DIT TENTAMEN IS IN ELEKTRONISCHE VORM BESCHIKBAAR GEMAAKT DOOR DE $\mathcal{TBC}$ VAN A–ESKWADRAAT. A–ESKWADRAAT KAN NIET AANSPRAKELIJK WORDEN GESTELD VOOR DE GEVOLGEN VAN EVENTUELE FOUTEN IN DIT TENTAMEN.

Tweede deeltoets Security

4 juli 2012, 13.30–15.30, 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.
Weging: vragen 1,2,3: elk 20%, vragen 4,5: elk 10%, vragen 6,7,8,9 elk 5%.

1. **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, zo nee waarom niet?
   (b) Marjan ontdekt (na nog meer zoeken) dat $8379^2 = 6504$. Kan zij hiermee de factoren van n vinden? Zo ja hoe, zo nee waarom niet?

2. **RSA Encryptie en Decryptietijd:** Het aanroepen van de *private* functie (decryptie) in RSA is veel duurder dan de *public* functie (encryptie).
   (a) Waarom is dit zo?
   (b) Geef een nauwkeurige schatting van de verhouding van decryptie- versus encryptietijd, zowel voor 1024-bits als voor 2048-bits keys.

3. **Zero Knowledge Logaritme:** Voor het identificatieprotocol van Schnorr heeft Alice een geheim getal a en een publiek getal $b = g^a$. De *Commit* van Alice is een getal $s = g^r$, Bobs *Challenge* is een random c, 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 nog veilig?

4. **Eulers ϕ:** Wat is de waarde van $\phi(3^k)$?

5. **DNS: Correctheid en Privacy:** Als je DNS gebruikt, loop je een risico op het terugkrijgen van foutieve IP-nummers en het risico dat je surfgedrag wordt gemonitord.
   (a) Welk van deze risico's wordt/worden ondervangen door DNSsec en hoe?
   (b) Welk van deze risico's wordt/worden ondervangen door server-certificaten en hoe?

6. **Delayed Ban:** Waarom worden cheaters in games soms pas na enkele weken gestraft? Wat is het probleem van deze *delayed ban* ten opzichte van de *direct ban*?

7. **Cribs:** Wat is in de klassieke cryptanalyse een *crib*? Hoe verkreeg men een crib? Zijn cribs relevant voor aanvallen op 3DES of AES?

8. **Plausible Deniability:** Wat wordt bedoeld met de *Plausible Deniability* feature van TrueCrypt? Voor wie is deze feature handig, en voor wie is deze een probleem?

9. **Hacker's Hat:** Waarin onderscheidt zich een *black hat hacker* van een *white hat hacker*? Waarin onderscheiden hackers zich van script kiddies?