Algebra & Security, Securitydeel

Datum : 28-06-2011
Zaal : SP 1
Tijd : 08:45-11:45 (beide delen)
Tijd : 08:45-10:45 (algebradeel)
Tijd : 08:45-10:15 (securitydeel)

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.

4. Ga uit van een LFSR met feedback polynoom $f(x) = x^5 + x^4 + 1$. Laat $\{s_i\}_{i\geq 0}$ de output reeks van dit register zijn wanneer de initiële staat wordt gegeven door $(s_0, s_1, s_2, s_3, s_4) = (0, 1, 1, 0, 1)$.

   (a) Wat is de periode van de output reeks? Wat is de periode van de output reeks als $f(x)$ een primitieve polynoom zou zijn?

   (b) Geef een kortere LFSR die dezelfde reeks kan genereren. Gebruik dat alle primitieve polynomen van graad 4 zijn: x^4+x+1, x^4+x^3+1; van graad 3 zijn: $x^3 + x + 1, x^3 + x^2 + 1$; en van graad 2 zijn: $x^2 + x + 1$.

5. Het RSA systeem wordt op een smart card gebruikt om documenten te signeren. De publieke parameters zijn $n = 55$ en $e = 17$. De smart card maakt gebruik van de Chinese Remainder Theorem om de documenten te signeren.

   (a) Laat de pre-calculaties zien (transformeer de prive sleutel d naar het CRT domein, i.e. bereken d_p, d_q, c_p, c_q) om dit systeem op te zetten.

   (b) Bereken de signature c van het bericht $m = 9$ door gebruik te maken van de CRT.

4. Consider an LFSR with the feedback polynomial $f(x) = x^5 + x^4 + 1$. Let $\{s_i\}_{i\geq 0}$ be the output sequence generated by this register, when the initial state is given by $(s_0, s_1, s_2, s_3, s_4) = (0, 1, 1, 0, 1)$.

(a) What is the period of the output sequence? What would the period be if $f(x)$ had been primitive?

(b) Give a shorter LFSR that can generate the same output sequence. Use that all primitive polynomials of degree 4 are: x^4+x+1, x^4+x^3+1; of degree 3 are: x^3+x+1, x^3+x^2+1; and of degree 2 are: x^2+x+1.

5. The RSA system is being used on a smart card to sign documents. Its public parameters are $n = 55$ and $e = 17$. The smart card makes use of the Chinese Remainder Theorem to sign documents.

   (a) Show the pre-calculations (transform the secret key d into the CRT domain, i.e. compute d_p, d_q, c_p, c_q) to set this up.

   (b) Compute the signature c of the message $m = 9$ using the CRT.

Puntenverdeling:

1			2			3								4		5	
a	b	c	a	b	c	a	b	c	d	e	f	g	h	a	b	a	b
4	5	5	5	3	6	3	2	4	4	5	3	5	4	8	8	8	8

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