CPSC 418 / MATH 318 — Introduction to Cryptography
ASSIGNMENT 2

Name: Harjee Johal
Student ID: 30000668

Problem 1 — Arithmetic in the AES MixColumns operation (22 marks)

(a) i. (a) (i) For this question, we are asked to prove that in AES MIXCOLUMNS arithmetic multiplying any 4-byte vector by y is a circular left shift by one byte. Suppose that a is a 4-byte vector such that $a = (a_3, a_2, a_1, a_0)$. Let $a(y) = a_3y^3 + a_2y^2 + a_1y + a_0$ be the polynomial representation of a. Thus, $a(y) * y$ is:

$$\begin{aligned} a(y) * y &= (a_3y^3 + a_2y^2 + a_1y + a_0) * y \\ &= a_3y^4 + a_2y^3 + a_1y^2 + a_0y. \end{aligned}$$

Next, we must perform reduction of $a(y)*y$ modulo *M(y)*. We are told that $M(y) = 0$ and that $M(y) = y^4+1$. From this, can determine that since $y^4+1 = 0$, then $y^4 = 1$. Applying this to $a(y) * y$, we get:

$$\begin{aligned} a(y) * y &= a_3y^4 + a_2y^3 + a_1y^2 + a_0y \\ &= a_3(1) + a_2y^3 + a_1y^2 + a_0y \\ &= a_2y^3 + a_1y^2 + a_0y + a_3. \end{aligned}$$

From this, we can see that $a(y)*y = (a_2, a_1, a_0, a_3)$ in vector form. When we compare the vector form of $a(y) * y$, (a_2, a_1, a_0, a_3) to the vector form of $a(y)$, (a_3, a_2, a_1, a_0), we can see that the bytes of $a(y) * y$ are the same bytes of $a(y)$, except that they have been circularly shifted to the left by one. Therefore, in AES MIXCOLUMNS arithmetic, the multiplication of any 4-byte vector a will result in its bytes being shifted circularly left by one byte.

ii. For this question, we are asked to prove that in AES MIXCOLUMNS arithmetic, $y^i = y^j$ for any integer $i \geq 0$ where $j \equiv i \ (mod 4)$ with $0 \leq j \leq 3$. If $i \equiv j$ mod (4), and i is an integer, then i can be rewritten in the form $i = 4k + j$, where k is an integer such that $i/4 = k$. Using this assertion, we can turn the equation $y^i = y^j$ into:

$$\begin{aligned} y^i &= y^j \\ y^{4k+j} &= y^j \\ (y^4)^k y^j &= y^j. \end{aligned}$$

We are told that in AES MIXCOLUMNS arithmetic, $M(y) = y^4 + 1 = 0$. From this, we find that $y^4 = 1$. We can use this equation substitute y^4 with 1, giving us:

$$
\begin{aligned}
(1)^k y^j &= y^j \\
y^j &= y^j.
\end{aligned}
$$

Thus, we can see that in this arithmetic, $y^i = y^j$ for any integer $i \geq 0$ where $j \equiv i \pmod 4$ with $0 \leq j \leq 3$.

iii. We are asked to prove that in this arithmetic, the multiplication of any 4-byte vector by $y^i \geq 0$ is a circular left shift by j bytes, where $j \equiv i \pmod 4$ with $0 \leq j \leq 3$. Suppose that a is a 4-byte vector represented as (a_3, a_2, a_1, a_0) .Let $a(y) = a_3y^3 + a_2y^2 + a_1y + a_0$ be the polynomial representation of a. In this arithmetic, we are told that $M(y) = y^4 + 1$ and that $M(y) = 0$. From this we get $y^4 = 1$. From part (a)(ii) we know that $y^i = y^j$ for any integer $i \geq 0$ where $j \equiv i \pmod 4$ with $0 \leq j \leq 3$. Therefore, there are four cases to be examined:

Case 1: j = 0. If $j = 0$, then $y^i = y^j = y^0 = 1$. Therefore, when we multiply $a(y)$ with y^i, we get:

$$
\begin{aligned}
a(y) * y^i &= a(y) * 1 \\
&= a(y).
\end{aligned}
$$

Therefore, $a(y) * y^0 = a(y) = (a_3, a_2, a_1, a_0)$, which is a left circular shift of a by 0 bytes. Thus, in this case the statement is proven true.

Case 2: j = 1. If $j = 1$, then $y^i = y^j = y^1 = y$. Therefore, when we multiply $a(y)$ with y^i, we get:

$$
\begin{aligned}
a(y) * y^i &= a(y) * y \\
&= (a_3y^3 + a_2y^2 + a_1y + a_0) * y \\
&= a_3y^4 + a_2y^3 + a_1y^2 + a_0y.
\end{aligned}
$$

Using the fact that in this arithmetic $y^4 = 1$, we can reduce this equation to:

$$
a(y) * y = a_3 + a_2y^3 + a_1y^2 + a_0y \qquad = a_2y^3 + a_1y^2 + a_0y + a_3.
$$

Therefore, $a(y) * y^1 = a(y) = (a_2, a_1, a_0, a_3)$, which is a left circular shift of a by 1 byte. Thus, in this case the statement is proven true.

Case 3: j = 2. If $j = 2$, then $y^i = y^j = y^2$. Therefore, when we multiply $a(y)$ with y^i, we get:

$$
\begin{aligned}
a(y) * y^i &= a(y) * y^2 \\
&= (a_3y^3 + a_2y^2 + a_1y + a_0) * y^2 \\
&= a_3y^5 + a_2y^4 + a_1y^3 + a_0y^2.
\end{aligned}
$$

Using the fact that in this arithmetic $y^4 = 1$, we can reduce this equation to:

$$\begin{aligned} a(y) * y &= a_3 y + a_2 + a_1 y^3 + a_0 y^2 \\ &= a_1 y^3 + a_0 y^2 + a_3 y + a_2. \end{aligned}$$

Therefore, $a(y) * y^2 = a(y) = (a_1, a_0, a_3, a_2)$, which is a left circular shift of a by 2 bytes. Thus, in this case the statement is proven true.

Case 4: j = 3. If $j = 3$, then $y^i = y^j = y^3$. Therefore, when we multiply $a(y)$ with y^i, we get:

$$\begin{aligned} a(y) * y^i &= a(y) * y^3 \\ &= (a_3 y^3 + a_2 y^2 + a_1 y + a_0) * y^3 \\ &= a_3 y^6 + a_2 y^5 + a_1 y^4 + a_0 y^3. \end{aligned}$$

Using the fact that in this arithmetic $y^4 = 1$, we can reduce this equation to:

$$\begin{aligned} a(y) * y &= a_3 y^2 + a_2 y + a_1 + a_0 y^3 \\ &= a_0 y^3 + a_3 y^2 + a_2 y + a_1. \end{aligned}$$

Therefore, $a(y) * y^3 = a(y) = (a_0, a_3, a_2, a_1)$, which is a left circular shift of a by 3 bytes. Thus, in this case the statement is proven true.

From this, we can see that the statement holds for all cases. Therefore, the statement is true.

(b) i. In the Rijndahl field GF(2^8), the bytes (01), (02), and (03) are, respectively:

$$\begin{aligned} c_1(x) &= 1 \\ c_2(x) &= x \\ c_3(x) &= x + 1. \end{aligned}$$

ii. From the previous part, we know that the Rijndahl representation of (02) is $c_2(x) = x$. The representation of b in the Rijndahl field GF(2^8), $b(x)$, is:

$$b(x) = b_7 x^7 + b_6 x^6 + b_5 x^5 + b_4 x^4 + b_3 x^3 + b_2 x^2 + b_1 x^1 + b_0.$$

Therefore, the value of $d = (02)b$ in the Rijndahl field can be computed as:

$$\begin{aligned} d &= (02)b \\ d(x) &= c_2(x) b(x) \\ &= (x)(b_7 x^7 + b_6 x^6 + b_5 x^5 + b_4 x^4 + b_3 x^3 + b_2 x^2 + b_1 x^1 + b_0) \\ &= b_7 x^8 + b_6 x^7 + b_5 x^6 + b_4 x^5 + b_3 x^4 + b_2 x^3 + b_1 x^2 + b_0 x. \end{aligned}$$

We are told that in this field, arithmetic is done modulo $m(x)$, where $m(x) = x^8 + x^4 + x^3 + x + 1$. We can use the fact that the modulus for a given modular arithmetic is always zero for the corresponding modular arithmetic to determine that $m(x) = 0$, since $m(x)$ is the modulus that corresponds to the Rijndahl field GF(2^8). Since $m(x) = 0 = x^8 + x^4 + x^3 + x + 1$, we find that $x^8 = x^4 + x^3 + x + 1$ in this field. We can substitute this into the expression determined for $d = (02)b$ to obtain:

$$\begin{aligned} d(x) &= b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x \\ &= b_7(x^4 + x^3 + x + 1) + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x \\ d(x) &= b_6x^7 + b_5x^6 + b_4x^5 + (b_3 + b_7)x^4 + (b_2 + b_7)x^3 + b_1x^2 + (b_0 + b_7)x + b7. \end{aligned}$$

Thus, we have determine the expression for $d(x)$. Given that d is a byte in the form $d = (d_7d_6d_5 \dots d_1d0)$, we can write the symbolic expression for each bit d_i of d in terms of the bits of b:

$$\begin{aligned} d_7 &= b_6 \\ d_6 &= b_5 \\ d_5 &= b_4 \\ d_4 &= b_3 + b_7 \\ d_3 &= b_2 + b_7 \\ d_2 &= b_1 \\ d_1 &= b_0 + b_7 \\ d_0 &= b_7. \end{aligned}$$

iii. From the part (i), we know that the Rijndahl representation of (03) is $c_3(x) = x+1$. The representation of b in the Rijndahl field GF(2^8), $b(x)$, is:

$$b(x) = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x^1 + b_0.$$

Therefore, the value of $e = (03)b$ in the Rijndahl field can be computed as:

$$\begin{aligned} e &= (03)b \\ e(x) &= c_3(x)b(x) \\ &= (x + 1)(b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x^1 + b_0) \\ &= b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x + b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + \\ &= b_7x^8 + (b_6 + b_7)x^7 + (b_5 + b_6)x^6 + (b_4 + b_5)x^5 + (b_3 + b_4)x^4 + (b_2 + b_3)x^3 + (b_1 + b_2)x^2 + (b \end{aligned}$$

We are told that in this field, arithmetic is done modulo $m(x)$, where $m(x) = x^8 + x^4 + x^3 + x + 1$. We can use the fact that the modulus for a given modular arithmetic is always zero for the corresponding modular arithmetic to determine that $m(x) = 0$, since $m(x)$ is the modulus that corresponds to the Rijndahl field

GF(2^8). Since $m(x) = 0 = x^8 + x^4 + x^3 + x + 1$, we find that $x^8 = x^4 + x^3 + x + 1$ in this field. We can substitute this into the expression determined for $e = (03)b$ to obtain:

$$
\begin{aligned}
e(x) &= b_7x^8 + (b_6 + b_7)x^7 + (b_5 + b_6)x^6 + (b_4 + b_5)x^5 + (b_3 + b_4)x^4 + (b_2 + b_3)x^3 + (b_1 + b_2)x^2 + (b_{\cdots} \\
&= b_7(x^4 + x^3 + x + 1) + (b_6 + b_7)x^7 + (b_5 + b_6)x^6 + (b_4 + b_5)x^5 + (b_3 + b_4)x^4 + (b_2 + b_3)x^3 + (\\
e(x) &= (b_6 + b_7)x^7 + (b_5 + b_6)x^6 + (b_4 + b_5)x^5 + (b_3 + b_4 + b_7)x^4 + (b_2 + b_3 + b_7)x^3 + (b_1 + b_2)x^2 +
\end{aligned}
$$

Thus, we have determine the expression for $e(x)$. Given that e is a byte in the form $e = (e_7e_6e_5 \ldots e_1e0)$, we can write the symbolic expression for each bit e_i of e in terms of the bits of b:

$$
\begin{aligned}
e_7 &= b_6 + b_7 \\
e_6 &= b_5 + b_6 \\
e_5 &= b_4 + b_5 \\
e_4 &= b_3 + b_4 + b_7 \\
e_3 &= b_2 + b_3 + b_7 \\
e_2 &= b_1 + b - 2 \\
e_1 &= b_0 + b_1 + b_7 \\
e_0 &= b_0 + b_7.
\end{aligned}
$$

(c) i.

ii.

Problem 2 — Error propagation in block cipher modes (12 marks)

(a) i.

ii.

iii.

iv.

v.

(b)

Problem 3 — Binary exponentiation (13 marks)

(a)

(b) i.

ii.

iii.

Problem 4 — A modified man-in-the-middle attack on Diffie-Hellman (10 marks)

(a)

(b)

(c)

Problem 5 — A simplified password-based key agreement protocol (8 marks)

(a)

(b)

(c)

Problem 6 — Primitive roots for safe primes (6 marks)

Problem 7 — Discrete logarithms with respect to different primitive roots (8 marks)

Problem 8 — An algorithm for extracting discrete logarithms (21 marks)

(a)

(b)

(c)

(d)

(e) i.

ii.

Problem 10 — Playfair cipher cryptanalysis, 10 marks