Eerste Herdeeltoets Security

20 augustus 2014, 13.30 – 15.30, BBG001.

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: Vraag 1, 3 en 5 elk 2pt, V2 1pt, V4 3pt.

1. **Kerckhoffs:** (a) Hoe luidt Kerckhoffs' Principe?
   (b) Noem (vijf) redenen om van dit principe uit te gaan.
2. **AES Rondes:** Uit welke vier stappen bestaat een ronde van AES? Hoeveel ronden worden er gebruikt?
3. **Diffie-Hellman key agreement:** In het Diffie-Hellman protocol heeft elke partij een private (x) en een publieke (y) sleutel.
   (a) Welke relatie geldt tussen deze twee getallen?
   (b) Beschrijf hoe Alice en Bob een symmetrische sleutel kunnen overeenkomen.
4. **3DES en AES:** Hoewel 3DES niet direct onveilig was, is DES/3DES vervangen door AES.
   (a) Wat zijn de sleutellengtes van DES, 3DES en AES?
   (b) Hoewel 3DES een vrij langere sleutel heeft, bestaat er een KPA tegen 3DES met een complexiteit van 2^{112}. Beschrijf (kort) deze aanval.
   (c) Wat is het geheugengebruik van die aanval, en is deze in de praktijk een probleem voor 3DES?
5. **Rainbow Table:** De OV-chip gebruikt(e) een sleuteltje van 48 bits, waarmee het systeem kwetsbaar bleek tegen een aanval met Rainbow Tables.

   Geef een schatting van de hoeveelheid opslagruimte die nodig is voor een dergelijke aanval op de OV-chip.