Algebra & Security, 191511410

Datum : 30-06-2015
Zaal : SP-3
Tijd : 08:45-11:45

Schrijf de uitwerkingen van de vraagstukken 1-2-3 (algebradeel) en de vraagstukken 4-5-6 (securitydeel) op aparte vellen papier
Motiveer al uw antwoorden en 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. (a) Bepaal van alle elementen van $U(20)$ de inverses.
   (b) Bepaal van alle elementen van $U(20)$ de ordes.
   (c) Is $U(20)$ cyclisch?
   (d) Gegeven is een isomorfisme $\phi : U(20) \to \mathbb{Z}_2 \oplus \mathbb{Z}_4$ met $\phi(3) = (0,1)$ en $\phi(13) = (1,1)$. Bepaal de beelden van alle andere elementen van $U(20)$ onder dit isomorfisme.

2. Zij $R_n = \{a + b\mathrm{i} \mid a, b \in \mathbb{Z}_n\}$, hierbij is i een symbool met de eigenschap: $\mathrm{i}^2 = -1$ en $n \in \mathbb{N}$, $n > 1$. Op R_n gebruiken we de voor de hand liggende optelling en vermenigvuldiging zodat R_n een ring is.
   (a) Geef de definitie van nuldeler.
   (b) Bepaal een nuldeler $g \in R_5$.
   (c) Stel dat $n = x^2 + y^2$ met $x, y \in \mathbb{N}$, $x \neq 0 \neq y$. Laat zien dat R_n nuldelers heeft. Hint: kijk nog eens goed naar het geval $n = 5$. Bepaal een nuldeler $g \in R_{13}$.

3. (a) Laat $a(x) = x^2 + a_1x + a_0 \in \mathbb{Z}_2[x]$. Bepaal alle mogelijke waarden van a_0 en a_1 waarvoor $a(x)$ irreducibel is.
   (b) Laat $b(x) = x^3 + b_2x^2 + b_1x + b_0 \in \mathbb{Z}_2[x]$. Bepaal alle mogelijke waarden van b_0, b_1 en b_2 waarvoor $b(x)$ irreducibel is.
   (c) Zij $p(x) = x^5 + p_4x^4 + p_3x^3 + p_2x^2 + p_1x + p_0 \in \mathbb{Z}_2[x]$. Bepaal alle $p(x)$ die gefactoriseerd kunnen worden in irreducibele polynomen van graad twee respectievelijk drie.
   (d) Bewijs dat $p(x) = x^5 + x^4 + x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$ irreducibel is.
   (e) Zij $\mathbb{F} = \mathbb{Z}_2[x]/<p(x)>$. Is $\mathbb{F}$ een lichaam?
   (f) Beschrijf de elementen van $\mathbb{F}$. Hoeveel elementen heeft $\mathbb{F}$?
   (g) Geef een basis van $\mathbb{F}$ opgevat als vectorruimte over $\mathbb{Z}_2$? Wat is de dimensie?
   (h) Bepaal de inverse van $x^2 + < p(x) >$.

ZOZ

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

4. (a) Kan een hashfunctie zo zijn dat verschillende berichten dezelfde hashwaarde geven? Leg uit.

   (b) Kan, bij symmetrische cryptografie, een encryptiealgoritme zo zijn dat verschillende plaintexts, met dezelfde sleutel, dezelfde ciphertext geven? Leg uit.

   (c) Stel dat je betalingsopdrachten aan je bank ongeëncrypt verstuurt, maar wel de hash ervan meestuurt, geëncrypt met de publieke sleutel van de bank. De bank kan dan met haar privésleutel de hash decrypten en controleren.
   Dit is niet veilig tegen een man-in-the-middle die met de betalingsopdracht knoeit: waarom niet? En hoe zou je dit systeem kunnen veranderen om het wel veilig te maken?

5. Beschouw een LFSR op GF(2^5) gegeven door de formule $A_{i+1}(x) = A_i(x) \cdot x \mod x^5 + x^2 + x^0$, met beginwaarde $A_0(x) = x^4 + x^3 + x^2 + x^1 + x^0$.

   (a) Bepaal $A_1(x)$, op twee manieren: door bovenstaande formule in te vullen, en door te schetsen wat er in het bijbehorende teruggekoppelde schuifregister gebeurt.

   Beschouw de reeks bits geproduceerd door een LFSR op GF(2^k) gebaseerd op een primitief polynoom.

   (b) Hoeveel 0'en komen er maximaal achter elkaar voor in die reeks, en hoeveel 1'en? Leg uit.

6. (a) Bereken zo efficiënt mogelijk $7^{11} \mod 10$ en laat zien hoe je dat doet.

   (b) Twee partijen hebben allebei een RSA-sleutelpaar gegenereerd, maar ongelukkigerwijs hebben beiden dezelfde p gekozen; wel zijn hun q's verschillend, en dus ook hun sleutels. Stel je hebt van beide partijen de publieke sleutel, en je weet (of vermoed) dat hun p's gelijk zijn, hoe kun je dan efficiënt van beiden de geheime sleutel berekenen?
   (Hint: gebruik het Euclidisch algoritme.)

Puntenverdeling:

1				2			3								4			5		6	
a	b	c	d	a	b	c	a	b	c	d	e	f	g	h	a	b	c	a	b	a	b
5	5	3	6	2	5	5	3	4	2	4	3	4	4	3	4	4	5	5	5	5	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: $1 + 9\frac{\text{punten}}{90}$