een Rainbow-table te bouwen om de hash te inverteren.
   (a) Hoe ziet een keten van deze tabel eruit?
   (b) Geef een schatting van de hoeveelheid werk om de tabel te bouwen.
   (c) Geef een schatting van de benodigde opslagruimte en van de query-tijd (tijd om een hash te inverteren).
6. **Korte berichten met AES:** Alice en Bob communiceren met heel korte berichten (slechts 3 tot 5 *bits* elk) en willen die versturen met AES; een gedeelde key k hebben ze al. Omdat communicatie duur is, is het niet wenselijk om elk berichtje uit te breiden tot een AES blok. Hoe kunnen Alice en Bob met AES korte berichten uitwisselen zonder de hoeveelheid bits te laten toenemen?