Algebra & Security, 191511410

Datum : 10-04-2013
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

$$M = \{\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in \mathbb{R}\}.$$

   (a) Laat zien dat $(M, +)$ en $(\mathbb{C}, +)$ isomorf zijn.

   (b) Laat zien dat $(M^*, \times)$ en $(\mathbb{C}^*, \times)$ isomorf zijn. Hierbij betekent het sterretje: met weglating van het nul-element.

2. (a) Schrijf de unitaire groep $U(231)$ op vier verschillende manieren als directe som van tenminste twee unitaire groepen.

   (b) Is $U(231)$ cyclisch?

   (c) Stel dat p en q twee verschillende priemgetallen zijn. Onder welke voorwaarde op p en q is $U(pq)$ cyclisch?

   (d) Is $U(9)$ cyclisch?

3. Zij $p(x) = x^2 + 2x + 2 \in \mathbb{Z}_3[x]$.

   (a) Ga na of $p(x)$ irreducibel is.

   (b) Bepaal de multiplicatieve orde van $x + <p(x)>$ in $\mathbb{F} = \mathbb{Z}_3[x]/<p(x)>$.

   (c) Is $p(x)$ een primitief polynoom?

   (d) Laat $\alpha \in \mathbb{F}$ een wortel zijn van $p(x)$. Druk de andere wortel van $p(x)$ uit in α.

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

4. (a) Aan hash-functies wordt o.a. de eis van "strong collision resistance" gesteld. Wat betekent dit precies, in eigen woorden?

   (b) Stel we nemen een (geheime) 128 bits sleutel; hiervan berekenen we de hash, van die hash berekenen we weer de hash, enz. Al deze hash-waarden plakken we achter elkaar, en deze reeks bits gebruiken we als keystream voor een streamcipher. Is dit een goed idee? Leg uit.

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

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

   waarin $A_i(x)$ voor $i \in \mathbb{N}$ polynomen op GF(2^k) zijn, en $p(x)$ een primitief polynoom.

   (a) We kunnen zo'n LFSR in hardware middels registers en EXORs implementeren. Druk het aantal daarvoor benodigde EXORs uit in eigenschappen van het polynoom $p(x)$, en leg dit uit.

   (b) Stel we zouden in (1) de vermenigvuldiging met x vervangen door vermenigvuldiging met x^2. Beredeneer wat voor invloed dit heeft op de lengte van de geproduceerde pseudo-random-reeks.

6. Beschouw RSA, met publieke sleutel (e, n) en geheime sleutel (d, n). Stel dat een (wo)man-in-the-middle een met de publieke sleutel gecodeerd bericht onderschept, kwadrateert modulo n, en doorstuurt naar de ontvanger.

   (a) Wat komt er na decryptie bij de ontvanger uit? Leg uit.

   (b) Zou er na kwadratering ook iets zinnigs/voorspelbaars uitkomen als AES was gebruikt i.p.v. RSA? Leg uit.

   (c) Bereken met zo weinig mogelijk vermenigvuldigingen 5^{85} mod 11, en laat zien hoe je dat doet.

Puntenverdeling:

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

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