Cryptography

PROF. DR. JOACHIM VON ZUR GATHEN, KONSTANTIN ZIEGLER

2. Assignment: MixColumns, CRT and units in $\mathbb{Z}_N$

(Due: Friday, 13 November 2009, 12^{00})

Exercise 2.1 (`MixColumns`). (12 points)

The `MixColumns`-step of the AES-algorithm takes place in the ring

$$S = \mathbb{F}_{256}[y]/\langle y^4 + 1 \rangle.$$

(i) The ring S is not a field. In particular, there are nonzero elements in S *without* a multiplicative inverse. Give an example and explain how you could check that property. $\boxed{2}$

(ii) The output b_3, b_2, b_1 and b_0 of the `MixColumns`-step for a column with entries a_3, a_2, a_1 and a_0 is determined by the product $\boxed{3}$

$$b_3y^3 + b_2y^2 + b_1y + b_0 = (\texttt{02} + \texttt{01}y + \texttt{01}y^2 + \texttt{03}y^3) \cdot (a_3y^3 + a_2y^2 + a_1y + a_0).$$

Expand the product over $\mathbb{F}_{256}[y]$, reduce it modulo $y^4 + 1$ and collect the terms with equal powers of y to obtain equations for b_3, b_2, b_1 and b_0.

(iii) Find a 4×4-matrix $\mathcal{M}$ with entries from $\mathbb{F}_{256}$ to express this multiplication as a matrix-vector product $\boxed{2}$

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} = \mathcal{M} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}.$$

(iv) Use this matrix-vector product to perform the `MixColumns`-operation on the following state of AES: $\boxed{3}$

$$\begin{bmatrix} \texttt{00} & \texttt{00} & \texttt{00} & \texttt{00} \\ \texttt{7A} & \texttt{00} & \texttt{00} & \texttt{00} \\ \texttt{01} & \texttt{00} & \texttt{01} & \texttt{00} \\ \texttt{00} & \texttt{00} & \texttt{00} & \texttt{AA} \end{bmatrix}$$

(v) The `InvMixColumns`-operation is the inverse of `MixColumns`. From exercise 1.3 (iii) you know that the product of $\texttt{02} + \texttt{01}y + \texttt{01}y^2 + \texttt{03}y^3$ with $\texttt{0B}y^3 + \texttt{0D}y^2 + \texttt{09}y + \texttt{0E}$ is $\texttt{01}$ in S. Use this information to write down the `InvMixColumns`-operation on a column b in matrix-vector-notation. $\boxed{2}$

Exercise 2.2 (Chinese Remainder Theorem). (14 points)

To investigate the structure of rings $(\mathbb{Z}_N, +, \cdot)$ with composite N it is useful to pick a suitable factorization $N = ab$ and look at the set $\mathbb{Z}_a \times \mathbb{Z}_b$ consisting of all pairs (x, y) with $x \in \mathbb{Z}_a$ and $y \in \mathbb{Z}_b$. We define addition and multiplication on $\mathbb{Z}_a \times \mathbb{Z}_b$ componentwise.

$\boxed{2}$ (i) Consider $20 = 5 \cdot 4$ and look at the map $\pi_1 : \mathbb{Z}_{20} \to \mathbb{Z}_4$ which maps an integer $0, 1, \ldots, 19 \in \mathbb{Z}_{20}$ to its remainder modulo 4. Prove that for any two elements $a, b \in \mathbb{Z}_{20}$ the following holds:

(†) $\quad \pi_1(a + b) = \pi_1(a) + \pi_1(b)$ and $\pi_1(a \cdot b) = \pi_1(a) \cdot \pi_1(b).$

Fill out a table with rows indexed by $\mathbb{Z}_4$ and columns indexed by $\mathbb{Z}_5$.

Note: a map having the properties (†) is called a *ring homomorphism*.

$\boxed{1}$ (ii) Pick two elements $x, y \in \mathbb{Z}_{20}$ (to make it interesting: the sum of the representing integers shall be larger than 20). First, add them in $\mathbb{Z}_{20}$ and then map to $\mathbb{Z}_5 \times \mathbb{Z}_4$. Second, map both to $\mathbb{Z}_5 \times \mathbb{Z}_4$ and add afterwards. What do you observe?

$\boxed{1}$ (iii) Pick two elements $x, y \in \mathbb{Z}_{20}$ (to make it interesting: the product of the representing integers shall be larger than 20). First, multiply them in $\mathbb{Z}_{20}$ and then map to $\mathbb{Z}_5 \times \mathbb{Z}_4$. Second, map both to $\mathbb{Z}_5 \times \mathbb{Z}_4$ and multiply afterwards. What do you observe?

$\boxed{2}$ (iv) Mark all the invertible elements in $\mathbb{Z}_5$, $\mathbb{Z}_4$, and $\mathbb{Z}_{20}$. What is their relationship?

$\boxed{4}$ (v) Revisit the previous four questions under the factorization $20 = 2 \cdot 10$.

Now consider two relatively prime positive integers $a, b \in \mathbb{Z}_{\geq 2}$.

$\boxed{1}$ (vi) Let x be any integer and suppose $x \pmod{ab}$ is invertible. Prove that $x \pmod{a}$ and $x \pmod{b}$ are also invertible.

$\boxed{2}$ (vii) Assume that an integer y is invertible modulo a and modulo b. Prove that y is then invertible modulo ab.

$\boxed{1}$ (viii) Conclude that there is a bijection between $\mathbb{Z}_{ab}^{\times}$ and $\mathbb{Z}_a^{\times} \times \mathbb{Z}_b^{\times}$.

Exercise 2.3 (Units in $\mathbb{Z}_N$). (6 points)

We prove the following useful

Theorem. *Let $N \geq 2$ be a positive integer and consider the ring $(\mathbb{Z}_N, +, \cdot)$ and $a \in \mathbb{Z}$. Then the following holds:*

$$a \in \mathbb{Z}_N^\times \Leftrightarrow \gcd(a, N) = 1.$$

(i) Assume $a \in \mathbb{Z}_N^\times$, so that there is a $b \in \mathbb{Z}_N$ with $ab = 1$ in $\mathbb{Z}_N$. Prove that $\gcd(a, N) = 1$. $\boxed{3}$

(ii) Let $a \in \mathbb{Z}_N$ and assume $\gcd(a, N) = 1$. Prove that there is an element $b \in \mathbb{Z}_N$ so that $\boxed{3}$

$$a \cdot b = 1 \text{ in } \mathbb{Z}_N.$$