Tweede Deeltoets Security

2 juli 2014, 17.00–19.00, Educ-α.

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:** Totaal te verdienen 21pt, cijfer is totaal gedeeld door 2.

1. $\mathbb{Z}_{21}^*$**:** Hoeveel is $\phi(21)$ en welke getallen zitten in $\mathbb{Z}_{21}^*$?

2. **Wortels van 1 modulo 299:** (a) Schrijf 1 als som van een 13-voud en een 23-voud.
   (b) Welke vier getallen in $\mathbb{Z}_{299}$ hebben kwadraat 1?

3. **Worteltrekken modulo priemgetal:** In deze opdracht is p een priemgetal met $p+1$ een viervoud (zoals 7, 11 of 23, maar *niet* 17 of 29). Als je (a) niet kunt bewijzen, mag je het toch gebruiken in (b).

   (a) Bewijs dat *als* $y \in \mathbb{Z}_p^*$ een kwadraat is, dan is $y^{\frac{p-1}{2}} = 1$.

   (b) Laat zien dat je, van een kwadraat y, een wortel kunt vinden als $x = y^{\frac{p+1}{4}}$.
   (c) Hoeveel tijd kost worteltrekken modulo een priemgetal van k bits?

4. **Elgamal samenwerking:** Bert en Ernie gebruiken beide Elgamal voor het ontvangen van berichten. Ze gebruiken algemeen bekende, gedeelde parameters g en p, hebben private sleutels a_1 resp. a_2, en publieke sleutels b_1 resp. b_2.

   (a) Om een bericht x aan Bert te sturen, kiest Aart een random k en stuurt $(g^k,\ x.b_1^k)$. Hoe ontsleutelt Bert de boodschap?
   (b) Aart vermenigvuldigt de twee publieke sleutels: $b = b_1.b_2$ en versleutelt een bericht m met sleutel b. Welke waarde moet als bijpassende geheime sleutel worden gebruikt?
   (c) Aart versleutelt een bericht met de nieuwe sleutel b. Laat zien hoe Ernie en Bert kunnen samenwerken om het bericht te ontsleutelen, zonder hun geheime sleutel aan iemand te geven.

5. **RSA Plaintext verdubbeling:** Alice heeft een public RSA key $(m,\ e)$ gepubliceerd en Bob heeft haar een bericht x gestuurd, versleuteld als ciphertext y. Oscar kent x niet, maar wil Alice sowieso een bericht sturen met daarin het *dubbele* van wat Bob stuurt.

   (a) Hoe wordt de waarde y berekend uit x en hoe kan Alice de waarde van x berekenen uit y?
   (b) Beschrijf hoe Oscar, zonder de waarde van x te kennen, een bericht aan Alice kan sturen dat zal ontsleutelen naar de waarde $2x$.

6. **Hashfuncties:** Hashfuncties (ook wel fingerprints genaamd) worden gebruikt bij het maken van een digitale handtekening.

   (a) Wanneer is een hashfunctie *one-way*, wanneer *zwak botsingsvrij* en wanneer *sterk botsingsvrij*?
   (b) Hoe werkt de verjaardagsaanval en welke eigenschap van de hashfunctie beschermt ertegen?

7. **NIST over RSA:** Het *National Institute of Standards and Technology* heeft per januari 2012 de aanbevolen sleutellengte van RSA verhoogd.

   Wat is de nieuwe sleutellengte? Wat is je oordeel over de veiligheid van de oude sleutellengte?

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

9. **Password Antipattern:** Wat is het Password Antipattern? Waarom is het onwenselijk, en hoe is het te voorkomen?

10. **Heartbleed Bug:** Is de Heartbleed Bug een fout in het SSL Protocol of in de implementatie? Welke test had deze bug kunnen voorkomen?