

## Algebra & Security, 191511410

Datum : 3-07-2012  
Zaal : HR C101  
Tijd : 8:45-11:45

Schrijf de uitwerkingen van de vraagstukken 1-2-3-4 (algebradeel) en de vraagstukken 5-6-7 (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. Zij  $(G, \cdot)$  de groep

$$G = \{M \mid M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad a, b, c, d \in \mathbb{Z}_{11} \quad \det M \neq 0\} \text{ met matrixvermenigvuldiging.}$$

(a) Laat zien dat  $G$  een groep is.

(b) Bepaal

$$\begin{bmatrix} 2 & 6 \\ 3 & 5 \end{bmatrix}^{-1}$$

(c) Bepaal het aantal elementen van  $G$ . Hint: bereken eerst het aantal  $2 \times 2$  matrices  $M$  in  $\mathbb{Z}_{11}^{2 \times 2}$ , de verzameling  $2 \times 2$  matrices over  $\mathbb{Z}_{11}$ , met  $\det M = 0$ .

2. (a) Schrijf de unitaire groep  $U(165)$  op vier verschillende manieren als directe som van unitaire groepen.

(b) Is  $U(165)$  cyclisch?

3. Is de verzameling  $S = \{a \mid a \in \mathbb{Z} \quad 2 \text{ deelt } a \text{ of } 3 \text{ deelt } a\}$  een deelring van  $\mathbb{Z}$ ?

4. Gegeven is het polynoom  $p(x) = 1 + x + x^3 + x^4 + x^5 \in \mathbb{Z}_2[x]$ .

(a) Laat zien dat er geen polynomen  $a(x), b(x) \in \mathbb{Z}_2[x]$  bestaan zodanig dat  $a(x)b(x) = p(x)$  en  $\text{gr } a(x) = 2$  en  $\text{gr } b(x) = 3$ .

(b) Beredeneer dat  $p(x)$  irreducibel is.

Definieer  $\mathbb{F} = \mathbb{Z}_2[x]/(p(x))$ .

(c) Is  $\mathbb{F}$  een lichaam?

(d) Hoeveel elementen heeft  $\mathbb{F}$ ?

- (e) Wat is de dimensie van  $\mathbb{F}$  als vectorruimte over  $\mathbb{Z}_2$ ?
- (f) Laat  $\mathbb{K}$  een lichaam zijn van dimensie  $d$  als vectorruimte over  $\mathbb{Z}_2$  en  $\mathbb{Z}_2 \subset \mathbb{K} \subset \mathbb{F}$ .  
Hoeveel elementen heeft  $\mathbb{K}$ ? Wat is de dimensie van  $\mathbb{F}$  opgevat als vectorruimte over  $\mathbb{K}$ ?
- (g) Beredeneer dat er geen lichamen strikt tussen  $\mathbb{Z}_2$  en  $\mathbb{F}$  zitten.

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

5. (a) Beschouw de volgende constructie, die als invoer een 128-bits sleutel  $K$  en een lang bericht  $X$  heeft. We encrypten de eerste 128 bits van  $X$  met AES onder  $K$ ; het resultaat hiervan EXOR'en we met de tweede 128 bits van  $X$ , gevolgd door weer een AES-encryptie onder  $K$ ; enzovoort, tot alle bits van  $X$  verwerkt zijn. Het resultaat is dus een getal van 128 bits. Als  $K$  nemen we de eerste 128 bits van  $\pi$  (en dit houden we niet geheim).  
Is deze constructie geschikt als cryptografische hash? Oftewel, heeft hij alle eigenschappen die van een cryptografische hash verwacht worden? Leg uit.
- (b) Beschouw een (hypothetische) blockcipher die met een blok grootte van 1 bit werkt, en in ECB-mode wordt gebruikt. Is dit equivalent met een streamcipher? Leg uit.
6. Beschouw een LFSR op basis van  $GF(2^6)$ .
- (a) Wat is de maximale lengte van de reeks die een dergelijk LFSR voortbrengt (alvorens te herhalen)? En waarom kan de reeks niet langer zijn dan dit?
- (b) In de wiskundige beschrijving van LFSRs komt altijd een polynoom voor, modulo hetwelk gerekend wordt. Normaliter is de laagste macht in dit polynoom  $x^0$ . Stel nu dat we een polynoom nemen waarin  $x^0$  niet voorkomt. Wat is dan de maximaal mogelijke lengte van de reeks? Leg uit.
7. (a) De AES-rondes bestaan uit vier stappen: Byte Substitution, ShiftRows, MixColumn, en Key Addition.  
Beschrijf kort (kwalitatief) wat ShiftRows en MixColumn doen, en leg uit waarom deze stappen nodig zijn; wat voor zwakte zou geïntroduceerd worden als deze stappen overgeslagen zouden worden?
- (b) Stel we verdubbelen de sleutelengte van RSA (bijv. van 512 naar 1024 bits). Hoe verandert dan de benodigde rekentijd voor een encryptie? En voor een decryptie? Leg uit.

Puntenverdeling:

1	2	3	4					5	6	7									
a b c	a b		a b c	d e f g	a b	a b	a b	a b	a b										
4	5	6	7	7	8	4	4	2	2	3	3	3	6	5	4	6	5	6	
1	5	3	5	4	2	2	3	1	1	3	3	4							

Voor een voldoende dient het puntentotaal voor de vragen 1-4 minimaal 22 en voor de vragen 5-7 minimaal 14 te zijn.

Als aan deze voorwaarde voldaan is dan wordt het tentamencijfer:

$$\text{Cijfer: } 1 + 9 \frac{\text{punten}}{90}$$

