Eerste Deeltoets Security

Woensdag 21 mei 2014, 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. Elke vraag geeft 2pt, cijfer is som plus 2 gedeeld door 1.6.

1. **Typen aanvallen:** (a) Wat betekenen de afkortingen KPA, COA, CPA en BFA?
   (b) Wat is het verschil tussen een KPA en een CPA?

2. **Entropie van DNA:** Alice stuurt Bob in een ASCII bestand (een Byte per letter) een DNA-sequence; deze bevat alleen de letters A, C, G en T. Zij versleutelt haar bericht met AES.
   (a) Wat is de entropie van de berichten?
   (b) Wat is de relatie tussen entropie, sleutellengte en kritieke lengte?
   (c) Hoe groot is de kritieke lengte voor deze berichten?

3. **Zwakte van DES en 3DES:** Tegen de veiligheid van DES zijn meerdere bedenkingen ingebracht nl.: (I) Door de korte sleutel is de kritieke lengte te laag; (II) DES is kwetsbaar tegen differentiële analyse; (III) De NSA heeft mogelijk een achterdeurtje ingebouwd; (IV) Door de korte sleutel is DES kwetsbaar tegen een BFA.
   (a) Zeg van elk hoe relevant ze zijn (1 zin per bedenking).
   (b) Wat is de sleutellengte van 3DES en welk van de bezwaren geldt voor 3DES?

4. **Rekenen in AES:** In AES wordt gerekend in het Finite Field $F = \mathbb{Z}_2[X]/X^8+X^4+X^3+X+1$. Laat $A = 01000011$ en $B = 00001010$.
   (a) Hoeveel elementen heeft F?
   (b) Hoe wordt een som (de $+$) in F berekend en wat is de uitkomst van $A + B$?
   (c) Hoe wordt een product (de $*$) in F berekend en wat is de uitkomst van $A * B$?

5. **Korte berichten met AES:** Alice en Bob communiceren met heel korte berichten (slechts 3 tot 5 *bits* elk) en willen die versturen met AES; een gedeelde key k hebben ze al. Omdat communicatie duur is, is het niet wenselijk om elk berichtje uit te breiden tot een AES blok. Hoe kunnen Alice en Bob met AES korte berichten uitwisselen zonder de hoeveelheid bits te laten toenemen?

6. **Reductiefuncties:** Bij een tabelaanval (Hellman of Rainbow) worden meerdere, verschillende reductiefuncties gebruikt.
   (a) Waarom is het nodig om meerdere functies te gebruiken?
   (b) Leg uit hoe Hellman en Rainbow tables verschillen in het gebruik van de reductiefuncties.

7. **A5 en tabelaanval:** Voor een tabelaanval op een systeem met N keys maak je meestal een tabel waarin $\Theta(N)$ keys verwerkt zijn, wat dan $\Theta(N)$ voorbereidingstijd kost.
   (a) Hoe lang zijn de keys van A5 en uit hoeveel bits bestaat een toestand van de stream generator?
   (b) Biryukov kon A5 kraken met een tabel die slechts een tienduizendste van de registertoestanden bevatte. Beschrijf twee oorzaken waarom dit mogelijk was.