# Tweede Toets Security

Woensdag 8 november 2017, 8.30 – 10.30, Educ-$\alpha$.

Motiveer je antwoorden *kort*! 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 5 is 2pt en de andere vragen elk 3pt. Maak vraag 1 en 2 op pagina 1, vraag 3 op p2, en vragen 4 en 5 op pagina 3.

1. **Is $\mathbb{Z}_m^*$ gesloten:** (a) Bewijs dat de verzameling $\mathbb{Z}_m^*$ gesloten is onder vermenigvuldiging. (Dat betekent: als $a \in \mathbb{Z}_m^*$ en $b \in \mathbb{Z}_m^*$, dan $a.b \in \mathbb{Z}_m^*$.)
   (b) Geef een concreet voorbeeld dat aantoont dat $\mathbb{Z}_m^*$ *niet* gesloten is onder optelling.

2. **Terug uit Subgroepen:** Reken in deze opdracht in $\mathbb{Z}_{221}$. De modulus 221 is 13 maal 17. Voor $a = 6$ is $a^2 = 36$.

   (a) Waaraan moeten de getallen $W_{13}$ en $W_{17}$ voldoen die je gebruikt om bij de CRT terug te rekeken uit de subgroepen naar de hoofdgroep?
   (b) Geef $W_{13}$ en $W_{17}$ en laat zien hoe je ze vindt.
   (c) Geef de andere drie wortels van 36, en laat zien hoe je ze vindt.

3. **RSA BerichtRange:** Alice gaat Bob een getal $x$ sturen, versleuteld met RSA. Oscar weet al dat $1000000 \leq x < 1000100$ en hij kent Bobs public key.

   (a) Leg uit hoe Oscar, na de ciphertext $y$ te onderscheppen, $x$ kan vinden.
   (b) Schat de hoeveelheid rekenwerk voor Oscar, in vergelijking met de decryptietijd voor Bob.
   (c) Hoe kunnen Alice en Bob zich beter beschermen tegen aanvallen als van de plaintext bekend is dat deze uit een vrij kleine verzameling komt?

4. **Signature en Hashing:** Een veelgebruikte manier om berichten te ondertekenen is SHA2RSA, wat wil zeggen dat van het bericht $M$ eerst een SHA2 hash $F$ wordt berekend, en dat die hash wordt gesigned met RSA.

   (a) Is voor SHA2RSA het Signen of het Verifiëren het duurst? Maakt het hierbij verschil of het bericht lang of kort is? Leg uit.
   (b) Kan de rekentijd voor Signen of Verifiëren worden verkort door het gebruik van de CRT? Leg uit.
   (c) De rekentijd voor Verifiëren kan worden beperkt door met het bericht, behalve $S$ ook $F$ mee te sturen. De hash hoeft dan bij verificatie niet te worden herberekend. Welke aanval is in dit aangepaste systeem mogelijk?

5. **Botnets en Cyberaanvallen:** (a) Wat is een Botnet?
   (b) Welke legale Botnets ken je?
   (c) Welke (vijf) landen hebben de grootste capaciteit voor cyber-aanvallen en wat zijn hun belangrijkste doelen?