Tweede Herdeeltoets Security

20 augustus 2014, 13.30 – 15.30, BBG001.

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, 2, 4 en 6 elk 2pt, 3 en 5 elk 3pt, 7 1pt; eind is totaal/1,4.

1. **Eulers ϕ:** Wat is de waarde van $\phi(4^k)$?
2. **Hash bij Handtekening:** Noem twee redenen om hashing te gebruiken bij RSA Signatures. Geef de *Sign* methode voor RSA signatures met hash.
3. **Wortels en Factoren:** Om het getal $n = 17741$ te factoriseren zoekt Marjan twee getallen met hetzelfde kwadraat mod n.

   (a) Na enig zoeken ontdekt Marjan dat (in $\mathbb{Z}_{17741}$) geldt $1000^2 = 6504$ en $16741^2 = 6504$. Kan zij hiermee de factoren van n vinden? Zo ja hoe, en wat zijn ze, zo nee waarom niet?
   (b) Marjan ontdekt (na nog meer zoeken) dat ook $8379^2 = 6504$. Kan zij hiermee de factoren van n vinden? Zo ja hoe, en wat zijn ze, zo nee waarom niet?
4. **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 $x_1.x_2$.
5. **Elgamal encryptie:** 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?
   (b) Welke relatie geldt tussen de secret key a en de bijbehorende public key b?
   (c) Bob stuurt Alice een bericht x, versleuteld met Elgamal. Schurk Oscar vervangt het bericht (u, v) door (u^2, v^2). Bewijs dat na ontsleuteling, Alice het bericht $x' = x^2$ leest.
6. **Certificaten:** Wat zijn de belangrijkste componenten van een sleutelcertificaat? Wat zijn de belangrijkste problemen van de certificaat-gebaseerde PKI?
7. **Pentest fasen:** Bij penetration tests worden drie fasen onderscheiden. Wat is het doel van *Reconnaissance*, wat is de rol van *payload* in de *Exploit* fase, en hoe heet de tweede fase?