Algebra & Security, 191511410

Datum : 2-07-2013
Zaal :
Tijd : 8:45-11:45

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 $p \in \mathbb{N}$ een priemgetal en $(G, \cdot)$ gegeven door

$$G = \{M \mid M = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \quad a, b, c \in \mathbb{Z}_p \quad \det M = 1\}$$

met matrixvermenigvuldiging.

(a) Laat zien dat G een groep is.

(b) Bepaal voor $p = 5$:

$$\begin{bmatrix} 2 & 2 \\ 0 & 3 \end{bmatrix}^{-1}$$

(c) Bepaal het aantal elementen van G.

(d) Bepaal voor $p = 5$, de orde van

$$\begin{bmatrix} 2 & 2 \\ 0 & 3 \end{bmatrix}$$

(e) Beredeneer dat voor $p = 3$, G isomorf is met $\mathbb{S}_3$, de permutatiegroep op drie symbolen.

2. (a) Schrijf de unitaire groep $U(440)$ op vier verschillende manieren als directe som van tenminste twee unitaire groepen.

(b) Is $U(440)$ cyclisch?

(c) Hoe kun je $U(8)$ schrijven als directe som van unitaire groepen?

3. Zij $p(x) = x^2 + 1 \in \mathbb{Z}_3[x]$.

(a) Ga na of $p(x)$ irreducibel is.

(b) Bepaal de multiplicatieve orde van $x + <p(x)>$ in $\mathbb{F} = \mathbb{Z}_3[x]/<p(x)>$.

(c) Is $p(x)$ een primitief polynoom?

(d) Laat $\alpha \in \mathbb{F}$ een wortel zijn van $p(x)$. Druk de andere wortel van $p(x)$ uit in α.

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

4. (a) Aan hash-functies worden vaak de eisen "weak collision resistance" en "strong collision resistance" gesteld. Wat is het essentiële verschil?

   (b) Bij het aanspreken van een https-website (bijv. van een bank) wordt public-key cryptografie gebruikt. Welke rol speelt het zgn. certificaat daarin? Beschrijf een aanval die door het gebruik van een certificaat onmogelijk wordt gemaakt.

5. Beschouw twee LFSRs, gebaseerd op *hetzelfde* primitieve polynoom $p(x)$ op GF(2^k), met *verschillende* beginwaarden $A_0 \neq 0$ and $B_0 \neq 0$:

$$A_{i+1}(x) = A_i(x) \cdot x \mod p(x) \tag{1a}$$
$$B_{i+1}(x) = B_i(x) \cdot x \mod p(x) \tag{1b}$$

   (a) Stel je heet Snowden en je hebt iets te verbergen voor de Amerikaanse overheid. Is het verstandig om dat te encrypten met een streamcipher waarvan de keystream uit een LFSR komt? Leg uit.

   (b) We construeren een nieuwe pseudo-random reeks door de EXOR te nemen van de beide door A en B geproduceerde reeksen. Wat is de herhalingsperiode van deze reeks, en wat kun je er nog meer over zeggen?
   (Hint: definieer $C_i = A_i + B_i$ en leid een vergelijking voor C_{i+1} af.)

6. (a) De "mix columns" stap in AES, en zijn inverse, worden beschreven door respectievelijk (in de gebruikelijke hexadecimale notatie):

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} B_0 \\ B_1 \\ B_2 \\ B_3 \end{pmatrix} \quad \text{en} \quad \begin{pmatrix} B'_0 \\ B'_1 \\ B'_2 \\ B'_3 \end{pmatrix} = \begin{pmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{pmatrix} \begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{pmatrix}.$$

   Aannemend (om het rekenwerk te beperken) dat $B_1 = B_2 = B_3 = 0$, toon aan dat $B'_0 = B_0$, dus dat de decryptie inderdaad werkt.

   (b) Leg in eigen woorden uit hoe de meet-in-the-middle attack op dubbele encryptie (bijv. "double DES") werkt.

   (c) AES bestaat uit 10 "rondes" achter elkaar, dus we zouden AES kunnen zien als twee keer "halfAES" achter elkaar, elk bestaande uit 5 zulke rondes. Waarom kan deze opdeling niet gebruikt worden voor een meet-in-the-middle attack?

Puntenverdeling:

1					2			3				4		5		6		
a	b	c	d	e	a	b	c	a	b	c	d	a	b	a	b	a	b	c
3	4	4	5	4	6	6	4	5	7	4	6	4	6	4	6	6	3	3

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