Eerste Toets Security

Maandag 7 oktober 2019, 8.30 – 10.30, Educ-Γ.

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. Maak vragen 1 en 2 op de voorkant, 3 en 4 op pagina 2, en 5 en 6 op pagina 3 (met overloop op pagina 4). Vraag 4 is 2pt, elke andere vraag 3pt.
Let op: er zijn ook vragen op de achterkant.

1. **Offline Kahoot:** Geef bij elke vraag het antwoord wat het beste past.

   (1) Caesar cipher is het zelfde als optellen in $\mathbb{Z}_m$ voor een arbitraire m. Is Caesar cipher een veilige encryptiemethode?
   (a) Ja. (b) Nee want het is te kraken met een brute-force attack. (c) Nee want het is te kraken met een known plaintext attack. (d) Nee want het aantal sleutels waaruit je kan kiezen is te klein.

   (2) Alice en Bob gebruiken AES encryptie met een sleutel van 256 bits. Hoe veel rondes heeft hun AES algoritme? (a) 10. (b) 12. (c) 14.(d) 16.

   (3) Alice en Bob communiceren via 3DES. Oscar probeert met brute kracht een bericht te ontsleutelen dat Alice naar Bob heeft gestuurd (ciphertext-only attack) . Hoe vaak moet Oscar in het slechtste geval het DES-algoritme uitvoeren?
   (a) $2^{112} + 2^{56}$ keer. (b) $2^{113} + 2^{56}$ keer. (c) 2^{168} keer. (d) $3 \cdot 2^{168}$ keer.

   (4) Alice is een programmeur in dienst van het TV-programma "love island". Bij dit programma mag het publiek stemmen op hun favoriete koppel van de tien koppels. Je favoriete koppel is uiterst privacy-gevoelige informatie. Welke encryptiemethode kan Alice het beste bij de stemming gebruiken? (a) Elgamal. (b) MD5. (c) Diffie Hellman. (d) DES.

   (5) Alice en Bob doen een sleuteluitwisseling met behulp van de groep $\mathbb{Z}^*_{4099}$ met een generator g met orde 2011. Eve probeert de gedeelde sleutel te achterhalen met behulp van het algoritme van Shanks. Hoeveel tabelwaarden zal Eve opslaan bij deze aanval?
   (a) 11. (b) 45. (c) 130. (d) 2^{1006}.

   (6) Welke elementen zitten *niet* in de groep $\mathbb{Z}^*_{231}$?
   (a) {-13, -3, 9, 14, 286 }. (b) {-30, -13, -3, -2 }. (c) {-3, 2, 9, 14 }. (d) {-3, 9, 14, 286 }.

   (7) Een quantumcomputer kan in polynomiale tijd: (a) Een getal priemfactoriseren. (b) Een Known Plaintext Attack op AES uitvoeren. (c) Exponentieel veel matrices vermenigvuldigen. (d) Alle drie de opties.

   (8) Alice en Bob doen een sleuteluitwisseling in de groep $\mathbb{Z}^*_{29}$ met de generator 16. Alice kiest als privesleutel het getal 2, en Bob het getal 5. Wat is de gedeelde sleutel? (a) 1. (b) 7. (c) 23. (d) 24.

   (9) Hoe veel rondes heeft het DES algoritme? (a) 10. (b) 12. (c) 14. (d) 16.

   (10) Welk statement over DES is waar? (a) DES gebruikt 8 unieke S-boxen die allemaal niet inverteerbaar zijn. (b) De f-functie voert een XOR uit op twee strings van 32 bits. (c) Elke ronde wordt de sleutel bij DES 1 stap naar links geroteerd. (d) Je kunt het resultaat van DES decrypten door de uitkomst nog een keer door DES te draaien.

2. **AES:** (a) Welke vier stappen worden er in elke ronde van AES uitgevoerd?
   (b) In AES wordt er gerekend in de polynoomruimte $\mathbb{Z}_2[X]/(x^8 + x^4 + x^3 + x + 1)$. Wat is de betekenis van de volgende drie symbolen in die notatie?
   (1) $\mathbb{Z}_2$; (2) [X] (3) $/(x^8 + x^4 + x^3 + x + 1)$?
   (c) Reken uit in de polynoomruimte: $00101111 \cdot 00100100$.

3. **Begrippen:** Beantwoord in 1 of 2 zinnen per vraag (max. halve pagina samen):
   (a) Wat is een *Security Parameter*?
   (b) Wat is een *Key Stream Generator*?
   (c) Wat is het *Principe van Kerckhoffs*?

4. **Optellen in $\mathbb{Z}_m$:** Een getal in $\mathbb{Z}_m$ is een restklasse, in feite een verzameling van gehele getallen, waarbij twee getallen a_1 en a_2 in dezelfde klasse zitten wanneer ze equivalent zijn, dus als $a_1 \equiv_m a_2$ geldt.
   (a) Hoe is de relatie $\equiv_m$ gedefinieerd?
   (b) Bewijs dat als $a \equiv_m a'$ en $b \equiv_m b'$, dan $(a + b) \equiv_m (a' + b')$

5. **Elgamal:** De encryptie van Elgamal maakt gebruik van de multiplicatieve groep $\mathbb{Z}_p^*$ voor een priemgetal p en generator $g \in \mathbb{Z}_p^*$ met orde q.
   (a) We noemen G de verzameling van alle machten van g (in $\mathbb{Z}_p^*$). Bewijs dat voor elke $y \in G$, er een getal $y' \in G$ bestaat zodanig dat $y \cdot y' = 1$.
   (b) Wat zijn de eisen aan de generator $g \in \mathbb{Z}_p^*$ bij Elgamalencryptie?
   (c) Wat is het *discrete logaritme probleem*? Bob stuurt met Elgamalencryptie een bericht naar Alice. Stel dat Eve het discrete logaritme probleem op kan lossen in polynomiale tijd, hoe kan zij dan Bobs bericht ontsleutelen?

6. **A5 en Stroomversleutelen:** A5 heeft een Key Stream Generator om per datablok een streamblok te berekenen.
   (a) Welke inputs gebruikt de KSG en uit hoeveel bits bestaan die? Hoeveel bits heeft de output?
   (b) Stroomversleuteling is kwetsbaar voor manipulatie van berichten. Hoe kan Eve, zonder de sleutels te kennen, een blok van de ciphertext Y zo manipuleren dat na decryptie de bits 0 t/m 31 juist zijn, maar bits 32 t/m 63 zijn veranderd in random bits?
   (c) Hoe kan Eve, zonder de sleutels te kennen, een ciphertext Y zo manipuleren dat na decryptie de bits 0 t/m 31 juist zijn, maar bits 32 t/m 63 zijn veranderd in nullen?