Algebra & Security, 191511410

Datum : 01-07-2014
Zaal : Sportcentrum
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 een groep met $|G| = 33$.
   (a) Stel $g \in G$, wat zijn de mogelijkheden voor de orde $|g|$.
   (b) Laat $g_1, g_2 \in G$ met $|g_1| = |g_2| = 11$ en definieer:
   $$H_i = \{g_i^k \mid k = 1, \ldots, 11\}$$
   Laat zien dat
   $$H_1 = H_2 \quad \text{of} \quad H_1 \cap H_2 = \{\text{e}\}.$$
   (c) Wat is het maximaal aantal elementen van orde 11 in G?
   (d) Als $|g| = 33$, wat is dan $|g^{11}|$?
   (e) Laat zien dat er een $g \in G$ is met $|g| = 3$.
   (f) Kun je op soortgelijke manier concluderen dat er een element $h \in G$ bestaat met $|h| = 11$?

2. Beschouw de ring $R = \mathbb{Z}[x]$ met daarin de verzameling A gedefinieerd door:
   $$A = \left\{p_0 + p_1x + p_2x^2 + p_3x^3 + \cdots + p_nx^n \mid n \geq 0, \quad p_i \in \mathbb{Z}, \quad p_0, p_1 \text{ even } \right\}$$
   (a) Laat zien dat A een ideaal in R is.
   (b) Definieer $K = R/A$. Karakteriseer de elementen van K. Hoeveel elementen heeft K?
   (c) Is K een integriteitsgebied?
   (d) Is K een lichaam?
   (e) Is A een priemideaal?
   (f) Is A een maximaal ideaal?

3. Laat $p(x) = x^3 + 2x + 2 \in \mathbb{Z}_3[x]$.
   (a) Laat zien dat $p(x)$ irreducibel is.
   (b) Ga na of $p(x)$ een primitief polynoom is.

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

4. Alice stelt een contract op voor een financiële transactie met Bob. Bob gaat akkoord met dit contract; ten bewijze daarvan berekent hij een hash van het contract, encrypt deze met zijn private RSA-sleutel, en geeft het resultaat aan Alice.

   (a) Leg uit hoe dit als electronische handtekening functioneert: met wat voor argumentatie kan Alice een (cryptografisch deskundige) rechter ervan overtuigen dat Bob het contract écht ondertekend heeft?

   (b) Welke van de drie security-eigenschappen van de hash-functie speelt of spelen hier een rol? Leg uit.

5. Beschouw een variant van de LFSR beschreven door de volgende formule:

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

   met $A_i(x)$ polynomen op GF(2^k), en $p(x)$ een k-de-graads polynoom.

   (a) Zou het een goed idee zijn om met een dergelijke constructie de pseudo-random bits voor een streamcipher te genereren? Leg uit.

   Neem vanaf nu $k = 7$ en $p(x) = x^7 + x^3 + 1$.

   (b) Schets hoe deze LFSR-variant als teruggekoppeld schuifregister geïmplementeerd kan worden, en leg uit hoe je hier op komt vanuit de formule.

   (c) Beredeneer dat deze LFSR-variant een reeks produceert die net zo lang is als die van de "gewone" LFSR (d.w.z., zonder de extra $1 + x$ term).

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) Bij gebruik van AES wordt aanbevolen een andere mode dan ECB ("Electronic Code Book") te gebruiken. Wat is het nadeel van ECB? Beschrijf ook een andere mode (naar keuze) en leg uit hoe die het nadeel van ECB voorkomt.

Puntenverdeling:

1						2						3		4		5			6	
a	b	c	d	e	f	a	b	c	d	e	f	a	b	a	b	a	b	c	a	b
2	8	4	4	4	3	8	4	4	2	2	2	4	7	4	5	3	5	5	5	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: $1 + 9\frac{\text{punten}}{90}$