Tweede 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: Vraag 3 is 2pt, vraag 5 is 1pt, de andere elk 3pt. Maar vragen 1 en 2 op pagina 1, vragen 3 en 4 op pagina 2 en vragen 5 en 6 op pagina 3. Bonusvraag 7 voor 1pt achterop. T2 wordt totaal gedeeld door 1,5.

1. **Lagrange:** Piet moet 13^{1027} uitrekenen in $\mathbb{Z}_{1536}$ maar hij is lui en wil zich rekenwerk besparen door de Stelling van Lagrange te gebruiken. (NB: $1536 = 2^9 \cdot 3$.)
   (a) Hoe luidt de Stelling van Lagrange?
   (b) Hoeveel is $\phi(1536)$?
   (c) Geef 13^{1027} mod 1536.
2. **RSA Exponenten:** Het RSA algoritme gebruikt, behalve een modulus m, een encryptie-exponent e en een decryptie-exponent d.
   (a) Welke relatie geldt tussen e en d?
   (b) Hoe wordt de e bepaald?
   (c) Is bij RSA de encryptie of de decryptie sneller? Hoeveel keer zo snel?
3. **Elgamal kosten:** Hoe luiden de encryptie en decryptieformules van Elgamal? Is de Elgamal private functie duurder of goedkoper dan de publieke, en wat is de kostenverhouding?
4. **RSA met Hashing:** Voor de ondertekening van berichten wordt meestal SHA2RSA gebruikt, dwz., RSA signing in combinatie met (SHA2) hashes.
   (a) Beschrijf de controle van een ontvangen bericht M met signature S.
   (b) Noem (minstens twee) voordelen van het hashen (ten opzichte van pure RSA signatures).
   (c) Boris Boef wil een bestaande app in Google Play vervangen door zijn spyware, maar zo, dat de signature op de app geldig blijft. Welke eigenschap van de hashfunctie moet dit voorkomen?
5. **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)?
6. **Blinde Logaritme:** De NSA heeft een kolossale machine gebouwd waarmee ze, voor een bepaalde publieke modulus p en generator g, de discrete logaritme kunnen berekenen. Om hun ontwikkelkosten terug te verdienen, bieden ze de service commercieel aan: als je ze een $y \in \mathbb{Z}_p^*$ stuurt en een Bitcoin, krijg je een $x < p-1$ waarvoor geldt $g^x = y$. Simon heeft wel een Bc over voor de log van zeker getal y, maar hij wil niet dat de NSA weet in welk getal hij geïnteresseerd is.
   (a) Simon kiest een random $b \in \mathbb{Z}_p^*$ en stuurt $y' = y.b$ naar de NSA. Welke informatie geeft dit de NSA over y?
   (b) Simon vreest dat de NSA hem bedriegt en een fout antwoord stuurt. Wat kan Simon doen om zekerheid te krijgen over de juistheid van het gekochte getal?
   (c) Hoe kan Simon uit het gekochte antwoord de log van y berekenen?
7. **Eindejaarsvraag:** Vooruit, nu het nog net kan: hoeveel is $\phi(2015)$?