Algebra & Security, code 151141

Datum : 07-04-2010
Zaal : WA 1
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.

1. Ga na of $U(10)$ en $U(12)$ isomorf zijn.

2. Zij G de verzameling matrices gegeven door:

$$G = \{\begin{bmatrix} \alpha & \beta \\ 2\beta & \alpha \end{bmatrix} \mid \alpha, \beta \in \mathbb{Z}_3 \ \ (\alpha, \beta) \neq (0,0)\}.$$

   Op G beschouwen we de bewerking matrixvermenigvuldiging.

   (a) Laat zien dat G met matrixvermenigvuldiging een groep is.

   (b) Geef de definitie van groepsisomorfisme.

   (c) Zij $\mathbb{F} = \mathbb{Z}_3[x]/ < x^2 + 1 >$. Laat zien dat $\phi : G \to \mathbb{F}\backslash\{0\}$ gedefinieerd door

$$\phi\left(\begin{bmatrix} \alpha & \beta \\ 2\beta & \alpha \end{bmatrix}\right) = \alpha + \beta x$$

   een groepsisomorfisme tussen G en de vermenigvuldigingsgroep van het lichaam $\mathbb{F}$ definieert.

3. Zij $p(x) \in \mathbb{Z}_7[x]$ gegeven door: $p(x) = x^2 + 3x + 1$ en $I =< p(x) >$ het ideaal in $\mathbb{Z}_7[x]$ voortgebracht door $p(x)$.

   (a) Laat zien dat $p(x)$ irreducibel is.

   (b) Beargumenteer dat $\mathbb{F} = \mathbb{Z}_7[x]/I$ een lichaam is.

   (c) Uit hoeveel elementen bestaat $\mathbb{F} = \mathbb{Z}_7[x]/I$?

   (d) Bepaal de inverse van $2x + 3 + I$ in $\mathbb{F}$.

English

4. Consider an affine linear block cipher defined with $A = \begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 0 \\ 3 & 6 & 0 \end{pmatrix}$ and $b = (0, 9, 1)$ as a column vector in the Galois Field GF(p) with $p = 11$. Let the plaintext be $m = (7, 8, 1, 0, 10, 9, 2, 3, 4, 7, 8, 1)$.

   (a) Encrypt the plaintext m using ECB mode and CTR mode (with counter = (0, 3, 1)). The counter increments (0, 3, i) to (0, 3, $i + 1$ mod p) at each step.

   (b) Compute the CBC-MAC and CMAC for the plaintext m.

   (c) Why does ECB mode provide weak security? Demonstrate it by using the result from 4a.

   (d) Construct a plaintext which has the same CBC-MAC as the one in item 4b.

5. (a) Let $p = 47$ (the order of the group) and $\alpha = 7$ (the generator of the cyclic group) be the parameters of an ElGamal encryption scheme. If the private key of Alice is $a = 10$, what will be her public key? Bob wants to send a message $m = 37$ to Alice. What will be the corresponding ciphertext c if the used ephemeral key is $k = 5$? How can Alice recover the plaintext from c?

   (b) Demonstrate how to compute the RSA decryption (private) key given the prime numbers $p = 23$, $q = 11$ and the public exponent $e = 7$. What will be the corresponding ciphertext c for the binary string 110101? Show how to decrypt c. Can $e = 5$ be used as a public exponent and explain why?

   (c) Show the correctness of the Digital Signature Algorithm (DSA). DSA specifies that if the signature generation process results in a value $s = 0$, a new value of k should be generated and the signature must be recalculated. Why?

Nederlands

4. Ga uit van een affien lineair *block cipher* gedefinieerd door $A = \begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 0 \\ 3 & 6 & 0 \end{pmatrix}$ en $b = (0, 9, 1)$ als een kolom vector in de Galois Lichaam GF(p) met $p = 11$. Laat de *plaintext* (klare tekst) zijn: $m = (7, 8, 1, 0, 10, 9, 2, 3, 4, 7, 8, 1)$.

(a) Encrypt de plaintext m met ECB mode en CTR mode (met counter = (0, 3, 1)). De counter incrementeert (0, 3, i) naar (0, 3, $i + 1 \bmod p$) bij elke stap.

(b) Bereken de CBC-MAC en CMAC van plaintext m.

(c) Waarom verschaft ECB mode weak security? Toon dit aan door gebruik te maken van de resultaten van 4a.

(d) Construeer een plaintext met dezelfde CBC-MAC als die uit 4b.

5. (a) Laat $p = 47$ (de orde van de groep) en $\alpha = 7$ (de generator van de cyclische groep) de parameters van een ElGamal encryptie schema zijn. Als de private key van Alice $a = 10$ is, wat is dan haar public key? Bob wil een bericht $m = 37$ naar Alice versturen. Wat zal de corresponderende ciphertext c zijn, als de gebruikte ephemeral key $k = 5$ is? Hoe kan Alice de plaintext terug halen uit c?

(b) Laat zien hoe de RSA decryption key is te berekenen, gegeven de priemgetallen $p = 23$, $q = 11$ en de public exponent $e = 7$. Wat zal de corresponderende ciphertext c zijn voor de binaire string 110101? Laat zien hoe c te decrypten. Kan $e = 5$ gebruikt worden als een public exponent - leg uit waarom.

(c) Toon de correctheid van de Digital Signature Algorithm (DSA) aan. DSA specificeert dat als het signature generatie proces resulteert in een waarde $s = 0$, er en nieuwe waarde voor k gegenereerd dient te worden en de signature opnieuw moet worden berekend. Waarom?

Puntenverdeling:

1	2			3				4				5		
	a	b	c	a	b	c	d	a	b	c	d	a	b	c
12	10	4	10	5	5	5	7	2 (ECB) 3 (CTR)	2 (CBC) 3 (CMAC)	4	4	4	4	6

Voor een voldoende dient het puntentotaal voor de vragen 1-3 minimaal 25 en voor de vragen 4-5 minimaal 14 te zijn.
Als aan deze voorwaarde voldaan is dan wordt het tentamencijfer:
Cijfer: $1 + \frac{\text{punten}}{10}$