# Algebra & Security, 191511410

Datum : 9-04-2014
Zaal : Sportcentrum
Tijd : 13:45-16:45

**Schrijf de uitwerkingen van de vraagstukken 1-2-3 (algebradeel) en de vraagstukken 4-5-6 (securitydeel) op aparte vellen papier, dit in verband met parallelle correctie.**
**Motiveer al uw antwoorden**
**Besteed niet te veel tijd aan een afzonderlijk onderdeel. Indien u een onderdeel niet kunt oplossen dan kunt u het resultaat van dat onderdeel in latere onderdelen toch gebruiken.**

1. De verzameling $M$ is gedefinieerd als

$$M = \{\begin{bmatrix} b & a \\ 0 & b \end{bmatrix} \mid a, b \in \mathbb{Z}, b \geq 1 \quad \text{ggd}(a,b) = 1\}.$$

Definieer op $M$ de vermenigvuldiging $*$ als volgt:

$$\begin{bmatrix} b & a \\ 0 & b \end{bmatrix} * \begin{bmatrix} d & c \\ 0 & d \end{bmatrix} = \begin{bmatrix} b & a \\ 0 & b \end{bmatrix} \cdot \begin{bmatrix} d & c \\ 0 & d \end{bmatrix} \frac{1}{\text{ggd}(ad+bc, bd)}$$

Hierbij is $\cdot$ de gewone matrixvermenigvuldiging.

   (a) Laat zien dat $(M, *)$ een groep is.

   (b) Laat zien dat $(M, *)$ en $(\mathbb{Q}, +)$ isomorf zijn.

2. (a) Uit hoeveel elementen bestaat $U(1000)$?

   (b) Laat zien dat elke $x \in U(1000)$ voldoet aan $x^{100} = 1$.

3. (a) Zij $x^2 + ax + b \in \mathbb{Z}_2[x]$. Voor welke waarde(n) van $a, b \in \mathbb{Z}_2$ is dit polynoom irreducibel?

   (b) Zij $p(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Z}_2[x]$. Voor welke waarde(n) van $a, b, c, d \in \mathbb{Z}_2$ is $\mathbb{Z}_2[x]/ < p(x) >$ een lichaam?

   (c) Bepaal alle primitieve polynomen van graad vier in $Z_2[x]$.

   (d) Laat nu $p(x) = x^4 + x + 1$. Bepaal de inverse van $x + 1 + < p(x) >$ in $\mathbb{Z}_2[x]/ < p(x) >$.

   (e) Laat zien dat $\mathbb{Z}_2[x]/ < x^4 + x + 1 >$ en $\mathbb{Z}_2[x]/ < x^4 + x^3 + 1 >$ isomorf zijn.

ZOZ

**Gebruik een apart vel papier voor de volgende (security) opgaven.**

4. (a) Alice stuurt Bob een grote file toe per e-mail, en om te controleren of die file onderweg niet veranderd is, vraagt Bob haar telefonisch om een hash van die file. Welke van de drie security-eigenschappen van de hash-functie speelt/spelen hier een rol? Leg uit.

   (b) Beschouw AES met een bloklengte van 128 bits en sleutellengte van 192 bits. Hoeveel blokken plaintext en bijbehorende ciphertext moeten worden onderschept om te zorgen dat een "exhaustive keysearch" naar alle waarschijnlijkheid maar 1 passende sleutel vindt? Leg uit.

   (c) Zelfde vraag als (b) maar dan over RSA met $p$ en $q$ van elk 512 bits, waarbij de publieke sleutel wel bekend is en de private sleutel "exhaustive" gezocht wordt.

5. In het algemeen worden LFSR's beschreven door de volgende formule:

   $$A_{i+1}(x) = A_i(x) \cdot x \mod p(x)$$

   waarin $A_i(x)$ voor $i \in \mathbb{N}$ polynomen op GF($2^k$) zijn.

   (a) Waarom kan, welke $p(x)$ je ook kiest, de periode van de gegenereerde reeks nooit $2^k$ worden?

   (b) Stel $p(x) = x^k + x^0$. Schets het bijbehorende teruggekoppelde schuifregister. Wat kan de lengte van de gegenereerde reeks worden? Is dit polynoom (dus) reducibel of irreducibel?

6. (a) Bereken met zo weinig mogelijk vermenigvuldigingen $7^9 \bmod 9$, en laat zien hoe je dat doet.

   (b) Het Diffie-Hellman algoritme is gebaseerd op machtsverheffingen modulo een priemgetal. Kan de Chinese Reststelling gebruikt worden om deze berekeningen te versnellen? Hoe, of waarom niet?

Puntenverdeling:

| 1 | | 2 | | 3 | | | | | 4 | | | 5 | | 6 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | a | b | a | b | c | d | e | a | b | c | a | b | a | b |
| 7 | 8 | 7 | 8 | 4 | 6 | 7 | 7 | 4 | 5 | 5 | 3 | 3 | 6 | 6 | 4 |

Voor een voldoende dient het puntentotaal voor de vragen 1–3 minimaal 22 en voor de vragen 4–6 minimaal 14 te zijn.
Als aan deze voorwaarde voldaan is dan wordt het tentamencijfer:
Cijfer: $1 + 9\frac{\text{punten}}{90}$