Algebra & Security, 191511410

Datum : 11-04-2012
Zaal : SC
Tijd : 13:45-16:45

Schrijf de uitwerkingen van de vraagstukken 1-2-3-4 (algebradeel) en de vraagstukken 5-6-7 (securitydeel) op aparte papieren, 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 het resultaat van dat onderdeel in latere onderdelen toch gebruiken.

1. Zij $(G, \cdot)$ een groep. Definieer

$$Z(G) = \{h \in G \mid \forall g \in G : \quad g \cdot h = h \cdot g\}.$$

   (a) Laat zien dat $Z(G)$ een ondergroep van G is.

   (b) Zij nu G de matrixgroep met als bewerking matrixvermenigvuldiging

$$G = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \quad ad - bc \neq 0\}.$$

   Bepaal $Z(G)$.

   (c) Laat zien dat $Z(G)$ isomorf met $\mathbb{R}\backslash\{0\}$ met de gewone vermenigvuldiging is.

2. Is de unitaire groep $U(34)$ cyclisch?

3. Beschouw de ring van polynomen met rationale coëfficiënten, $\mathbb{Q}[x]$.

   (a) Geef de definitie van maximaal ideaal.

   (b) Laat zien dat $< x >$, het ideaal voortgebracht door het polynoom x, een maximaal ideaal is.

   (c) Laat zien dat $\mathbb{Q}[x]/ < x >$ isomorf is met $\mathbb{Q}$.

4. (a) Laat zien dat $f(x) \in \mathbb{Z}_2[x]$ met $f(x) = x^2 + x + 1$ het enige irreducibele polynoom van graad twee in $\mathbb{Z}_2[x]$ is.

   (b) Laat α een wortel van $x^2 + x + 1$ in een lichaamsuitbreiding van $\mathbb{Z}_2$ zijn. Bepaal de (multiplicatieve) inverse van $\alpha \in \mathbb{Z}(\alpha)$.

   (c) Bepaal een irreducibel polynoom $p(x) \in \mathbb{Z}_2[x]$ van graad vier.

   (d) Construeer een lichaam van zestien elementen.

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

5. Bij een (binaire) streamcipher kan een man-in-the-middle die de sleutel niet kent, doelbewust één bit van de plaintext veranderen door het corresponderende bit van de ciphertext te veranderen.

   (a) Kan een man-in-the-middle dat ook doen als deze streamcipher wordt vervangen door AES? Hangt dit nog af van de gekozen mode (ECB, OFB, etc.)? Leg uit.

   (b) Men wil dit probleem oplossen door na elke 4096 databits die met de streamcipher versleuteld zijn, onversleuteld de SHA-1 hash van die 4096 versleutelde databits te versturen. Is dit afdoende, in de zin dat de man-in-the-middle niet meer onopgemerkt met de bits kan knoeien? Leg uit.

6. Beschouw een LFSR die beschreven wordt door

$$A_{i+1}(x) = A_i(x) \cdot (x+1) \mod x^6 + x^3 + 1$$

   in GF(2^5). Merk op dat i.t.t. de voorbeelden uit het college, hier niet met x wordt vermenigvuldigd, maar met $x+1$.

   (a) Aannemend dat de beginwaarde $A_0(x) = x^5 + x^4$ is, bepaal de eerste 2 bits die er "links" worden uitgeschoven.

   (b) Schets (in Galois-vorm) een blokdiagram met schuifregisters en EXORs dat deze LFSR implementeert. Geef voldoende toelichting zodat duidelijk is hoe je van de algebraische formule naar je diagram komt.

7. Beschouw het versnellen van RSA-berekeningen.

   (a) Bereken zonder rekenmachine $5^9 \mod 11$, gebruikmakend van een efficiënt algoritme, en laat zien hoe je dat doet.

   (b) De Chinese Reststelling (Chinese Remainder Theorem) kan worden gebruikt om de *private*-key-berekening (meestal decryptie) van RSA flink te versnellen. Waarom kan de CRT niet worden gebruikt om de *public*-key-kant te versnellen?

Puntenverdeling:

1			2	3			4				5		6		7	
a	b	c		a	b	c	a	b	c	d	a	b	a	b	a	b
6	8	5	8	2	8	6	3	5	3	4	4	4	4	8	8	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:
Cijfer: $1 + 9\frac{\text{punten}}{80}$