Eerste Toets Security

12 oktober 2016, 8.30 – 10.30, Educ-a.

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. Vraag 2 is 2pt, de andere 3pt; samen 14, je cijfer T1 is totaal gedeeld door 1,4.
Pagina's Maak vraag 1 en 2 op pagina 1, vraag 3 op pagina 2, en vraag 4 en 5 op pagina 3.

1. **Aanmelden bij Router:** Een Wifi-router A mag een connectie met mobiel station B alleen accepteren wanneer B dezelfde WPA sleutel k kent als aanwezig in A. Om dit te controleren, kiest de router een random x, stuurt die naar het mobiele station, en verwacht $E_k(x)$ terug.
   (a) Waarom eist A niet gewoon dat B de waarde k opstuurt?
   (b) Leg uit, hoe dit mechanisme het encryptie-algoritme E blootstelt aan een CPA.
   (c) Welke maatregel wordt genomen om het risiko van een CPA te verkleinen?

2. **Entropie van AlfaRetSpace:** De karakterset `AlfaRetSpace` bestaat uit alle hoofd- en kleine letters, de `RETURN` en de spatie. Wat is de entropie van ASCII-bestanden die uit de karakterset `AlfaRetSpace` bestaan?

3. **Reductiefunctie:** Om een OneWay-functie $f : K \longrightarrow Y$ aan te vallen met een Rainbowtable heb je een *reductiefunctie* R nodig. Zeg van deze acht beweringen over reductiefuncties of ze WAAR of ONWAAR zijn, en *in 1 zin waarom*. Hier is N de grootte van K.
   (a) R reduceert de complexiteit van de aanval van $N^{2/3}$ naar $N^{1/2}$.
   (b) Je gebruikt R bij het bouwen van de tabel, maar tijdens de feitelijke aanval (query) is hij niet meer nodig.
   (c) R is een functie van Y naar K.
   (d) De rekentijd van de reductie is heel belangrijk, want bij het bouwen van de keten wordt R evenvaak aangeroepen als f.
   (e) Je gebruikt verschillende reductiefuncties zodat je de uitkomst als een random element van K kunt beschouwen.
   (f) R is de inverse van f.
   (g) Een Rainbow-table gebruikt dezelfde reductiefunctie in een hele keten.
   (h) Je gebruikt verschillende reductiefuncties om het *mergen* van ketens te voorkomen.

4. **Cryptografische sleutels:** (a) Alice stuurt een bericht aan Bob en versleutelt dit met *asymmetrische* cryptografie. Gebruikt zij dan (i) de publieke sleutel van Alice; (ii) de geheime sleutel van Alice; (iii) de publieke sleutel van Bob; of (iv) de geheime sleutel van Bob?
   (b) In een groep van 24 personen moet iedereen vertrouwelijk met elk ander kunnen communiceren. Hoeveel sleutels zijn nodig als zij dit willen doen met *symmetrische* cryptografie?
   (c) Naar schatting kunnen alle Bitcoin-miners ter wereld samen ongeveer 2^{80} decrypties per seconde uitvoeren. Schat de rekentijd die een Known-Plaintext Attack tegen 3DES kost als je al die miners een poosje mag gebruiken.

5. **Het A5 algoritme voor GSM:** Mobiele telefoongesprekken worden beveiligd tegen afluisteren met het A5/1 algoritme.
   (a) Wat is de key-lengte van A5/1? Wat zijn de groottes van de drie schuifregisters?
   (b) Warom kan een key K maximaal ongeveer 5 uur worden gebruikt?
   (c) Telefoonmaatschappijen zijn verplicht om op verzoek telefoontaps te plaatsen wanneer iemand verdacht wordt van een misdrijf. Hoe hebben de telefoonmaatschappijen toegang tot een GSM-gesprek?