Tweede Deeltoets Security

3 juli 2015, 8.30–10.30, Educatorium-Γ.

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. Vragen 2 en 4 zijn 3pt, de andere elk 2pt. Maak vraag 1 en 2 op pagina 1, 3 en 4 op pagina 2 en 5 en 6 op pagina 3.

1. **Euclides:** Bereken met het algoritme van Euclides de waarde van $d = \text{ggd}(1230, 504)$. Laat alle tussenresultaten zien. Bereken x en y waarvoor geldt dat $d = 1230x + 504y$.

2. **Code Signing:** Martin wil een malafide, creditcardstelende app MM in de iPad Appstore plaatsen. Helaas voor Martin worden alle apps eerst door Apple bekeken, en alleen apps die *geen* creditcards stelen worden ondertekend (met een Hash plus RSA mechanisme). De controle op de inhoud van de apps is vrij goed, en de RSA handtekening van Apple kan Martin niet namaken. Martin probeert een goedgekeurde, bonafide app BB te vervangen door MM, maar zo dat de signature onder BB nu geldig is voor MM.

   (a) Eerst probeert Martin, zelf een goeie app BB te maken naast zijn eigen MM. Welke eigenschap van de gebruikte hashfunctie zal moeten voorkomen dat Martin slaagt? Leg uit.
   (b) Martin probeert, een reeds bestaande veelgebruikte app BB te vervangen door MM. Welke eigenschap van de gebruikte hashfunctie zal moeten voorkomen dat Martin slaagt? Leg uit.
   (c) Schat hoeveel werk de aanvallen in (a) en (b) zijn, als Apple een hashwaarde van 192 bits gebruikt.

3. **RSA Encryptie versus Decryptie:** Kees gaat RSA gebruiken met een sleutellengte van 3072 bits. Om de *encryptietijd* laag te houden, besluit hij de waarde $e = 17$ te nemen. Geef een schatting van de verhouding tussen encryptie- en decryptietijd.

4. **Wortel Funding:** Instant Root Incorporated (Inst Inc) ontwikkelt een app voor modulair worteltrekken. Na invoer van een modulus m (max. 3072bits) en een getal $b < m$, produceert de InstInc app een getal a (als dat bestaat) dat voldoet aan $a^2 = b \pmod{m}$. De nodige 500.000 euro wil InstInc met crowd funding bij elkaar brengen.

   (a) Laat zien hoe je door deze app slim te gebruiken, de factoren van m kunt vinden.
   (b) Denk je dat Inst Inc de investering kan terugverdienen?
   (c) Bij nadere lezing van het persbericht zie je, dat de nieuwe app alleen zal werken als m een priemgetal is. Denk je nu dat Inst Inc de investering kan terugverdienen?

5. **Elgamal rekentijd:** Voor Elgamal encryptie worden gedeelde parameters, een modulus en een generator g gebruikt. De private key is een getal a en de public key is $b = g^a$. Je hoort geruchten dat bij Elgamal, de *encryptie* tweemaal zo duur is als de *decryptie*, maar dat je de berekening kunt versnellen door een Chinese stelling te gebruiken.

   (a) Klopt het dat encryptie zoveel duurder is, en waarom?
   (b) Hoeveel kun je de berekening versnellen met die Chinese stelling?

6. **Een Kraak bij SecuCert:** Chinese hackers hebben ingebroken bij Certificate Authority SecuCert en de geheime signing key gestolen, waardoor zij valse SecuCert-websitecertificaten kunnen uitgeven. Lia weet dat `gmail.com` niet beveiligd is met een SecuCert-certificaat, maar met een GeoTrust-certificaat. Kan Lia veilig naar `gmail.com` gaan, en welke maatregelen moet zij eventueel nemen?