Tweede Toets Security

2 november 2015, 8.30–10.30, Educ-α.

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 de vragen 1, 2 en 3 op de eerste bladzijde, vragen 4, 5 en 6 op de tweede bladzijde, vragen 7 en 8 op de derde bladzijde. Vragen 1, 2, 5 en 8 zijn 2pt, vraag 3 is 1pt, vragen 4, 6 en 7 zijn 3pt. Te halen 18pt, T2 is totaal plus 1 gedeeld door 1,8.

1. **ϕ:** Geef de definitie van $\phi(m)$. Hoeveel is $\phi(77)$? Hoeveel is $\phi(2^t)$?

2. **Inverse:** Wat is de inverse van 203 modulo 1004?

3. **Authenticatie tegen Meaconing:** Een land dat werd bespioneerd door een Amerikaanse drone kon deze verkeerd laten vliegen door valse GPS-signalen te spoofen (Meaconing). Waarom is het niet mogelijk om GPS signalen betrouwbaar te authenticeren met een HMAC (Hashed Message Authentication Code)?

4. **Existential Forgery:** Als een aanvaller een digitaal bericht met geldige handtekening produceert, spreken we van een *vervalsing* of *forgery*. We onderscheiden *existential* en *universal* forgery.
   (a) Waarom wordt een existential forgery doorgaans niet als groot probleem beschouwd?
   (b) Hoe kun je *hashing* gebruiken om existential forgery onmogelijk te maken?
   (c) Laat zien hoe een existential forgery wordt gedaan voor RSA handtekeningen.

5. **Certificaten:** Wat zijn de belangrijkste componenten van een sleutelcertificaat? Wat zijn de belangrijkste problemen van de certificaat-gebaseerde PKI?

6. **Blinde RSA decryptie:** Iemand heeft Bob een bericht y gestuurd, per ongeluk gecrypt met de public RSA key van Alice. Er geldt dus $y = x^e \pmod m$, berekend met de public key van Alice, en Bob wil x weten. Alice stemt erin toe, het bericht *ongezien* voor Bob te decrypten. Daarom bedenkt Bob een random getal b en geeft hij aan Alice een getal $y' = y.b$ ter decryptie.
   (a) Hoe berekent Alice de decryptie x' van een RSA-bericht?
   (b) Bob kan uit x' de juiste decryptie van y berekenen, mits hij over b^d beschikt. Hoe?
   (c) Hoe komt Bob, zonder d te kennen, aan het getal b^d?

7. **Zero Knowledge met Schnorr:** Bij het protocol van Schnorr heeft Bob een publiek getal b. Alice toont door een Commit/Challenge/Respons aan, over getal a te beschikken waarvoor $b = g^a$ geldt. De *Commit* van Alice is een getal $s = g^r$ (random r), Bobs *Challenge* is een random c, en Alice' *Respons* is $y = r + a.c$ (wat voldoet aan $g^y = s.b^c$).
   (a) Kan een aanvaller, of Bob zelf, bij b een getal a berekenen met $g^a = b$?
   (b) Waarom is het van belang dat Bob de Commit ziet *voordat* hij een Challenge geeft?
   (c) Bob wil extra zekerheid, en verlangt van Alice dat zij, na het geven van s, antwoord geeft op *twee* challenges c_1 en c_2. Is het protocol dan veiliger of minder veilig?

8. **Versnelling met CRT:** Meestal zijn de p en q, factoren van de modulus bij RSA, ongeveer even lang (half zo lang als de modulus). Je collega wil een p gebruiken die tweemaal zo lang is als de q. Welke speedup is dan te verwachten van de Chinese Reststelling bij decryptie? En welke speedup bij encryptie?