Opgaven Getaltheorie en Cryptografie (deel 1)

Inleverdatum: 28 februari 2002

1. We vatten $\{0,1\}$ op als het lichaam $\mathbb{F}_2$. Een schuifregisterrij is een rij $\{s_n\}_{n=0}^{\infty}$ in $\mathbb{F}_2$ gegeven door r startwaarden $s_0, \ldots, s_{r-1} \in \mathbb{F}_2$ en door een recurrentie

$$s_n = f(s_{n-1}, \ldots, s_{n-r}) \quad (n \geq r)$$

waarbij f een functie van $\mathbb{F}_2^r$ naar $\mathbb{F}_2$ is. Schuifregisterrijen worden gebruikt als bouwsteen van conventionele cryptosystemen.

a) Definieer de afbeelding $T : \mathbb{F}_2^r \to \mathbb{F}_2^r$ door

$$T(x_1, x_2, \ldots, x_r) = (x_2, x_3, \ldots, x_r, f(x_r, x_{r-1}, \ldots, x_1)).$$

Beschouw de vectoren $\mathbf{s}_n = (s_n, s_{n+1}, \ldots, s_{n+r-1}) \in \mathbb{F}_2^r$ $(n \geq 0)$. Laat zien dat $\mathbf{s}_{n+1} = T\mathbf{s}_n$ voor alle $n \geq 0$. Bewijs hiermee dat de rij $\{\mathbf{s}_n\}$ $(n \geq 0)$ uiteindelijk periodiek is met periode $\leq 2^r$, d.w.z. er zijn getallen n_0 en p met $n_0 \geq 0$ en $1 \leq p \leq 2^r$ zodat $\mathbf{s}_{n+p} = \mathbf{s}_n$ voor alle $n \geq n_0$. (Aanwijzing: er zijn i, j met $0 \leq i < j \leq 2^r$ en $\mathbf{s}_i = \mathbf{s}_j$; pas nu T toe.) Laat dan zien dat de rij $\{s_n\}$ ook uiteindelijk periodiek is met periode $\leq 2^r$.

b) Veronderstel dat $f(x_1, \ldots, x_r) = x_1 + g(x_2, \ldots, x_r)$ voor zekere functie $g : \mathbb{F}_2^{r-1} \to \mathbb{F}_2$, waarbij $+$ de optelling in $\mathbb{F}_2$ is. Bewijs dat de bovengenoemde afbeelding T inverteerbaar is. Laat zien dat de rij $\{\mathbf{s_n}\}$ periodiek is met periode $\leq 2^r$, d.w.z. er is een getal p met $1 \leq p \leq 2^r$ zodat $\mathbf{s}_{n+p} = \mathbf{s}_n$ voor alle $n \geq 0$. Laat dan zien dat de rij $\{s_n\}$ ook periodiek is met periode $\leq 2^r$.

2. Een lineaire schuifregisterrij is een rij $\{s_n\}_{n=0}^{\infty}$ in $\mathbb{F}_2$ gegeven door r startwaarden $s_0, \ldots, s_{r-1} \in \mathbb{F}_2$, niet alle gelijk aan 0, en door een lineaire recurrentie

$$s_n = c_1 s_{n-1} + c_2 s_{n-2} + \cdots + c_r s_{n-r} \quad (n \geq r)$$

waarbij $c_1, c_2, \ldots, c_r \in \mathbb{F}_2$, $c_r \neq 0$, en waarbij de optelling en vermenigvuldiging die van $\mathbb{F}_2$ zijn. We definiëren het karakteristieke polynoom van deze rij door $f(X) = X^r + c_1 X^{r-1} + \cdots + c_t$.

a) Beschouw de vectoren $\mathbf{s}_n = (s_n, s_{n+1}, \ldots, s_{n+r-1})$ $(n \geq 0)$. Bewijs met inductie naar n dat $\mathbf{s}_n \neq \mathbf{0}$ voor alle $n \geq 0$ (gebruik de aannamen $\mathbf{s}_0 \neq \mathbf{0}$ en $c_r \neq 0$). Leid hieruit af dat de rij $\{s_n\}$ periodiek is met periode $\leq 2^r - 1$.

b) We nemen nu aan dat het karakteristieke polynoom f primitief is. Bewijs dat in dat geval de rij $\{s_n\}$ periodiek is met periode gelijk aan $2^r - 1$, m.a.w. het kleinste getal p zodat $s_{n+p} = s_n$ voor alle $n \geq 0$ is $p = 2^r - 1$.

Aanwijzingen:
De aanname dat f primitief is impliceert dat we het eindige lichaam $\mathbb{F}_{2^r}$ kunnen representeren als

$$\begin{aligned}\mathbb{F}_{2^r} =&\{x_0 + x_1\alpha + x_2\alpha^2 + \cdots + x_{r-1}\alpha^{r-1} : x_0, \ldots, x_{r-1} \in \mathbb{F}_2\} \\ &\text{met } f(\alpha) = 0\end{aligned} \tag{1}$$

en dat α een voortbrenger is van $\mathbb{F}_{2^r}^*$. Met andere woorden,

$$\mathbb{F}_{2^r}^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{2^r-2}\}, \quad \alpha^{2^r-1} = 1 \tag{2}$$

en voor elke vector $\mathbf{x} = (x_0, \ldots, x_{r-1}) \in \mathbb{F}_2^r$ met $\mathbf{x} \neq \mathbf{0}$ is er een t met $0 \leq t \leq 2^r - 2$ zodat

$$x_0 + x_1\alpha + \cdots + x_{r-1}\alpha^{r-1} = \alpha^t\,. \tag{3}$$

Een functie $\varphi : \mathbb{F}_{2^r} \to \mathbb{F}_2$ heet lineair als $\varphi(\lambda x + \mu y) = \lambda\varphi(x) + \mu\varphi(y)$ voor $\lambda, \mu \in \mathbb{F}_2$, $x, y \in \mathbb{F}_{2^r}$.
Bewijs nu het volgende:

b1) Definieer de functie $\varphi : \mathbb{F}_{2^r} \to \mathbb{F}_2$ door

$$\begin{aligned}\varphi(x_0 + x_1\alpha + \cdots + x_{r-1}\alpha^{r-1}) =& s_0x_0 + s_1x_1 + \cdots + s_{r-1}x_{r-1} \\ &(x_0, \ldots, x_{r-1} \in \mathbb{F}_2)\,.\end{aligned}$$

Laat zien dat φ lineair is en bewijs met inductie naar n dat $\varphi(\alpha^n) = s_n$ voor alle $n \geq 0$.

b2) Zij $1 \leq p < 2^r - 1$. Bewijs dat er een t met $0 \leq t < 2^r - 1$ bestaat zo dat $s_{n+p} - s_n = s_{n+t}$ voor alle $n \geq 0$. Gebruik b1), (2) en de lineariteit van φ.

b3) Bewijs dat de rij $\{s_n\}_{n=0}^{\infty}$ periodiek is met periode $2^r - 1$.

3. Zij $\{s_n\}$ een lineaire schuifregisterrij als in Opgave 2 waarbij het karakteristieke polynoom f primitief is. De bedoeling is aan te tonen dat zulke rijen enkele mooie statistische eigenschappen hebben.

a) Beschouw de vectoren $\mathbf{s}_n = (s_n, s_{n+1}, \ldots, s_{n+r-1})$. Bewijs dat alle vectoren $\mathbf{s}_n$ $(n = 0, 1, \ldots, 2^r - 2)$ verschillend zijn en dat $\{\mathbf{s}_0, \ldots, \mathbf{s}_{2^r-2}\} = \mathbb{F}_2^r \backslash \{\mathbf{0}\}$.

b) Bewijs dat onder de termen s_n $(n = 0, 1, 2, \ldots, 2^r - 2)$ $2^{r-1} - 1$ keer een 0 voorkomt en 2^r keer een 1.
(Aanwijzing: laat zien dat er onder de vectoren in $\mathbb{F}_2^r \backslash \{\mathbf{0}\}$ precies $2^{r-1} - 1$ zijn waarvan de eerste coördinaat gelijk is aan 0. Deze vectoren corresponderen met $2^{r-1} - 1$ indices n.)

c) Bewijs dat onder de paren (s_n, s_{n+1}) $(n = 0, 1, 2, \ldots, 2^r - 2)$ het patroon $(0, 0)$ $2^{r-2} - 1$ keer voorkomt, en elk van de patronen $(0, 1), (1, 0), (1, 1)$ 2^{r-2} keer. Bewijs een generalisatie voor drietallen (s_n, s_{n+1}, s_{n+2}) $(n = 0, 1, \ldots, 2^r - 2)$, viertallen $(s_n, s_{n+1}, s_{n+2}, s_{n+3})$,..., r-tallen?
(Aanwijzing voor paren: bekijk van alle vectoren in $\mathbb{F}_2^r \backslash \{0\}$ de eerste twee coordinaten.)

4. Zijn V, W vectorruimten over $\mathbb{F}_2$. Een afbeelding $\psi : V \to W$ heet lineair als $\psi(\lambda\mathbf{x} + \mu\mathbf{y}) = \lambda\psi(\mathbf{x} + \mu\psi(\mathbf{y})$ voor alle $\lambda, \mu \in \mathbb{F}_2$, $\mathbf{x}, \mathbf{y} \in V$. Een afbeelding $\varphi : V \to W$ heet affien als er een lineaire afbeelding $\psi : V \to W$ en een vector $\mathbf{b} \in W$ bestaan zodat $\varphi(\mathbf{x}) = \psi(\mathbf{x}) + \mathbf{b}$ voor $\mathbf{x} \in V$.

a) Bewijs dat de samenstelling van twee affiene afbeeldingen weer affien is.

b) Zij $\varphi : V \to V$ een affiene afbeelding, gegeven door $\varphi(\mathbf{x}) = \psi(\mathbf{x}) + \mathbf{b}$ waarbij $\psi : V \to V$ lineair is. Bewijs dat φ inverteerbaar is dan en slechts dan als ψ inverteerbaar is.

c) Zij $\varphi : V \to W$ een affiene afbeelding. Laat zien dat $\varphi(\mathbf{x}+\mathbf{y})+\varphi(\mathbf{0}) = \varphi(\mathbf{x})+\varphi(\mathbf{y})$ voor $\mathbf{x}, \mathbf{y} \in V$.

5.*a)* Laat zien dat het polynoom $F = X^8 + X^4 + X^3 + X + 1 \in \mathbb{F}_2[X]$ dat in Rijndael gebruikt wordt irreducibel is.

b) Zij f de functie van $\mathbb{F}_{2^8} \to \mathbb{F}_{2^8}$ gedefinieerd door $f(0) = 0$, $f(x) = x^{-1}$ voor $x \neq 0$. Bewijs: als $x, y \in \mathbb{F}_{2^8}$, $f(x + y) + f(0) = f(x) + f(y)$, $x \neq y$, $xy \neq 0$ dan is $x^2 + xy + y^2 = 0$.

c) Bepaal het aantal paren $(x, y) \in \mathbb{F}_{2^8} \times \mathbb{F}_{2^8}$ waarvoor $f(x+y)+f(0) = f(x)+f(y)$. Concludeer hieruit dat f niet affien is. Laat dan zien dat de afbeelding $S : \mathbb{F}_{2^8} \to \mathbb{F}_{2^8}$ gedefinieerd op blz. 3.15 van het dictaat (in de beschrijving van BS) niet affien is.

Aanwijzing: neem $x, y \in \mathbb{F}_{2^8}$ met $f(x+y)+f(0) = f(x)+f(y)$, $x \neq y$, $xy \neq 0$ en laat $\beta = x/y$. Zij $\mathbb{F}$ het kleinste deellichaam van $\mathbb{F}_{2^8}$ dat β bevat. Hoeveel elementen heeft dit lichaam?

d) Om de implementatie te vereenvoudigen is het blokcijfer Rijndael zo geconstrueerd dat ontcijferen op bijna dezelfde manier gaat als vercijferen.

De klare-tekstruimte, cijfertekstruimte en sleutelruimte zijn alle gelijk aan $\mathcal{V}$, waarbij $\mathcal{V}$ de vectorruimte is bestaande uit alle 4×4-matrices met elementen uit $\mathbb{F}_{2^8}$.

Voor gegeven klare tekst $M \in \mathcal{V}$ en sleutel $K \in \mathcal{V}$ wordt de Rijndael-cijfertekst $C = E_K(M)$ als volgt berekend: (de operatie + geeft de optelling in $\mathcal{V}$ aan):

1) bereken $K_0, K_1, \ldots, K_{10}$ uit K m.b.v. KE.

2) bereken achtereenvolgens $M_1, M_2, \ldots, M_{10}$ door

$$\begin{aligned} M_1 &= MC \circ SR \circ BS(M + K_0), \\ M_i &= MC \circ SR \circ BS(M_{i-1} + K_{i-1}) \quad \text{voor } i = 2, \ldots, 9, \\ M_{10} &= SR \circ BS(M_9 + K_9), \\ C = E_K(M) &= M_{10} + K_{10}. \end{aligned}$$

Definieer nu

$$\begin{aligned} &K'_0 = K_{10}, \\ &K'_1 = MC^{-1}(K_9),\ K'_2 = MC^{-1}(K_8), \ldots,\ K'_9 = MC^{-1}(K_1), \\ &K'_{10} = K_0, \end{aligned}$$

$$M'_1 = MC^{-1}(M_9 + K_9), M'_2 = MC^{-1}(M_8 + K_8), \ldots, M'_9 = MC^{-1}(M_1 + K_1),$$
$$M'_{10} = M + K_0.$$

Bewijs dat

$$\begin{aligned} M'_1 &= MC^{-1} \circ SR^{-1} \circ BS^{-1}(C + K'_0), \\ M'_i &= MC^{-1} \circ SR^{-1} \circ BS^{-1}(M'_{i-1} + K'_{i-1}) \quad \text{voor } i = 2, \ldots, 9, \\ M'_{10} &= SR^{-1} \circ BS^{-1}(M'_9 + K'_9), \\ M = D_K(C) &= M'_{10} + K'_{10} \end{aligned}$$

(dus ontcijferen gaat op precies dezelfde manier als vercijferen, met dien verstande dat BS, SR, MC moeten worden vervangen door hun inversen BS^{-1}, SR^{-1}, MC^{-1}).
Aanwijzing: laat eerst zien dat $SR \circ BS = BS \circ SR$ en dat MC lineair is.