Tweede Toets Security

9 november 2016, 8.30 – 10.30, 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. **Punten:** Vraag 1 en 6 zijn is 2pt, de andere 3pt.
Pagina's: Maak vraag 1 en 2 op pagina 1, vraag 3 en 4 op pagina 2, en vraag 5 en 6 op pagina 3.

1. **Gegeven fractie als ϕ:** Noem vijf getallen m waarvoor geldt $\phi(m) = \frac{1}{2}m$.
   Noem vijf getallen m waarvoor geldt $\phi(m) = \frac{1}{3}m$.

2. **Signature en Hash:** Een veelgebruikte manier om berichten te ondertekenen is SHA2RSA, wat wil zeggen dat van het bericht eerst een SHA2 hash wordt berekend, en dat die hash wordt gesigned met RSA. Oscar wil Alice's handtekening vervalsen onder bericht M, door eerst een *existentiële vervalsing* (F, S) te produceren, en dan M zo te veranderen dat SHA2(M) $= F$.
   (a) Is het mogelijk een existentiële vervalsing te maken? Zoja hoe, zonee waarom niet?
   (b) Is het mogelijk om M zo te veranderen dat de hash F is? Zoja hoe, zonee waarom niet?
   (c) Is voor SHA2RSA het Signen of het Verifiëren het duurst? Maakt het hierbij verschil of het bericht lang of kort is? Leg uit.

3. **RSA Rekentijd:** Leo gebruikt RSA software op zijn PC, heeft een public key van 2048 bits en gebruikt de standaardwaarde $e = 65537$.
   (a) Leo doet wat metingen aan de encryptie en ziet dat een *RSA encryptie* hem ongeveer 4,3ms (dus 0,0043 seconde) kost. Geef een schatting van de tijd voor een RSA *decryptie*.
   (b) Leo is bang dat, bij een heel kleine input x, de encryptie berekend wordt *zonder dat daadwerkelijk reducties plaatsvinden*. Dan zou x heel makkelijk uit y terug te rekenen zijn. Kun je Leo geruststellen?
   (c) Tot hoeveel milliseconde kun je encryptie en decryptie versnellen door gebruik van de CRT?

4. **Getalberekeningen:** (a) Bereken met Euclides de grootste gemene deler van 2358 en 1599; laat de tussenstappen zien.
   (b) Modulo 17741 hebben 1000 en 8379 hetzelfde kwadraat. Wat is dat kwadraat? Laat zien hoe je hieruit met een polynomiale berekening de factoren van 17741 kunt vinden.
   (c) Hoeveel vermenigvuldigingen kost het om a^{213} te berekenen?

5. **Elgamal Kopie maken:** Alice gebruikt voor het ontvangen van berichten een Elgamal key-pair waarvan het publieke getal b (en modulus p en generator g) op haar website staat.
   (a) Bob wil Alice getal x sturen; beschrijf de encryptie en het codebericht.
   (b) Oscar ziet het bericht Y dat Bob aan Alice stuurt en wil, zonder dat hij x kent, Alice ook bericht x sturen. Maar Alice filtert haar berichten op herhalingen van de ciphertekst, dus zelf Y ook sturen kan Oscar niet. Beschrijf hoe Oscar een bericht Y' kan berekenen dat verschilt van Y, maar dezelfde waarde oplevert bij decryptie.
   (c) Zijn de Elgamal-berekeningen duurder of goedkoper dan de berekeningen van het RSA-systeem?

6. **Zero Knowledge Wortel:** Alice wil tegenover Bob bewijzen dat zij een wortel a kent van een publiek getal b in $\mathbb{Z}_m$. Als eerste stuurt Alice een getal s. Dan stuurt Bob een random bit c, en als c is 0, moet Alice een wortel van s sturen.
   (a) Hoe kent Alice de wortel van s? Welk getal moet Alice sturen als c is 1?
   (b) Door een virus in Alice' computer kan Bob de Random Number Generator beïnvloeden. Kan Bob hierdoor het geheime getal a achterhalen? Leg uit.