Tweede Herdeeltoets Security

Woensdag 19 augustus 2015, 13.30–15.30, BBG169.

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 en 7 zijn 3pt, de andere vragen elk 2pt. Te halen 16pt, cijfer is totaal gedeeld door 1.5. Maak vraag 1 en 2 op pagina 1, vragen 3, 4 en 5 op pagina 2, en vragen 6 en 7 op pagina 3.

1. **Elgamal is Multiplicatief:** Het Elgamal encryptiesysteem gebruikt een modulus p, generator g, en een orde q. De ElGamal-encryptie van x is het paar $(u, v) = (g^k, b^k.x)$.
   (a) Welke relatie geldt tussen p, g, en q en welke tussen de secret key a en de public b?
   (b) Bob stuurt Alice een bericht x, versleuteld met Elgamal. Met welke formule ontsleutelt Alice dit?
   (c) Schurk Oscar kan aan het bericht niet de x aflezen, maar wenst dat Alice bij ontsleuteling een f maal zo grote waarde leest als Bob heeft verstuurd. Hij vervangt het bericht (u, v) door $(u \cdot u_f, v \cdot v_f)$, waar (u_f, v_f) een encryptie van f is. Slaagt Oscar in zijn opzet?

2. **RSA met kleine d:** Decryptie bij RSA is gebaseerd op de regel $x^{\phi(m)} = 1 \pmod m$. Iemand beweert dat je een kleinere decryptie-exponent kunt vinden als je gebruikt dat $x^{\lambda(m)} = 1 \pmod m$, waar $\lambda(m) = kgv(p-1, q-1)$, het kleinste gemeenschappelijke veelvoud van $p-1$ en $q-1$.
   (a) Bewijs dat $x^{\lambda(m)} = 1 \pmod m$.
   (b) Is $\lambda(m)$ inderdaad kleiner dan $\phi(m)$?

3. **RSA Handtekening met Certificaat:** Alice ontvangt een bestand F, met een SHA1/RSA-handtekening S en een PKI-certificaat, van Bob. Beschrijf kort de stappen die Alice doet om de geldigheid van F te controleren.

4. **Extended Euclides:** Schrijf 3 als som van een 93-voud en een 129-voud. Laat de stappen van Euclides' Algoritme zien.

5. **$\phi(p^3)$:** In deze vraag is p een oneven priemgetal. Hoeveel is $\phi(p^3)$?

6. **RSA sleutellengte:** Je collega wil RSA gebruiken met een p van 850 bits lang, een q van 750 bits, een e van 600 bits, en zijn berekening voor d geeft een getal van 1600 bits. Voldoet zijn sleutel aan de recentste NIST aanbevelingen? Leg uit.

7. **Zero Knowlegde Wortel:** Alice wil tegenover Bob bewijzen dat zij een wortel a bezit van een publiek getal b in $\mathbb{Z}_m$. Als eerste stuurt Alice het kwadraat s van een random getal r. Dan stuurt Bob een random bit c, en als c is 0, moet Alice een wortel van s sturen.
   (a) Hoe heten de drie eisen waar een Zero Knowledge Protocol aan moet voldoen? Welk getal moet Alice sturen als c is 1?
   (b) Waarom moeten Alice en Bob dit meerdere keren doen, en hoeveel keer is nodig om de bedrieg-kans van Alice kleiner dan 1 op 10000 te maken?
   (c) Alice weet dat Bob een slechte Random Number Generator gebruikt en zij kan vooraf berekenen, wat de i^{de} random bit van Bob zal zijn. Hoe kan zij dit gebruiken om Bob te bedriegen?