Eerste Hertoets Security

21 dec 2015, 11.00–13.00, Ruppert-116.

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: Vragen 1, 4 en 5 zijn 3pt elk en vragen 2 en 3 zijn 2pt. Resultaat T1 is totaal plus 1,1 gedeeld door 1,3.

1. **Perfecte Verhulling en One-Time Pad:** (a) Wanneer noemen we een cryptosysteem *perfect verhullend*?
   (b) Bewijs dat het One Time Pad perfect verhullend is.
   (c) Waarom wordt het One Time Pad niet meer gebruikt (twee redenen)?

2. **Symmetrische en asymmetrische cryptografie:** Wat is het verschil tussen *symmetrische* en *asymmetrische* cryptografie? Noem van beide vormen (twee) voorbeelden.

3. **Zwakte van DES en 3DES:** Tegen de veiligheid van DES zijn meerdere bedenkingen ingebracht nl.: (I) Door de korte sleutel is de kritieke lengte te laag; (II) DES is kwetsbaar tegen differentiële analyse; (III) De NSA heeft mogelijk een achterdeurtje ingebouwd; (IV) Door de korte sleutel is DES kwetsbaar tegen een BFA.
   (a) Zeg van elk hoe relevant ze zijn (1 zin per bedenking).
   (b) Wat is de sleutellengte van 3DES en welk van de bezwaren geldt voor 3DES?

4. **Hash met Verlenger:** Op Willems Wonder Web moet je wachtwoord minstens zes letters zijn. Willem slaat de wachtwoorden niet plain op, als `[login, ww]` omdat hij beseft dat hackers het wachtwoordbestand kunnen stelen met SQL-injecties. En ook niet de combinatie `[login, SHA1(wachtw)]` omdat hij weet dat zesletterige wachtwoorden met Rainbow Tables te ont-hashen zijn.
   (a) Willems eerste idee is, de hash te *salten*. Hoe werkt dit, en waarom beschermt het Willems klanten onvoldoende?
   (b) Willem kiest een random, geheime verlengstring `vs` van lengte 6 en slaat gebruikersinfo op als `[login, SHA1(ww+vs)]`. Een aanvaller die dit bestand steelt, moet SHA1 terugrekenen voor strings van (minstens) 12 lang, wat teveel werk is. Simon de Schurk weet inderdaad een truuk om de wachtwoordlijst te stelen, en strings van 12 terughalen uit een hash kan hij inderdaad niet. Help Simon om de wachtwoorden van Willems Web te stelen.

5. **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.
   (c) Hoe groot moeten de gebruikte getallen zijn?