Eerste Deeltoets Security

7 oktober 2015, 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. Vragen 1 en 3 zijn 2pt, de andere vragen 3pt. Maak vragen 1 en 2 op pagina 1, vragen 3 en 4 op pagina 2, en vragen 5 en 6 op pagina 3.

1. **Sleutels:** (a) Als Alice een bericht stuurt aan Bob, versleuteld met public-key cryptografie, gebruikt Bob bij ontvangst: (i) Alice' publieke sleutel, (ii) Alice' geheime sleutel, (iii) Bobs (eigen) geheime sleutel, of (iv) Bobs publieke sleutel?
   (b) Een groep van 12 personen wil elkaar versleutelde berichten sturen, waarbij berichten alleen gelezen kunnen worden door de zender en ontvanger. Hoeveel sleutels zijn nodig als zij hiervoor symmetrische enctryptie gebruiken?
   (c) Hoeveel sleutels zijn nodig als deze 12 personen asymmetrische encryptie gebruiken?

2. **Kritieke lengte:** Alice stuurt Bob ASCII-bestanden, versleuteld met AES. Oscar weet dat Alice altijd alleen maar hoofdletters, punt, komma, spatie, backspace, newline en uitroepteken gebruikt.
   (a) Wat is de entropie van deze soort bestanden?
   (b) Bij welke lengte van het bestand is er maar 1 sleutel waarmee decryptie een correct bestand oplevert?
   (c) Moeten Alice en Bob aanvullende security-maatregelen nemen voor zulke berichten?

3. **De DES Miner:** Je koopt een Bitcoin Miner van 2TH (TeraHash per seconde) en herprogrammeert deze om DES decrypties uit te voeren. Het rekenwerk van een decryptie blijkt ongeveer evenveel te zijn als de hashes waar de machine voor verkocht werd.
   (a) Hoeveel tijd kost het je om een gegeven cipher-block te decrypten met alle DES sleutels?
   (b) Door het beluisteren van Wifi-verkeer hoor je een text X en een antwoord Y, beide 32 Byte lang, waarbij $Y = DES_k(X)$. Hoe snel kan jouw machine k vinden?

4. **Rekenen in AES:** In AES wordt gerekend in het Finite Field $F = \mathbb{Z}_2[X]/X^8 + X^4 + X^3 + X + 1$. Neem A = 00110001 (binaire notatie) en B = 0x1A (hexadecimale notatie).
   (a) Hoeveel elementen heeft F? Geef A in hex en geef B in Binaire notatie.
   (b) Hoe wordt een som in F berekend en wat is de uitkomst van $A + B$, binair en in hex?
   (c) Hoe wordt een product in F berekend en wat is de uitkomst van $A * B$, binair en in hex?

5. **Hashblocker:** Je ontwikkelt een adblock-systeem op basis van SHA2-hashes. Per categorie advertenties kies je een string, en de advertentie wordt met de SHA2-hash daarvan opgenomen in de webpagina. Gebruikers kunnen een of meer van de strings kopen, en nadat de string is opgeslagen in de browser worden ad's geblokkeerd die getagd zijn met de hash ervan.
   Het kraken van de hashfunctie moet 20 seconden duren, flink langer dan de tijd (3 sec) die een advertentie de user vertraagt.
   (a) Geef een schatting van hoe lang je de strings (van letters a t/m z) moet maken opdat een brutekracht-aanpak minstens 20 seconden duurt.
   (b) Je collega wijst je erop dat het kraken veel sneller zal gaan met een Rainbow Table. Hoe lang moet je de strings maken om te zorgen dat een RT-aanval 20s duurt?

6. **Stroomversleuteling en A5:** (a) Waarin verschilt stroomversleuteling van One-Time Pad?
   (b) Hoeveel schuifregisters gebruikt de sleutelgenerator van A5 en wat is hun grootte?
   (c) Hoe beïnvloeden de schuifregisters elkaar?