Algebra & Security, code 151141

Datum : 06-04-2011
Zaal : SC
Tijd : 13:45-16:45

Schrijf de uitwerkingen van de vraagstukken 1-2-3 (algebradeel) en de vraagstukken 4-5 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.

Vraagstukken 4 en 5 zijn zowel in het Engels als het Nederlands beschikbaar.

1. Zij $G_1 = U(20)$ (unitaire groep) en $G_2 = \mathbb{Z}_2 \oplus \mathbb{Z}_4$.
   (a) Geef alle elementen van G_1 en bepaal hun ordes.
   (b) Is G_1 cyclisch?
   (c) Geef de definitie van groepsisomorfisme.
   (d) Construeer een groepsisomorfisme $\phi : G_1 \to G_2$.
2. Zij $R = \{a + b\mathrm{i} \mid a, b \in \mathbb{Z}_3\}$, hierbij is i een element met de eigenschap: $\mathrm{i}^2 = 2$.
   (a) Laat zien dat elk element $a + b\mathrm{i} \neq 0$ een multiplicatieve inverse heeft.
   (b) Laat zien dat R met de gewone optelling en vermenigvuldiging een ring is.
   (c) Wat is de inverse van $1 + \mathrm{i}$?
3. Zij $p(x) \in \mathbb{Z}_5[x]$ gegeven door: $p(x) = x^3 + 2x^2 + 1$ en $I = < p(x) >$ het ideaal in $\mathbb{Z}_5[x]$ voortgebracht door $p(x)$.
   (a) Laat zien dat $p(x)$ irreducibel is.
   (b) Beargumenteer dat $\mathbb{F} = \mathbb{Z}_5[x]/I$ een lichaam is.
   (c) Uit hoeveel elementen bestaat $\mathbb{F} = \mathbb{Z}_5[x]/I$?
   (d) Bepaal de inverse van $2x + 3 + I$ in $\mathbb{F}$.
   (e) Laat zien dat $\mathbb{F}$ isomorf is met $\mathbb{Z}_5[x]/ < x^3 + 3x + 2 >$.

4. Let $\{s_i\}_{i\geq 0}$ be a sequence generated by a linear shift register with a primitive characteristic polynomial $f(x)$ of degree n.

   (a) Let $f(x) = x^7 + x + 1$ and let the output sequence start as follows $\{1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, \ldots\}$. What is the initial state? Verify the recurrence relation. Verify the given sequence. Find s_{50} and s_{129} (what is the period of this sequence)?

   (b) Show that the shortest LFSR that can output the sequence $\{0, 0, 1, 1, 0, 1, 1, 1, 0\}$ has degree 5. Give an LFSR of degree 5 that can output the sequence. Use that all primitive polynomials of
   degree 2 are: $x^2 + x + 1$
   degree 3 are: $x^3 + x + 1$, $x^3 + x^2 + 1$
   degree 4 are: $x^4 + x + 1$, $x^4 + x^3 + 1$
   degree 5 are: $x^5 + x^2 + 1$, $x^5 + x^3 + 1$, $x^5 + x^3 + x^2 + x + 1$, $x^5 + x^4 + x^3 + x^2 + 1$, $x^5 + x^4 + x^2 + x + 1$, $x^5 + x^4 + x^3 + x + 1$

5. (a) Generate two 6 bits prime numbers p and q and form an RSA modulus $n = p \cdot q$ (a 12 bits number). Let RSA public exponent $e = 3$. Compute the corresponding private key d. Illustrate RSA encryption with the plaintext $x = 101001101001$, then decrypt the ciphertext y using Chinese Remainder Theorem.

   (b) Common modulus attack: If a plaintext is encrypted twice with the RSA system using two RSA keys (n, e) and (n, f) and if $\gcd(e, f) = 1$, then the plaintext m can be recovered from the two ciphertext $c_e = m^e \pmod{n}$ and $c_f = m^f \pmod{n}$. How?

4. Laat $\{s_i\}_{i\geq 0}$ een rij zijn die gegenereerd is door een linear shift register met een primitieve karakteristieke polynoom $f(x)$ van graad n.

   (a) Laat $f(x) = x^7 + x + 1$ zijn en laat de uitvoerrij als volgt zijn $\{1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, \ldots\}$. Wat is de initiële toestand? Verifieer de recurrence relatie. Verifieer de gegeven rij. Vind s_{50} en s_{129} (wat is de periode van deze rij)?

   (b) Laat zien dat de kortste LFSR die de rij $\{0, 0, 1, 1, 0, 1, 1, 1, 0\}$ kan produceren graad 5 heeft. Geef een LFSR van graad 5 die deze rij produceert. Gebruik dat; alle primitieve polynomen van
   graad 2 zijn: $x^2 + x + 1$
   graad 3 zijn: $x^3 + x + 1$, $x^3 + x^2 + 1$
   graad 4 zijn: $x^4 + x + 1$, $x^4 + x^3 + 1$
   graad 5 zijn: $x^5 + x^2 + 1$, $x^5 + x^3 + 1$, $x^5 + x^3 + x^2 + x + 1$, $x^5 + x^4 + x^3 + x^2 + 1$, $x^5 + x^4 + x^2 + x + 1$, $x^5 + x^4 + x^3 + x + 1$

5. (a) Genereer twee 6 bits priemgetallen p en q en vorm een RSA modulus $n = p \cdot q$ (een 12 bits getal). Laat de RSA public exponent $e = 3$ zijn. Bereken de bijbehorende private key d. Illustreer een RSA encryptie met de plaintext $x = 101001101001$, decrypt de ciphertext y vervolgens door gebruik te maken van de Chinese Remainder Theorem.

   (b) Common modulus attack: Als een plaintext twee keer is ge-encrypt met een RSA systeem gebruik makend van de twee RSA keys (n, e) en (n, f), en als de $\gcd(e, f) = 1$, dan kan de plaintext m berekend worden uit de twee ciphertexts $c_e = m^e \pmod{n}$ en $c_f = m^f \pmod{n}$. Hoe?

Puntenverdeling:

1				2			3					4		5	
a	b	c	d	a	b	c	a	b	c	d	e	a	b	a	b
6	2	2	6	6	6	4	4	4	6	8	4	10	6	10	6

Voor een voldoende dient het puntentotaal voor de vragen 1-3 minimaal 22 en voor de vragen 4-5 minimaal 14 te zijn.
Als aan deze voorwaarde voldaan is dan wordt het tentamencijfer:
Cijfer: $1 + 9\frac{\text{punten}}{80}$