Algebra & Security, 191511410

Datum : 28-06-2016
Zaal : CR-2G
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, 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 $G = U(14)$ (unitaire groep).
   (a) Bepaal de orde van $5 \in G$.
   (b) Is G cyclisch?
   (c) Bepaal een isomorfisme van G naar een ondergroep van S_6, de groep van permutaties van zes symbolen, door van elk element van G het beeld in S_6 te geven. Schrijf deze beelden in disjuncte-cykel-vorm.
   (d) Bepaal met behulp van de vorige onderdelen, dus zonder verdere berekeningen, de ordes van de elementen van G.
2. Laat voor $n \geq 2$ $A_n = \{f(x) \mid f(x) \in \mathbb{Z}[x] \quad f(0) = 0 \mod n\}$.
   (a) Geef de definitie van priemideaal.
   (b) Kies $n = 3$, laat zien dat A_3 een priemideaal is.
   (c) Voor welke waarde(n) van n is A_n een priemideaal?
   (d) Ga na of A_3 een maximaal ideaal is.
3. Zij $p(x) \in \mathbb{Z}_5[x]$ gegeven door: $p(x) = x^3 + 2x^2 + 3$ en $I =< p(x) >$ het ideaal in $\mathbb{Z}_5[x]$ voortgebracht door $p(x)$.
   (a) Geef de definitie van irreducibel polynoom in $\mathbb{K}[x]$. Hierbij is $\mathbb{K}$ een lichaam.
   (b) Laat zien dat $p(x)$ irreducibel is.
   (c) Beargumenteer dat $\mathbb{F} = \mathbb{Z}_5[x]/I$ een lichaam is.
   (d) Beschrijf de algemene vorm van de elementen van $\mathbb{F} = \mathbb{Z}_5[x]/I$. Hoeveel verschillende elementen heeft $\mathbb{F}$?
   (e) Bepaal de inverse van $2x + 4 + I$ in $\mathbb{F}$.
   (f) Laat zien dat $\mathbb{F}$ isomorf is met $\mathbb{Z}_5[x]/< x^3 + 3x + 2 >$.

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

4. (a) Alice downloadt een grote zip-file als torrent, en om te controleren of er met die file niet geknoeid is (bijv. een virus erin gestopt), berekent ze de hash ervan en vergelijkt deze met de hash die de maker van de zip-file op zijn (voldoende beveiligde) website heeft gepubliceerd. Welke van de drie security-eigenschappen van de hash-functie speelt hier een rol? Leg uit, en leg ook uit waarom de andere twee geen rol spelen.

   (b) Beschouw DES met een bloklengte van 64 bits en sleutellengte van 56 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 1024 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 $p(x) = x^k + x^2$ (aannemend dat $k > 2$). Schets het bijbehorende teruggekoppelde schuifregister. Wat kan de lengte van de gegenereerde reeks worden? Is dit polynoom (dus) reducibel of irreducibel?

6. (a) Een veel gebruikte waarde voor de publieke exponent in RSA is $e = 65537 = 2^{16} + 1$. Leg uit waarom deze keuze rekentijd bespaart in vergelijking met andere mogelijkheden van dezelfde orde van grootte.

   (b) AES bestaat uit 10 "rondes" achter elkaar, dus we zouden AES kunnen zien als twee keer "halfAES" achter elkaar, elk bestaande uit 5 zulke rondes. Leg uit hoe een meet-in-the-middle attack in essentie werkt, en waarom AES ondanks deze opdeling niet kwetsbaar is voor een meet-in-the-middle attack.

Puntenverdeling:

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

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