Tweede Deeltoets Security

Vrijdag 5 juli 2013, 8.30 – 10.30, Educ-β.

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. Te behalen 19 punten, cijfer is (totaal plus 1) gedeeld door 2.

1. **Kwadraat met twee wortels:** Hier is $n = p \cdot q$ het product van twee grote priemgetallen. Veel getallen $b \in \mathbb{Z}_n$ zijn geen kwadraat (voor geen a geldt $a^2 = b$) en flink wat getallen zijn op vier manieren een kwadraat (er zijn precies *vier* verschillende a waarvoor $a^2 = b$). Er zijn ook getallen die precies *twee* wortels hebben.
   (a) Leg met de Chinese RestStelling uit hoe een getal twee wortels kan hebben.
   (b) Geef zo'n b voor het geval $n = 29 \cdot 37 = 1073$.

2. **Derdemachten:** In deze vraag moet je bewijzen dat $\mathbb{Z}_m^*$ gesloten is onder het nemen van derdemachten. Geef de definitie van $\mathbb{Z}_m^*$ en bewijs dat als $a \in \mathbb{Z}_m^*$, dan $a^3 \in \mathbb{Z}_m^*$.

3. **RSA is multiplicatief:** Bewijs dat: als je x_1 en x_2 versleutelt tot y_1 en y_2 met een RSA public key, en het *product* $y = y_1.y_2$ ontsleutelt met de bijbehorende private key, is het resultaat $x_1.x_2$.

4. **RSA Message Attack:** Oscar weet dat Alice honderdtachtig berichten M_1 t/m M_{180} heeft opgesteld, en er eentje aan Bob heeft gestuurd, versleuteld met RSA: $y = Enc_n(M_i)$.
   (a) Oscar beschikt over y en de publieke sleutel van Bob; kan hij bepalen welk van de berichten werd verstuurd?
   (b) Beschrijf (elk in één zin) twee manieren om RSA te beveiligen tegen deze message attacks.

5. **Elgamal kosten:** Bij RSA is de publieke functie veel goedkoper dan de private, maar bij Elgamal is dan niet zo. Hoe luiden de encryptie en decryptieformules van Elgamal? Is de Elgamal private functie duurder of goedkoper dan de publieke, en wat is de kostenverhouding?

6. **RSA Signature:** Behalve voor versleuteling, kun je RSA ook gebruiken om een handtekening te zetten.
   (a) Waaruit bestaat een RSA key pair, en hoe luidt de sleutelgeneratie procedure?
   (b) Hoe wordt de RSA handtekening berekend (functie *Sig*) en geverifieerd (functie *Ver*)?

7. **Zero Knowledge met Quisquater:** Voor het identificatieprotocol van Quisquater gebruiken Alice en Bob alleen een *publieke* RSA-sleutel (n, e). De publieke informatie bij Alice is een getal $b \in \mathbb{Z}_n^*$, en haar geheim is een getal a waarvoor $a^e = b$. De *Commit* van Alice is een getal $s = r^e$, Bobs *Challenge* is een random $c < e$, en Alice' *Respons* is $y = r.a^c$.
   (a) Welke *Check* doet Bob op het antwoord van Alice?
   (b) Waarom is het van belang dat Bob de Commit ziet *voordat* hij een Challenge geeft?
   (c) Bob vraagt extra zekerheid, en verlangt van Alice dat zij antwoord geeft op *twee* challenges c_1 en c_2. Is het protocol dan veilig?

8. **DNS: Middle Man:** Je netwerk adapter bevat het IP-adres van de DNS resolver.
   (a) Is hiermee een spoofing attack op je computer uitgesloten?
   (b) Welke bescherming biedt DNSSEC tegen zo'n aanval?

9. **Bell-LaPadula:** Waarom kent het Bell-LaPadula model, behalve **no read-up**, ook een **no write-down** regel?

10. **Bitcoin Mining vergoeding:** Hoe kunnen miners bitcoins verdienen? Waarom wordt de transactievergoeding in verhouding steeds belangrijker?