Brian Yee - 00993104
Introduction to Cryptography CPSC 418 Fall 2016
Department of Computer Science
University of Calgary

October 28, 2016

HOME WORK #2

Problem	Marks
1	
2	
3	
4	
5	
6	
7	
Total	

Problem 1. Conditional entropy

1.a)
$\boldsymbol{H(M|C) = \sum_{c \in C} p(C) \sum_{m \in M} p(M|C) log_2(\frac{1}{p(M|C)})}$
$\boldsymbol{H(M|C) = \sum p(C) \sum p(M|C) log_2(\frac{1}{p(M|C)})}$
$\boldsymbol{= 4 * \frac{1}{4}(\frac{1}{2} log_2(2) + \frac{1}{2} log_2(2))}$
$\boldsymbol{= 1}$

1.b)
$\boldsymbol{H(M|C) = \sum p(C) \sum p(M|C) log_2(\frac{1}{p(M|C)})}$
$\boldsymbol{= \sum p(C) \sum p(M) log_2(\frac{1}{p(M)})}$ (since with perfect secrecy, $\boldsymbol{p(M|C) = p(M)}$)
$\boldsymbol{= \sum p(M) log_2(\frac{1}{p(M)}) * \sum p(C)}$ (since the log is independent of C)
$\boldsymbol{= \sum p(M) log_2(\frac{1}{p(M)}) * |C| * \frac{1}{|C|}}$ (since each ciphertext is equiprobable)
$\boldsymbol{= \sum p(M) log_2(\frac{1}{p(M)}) * 1}$
$\boldsymbol{= \sum p(M) log_2(\frac{1}{p(M)})}$
$\boldsymbol{= H(M)}$

1.c)
No, since $\boldsymbol{p(M|C) = \frac{1}{2} \neq \frac{1}{4} = p(M)}$.

⟶ $\mathcal{A}$nswer

Problem 2. Binary polynomial arithmetic

2.a.i)
$\boldsymbol{x^3}$
$\boldsymbol{x^3 + 1}$
$\boldsymbol{x^3 + x}$
$\boldsymbol{x^3 + x + 1}$
$\boldsymbol{x^3 + x^2}$
$\boldsymbol{x^3 + x^2 + 1}$
$\boldsymbol{x^3 + x^2 + x}$
$\boldsymbol{x^3 + x^2 + x + 1}$

2.a.ii)
$\boldsymbol{x^3 = x * x * x}$
$\boldsymbol{x^3 + 1 = (x + 1)(x^2 - x + 1)}$
$\boldsymbol{x^3 + x = x(x^2 + x)}$
$\boldsymbol{x^3 + x + 1 =}$ irreducible
$\boldsymbol{x^3 + x^2 = x^2(x + 1)}$
$\boldsymbol{x^3 + x^2 + 1 =}$ irreducible
$\boldsymbol{x^3 + x^2 + x = x(x^2 + x + 1)}$
$\boldsymbol{x^3 + x^2 + x + 1 = (x + 1)(x^2 + 1)}$

2.a.iii)
Let $\boldsymbol{A(x)}$ be a degree 3 polynomial. If $\boldsymbol{A(x)}$ is reducible, then it must the product of a degree 1 polynomial and some other polynomial(s) (of degree 2 or 1). In either case, there is a polynomial of degree 1 as a factor. The two possible polynomials of degree 1 are $\boldsymbol{P_1 = x + 1}$ and $\boldsymbol{P_2 = x}$. If A is reducible, then either $\boldsymbol{P_1}$ or $\boldsymbol{P_2}$ is a factor of A. Notice $\boldsymbol{P_1}$ and $\boldsymbol{P_2}$ are respectively equal to zero when $\boldsymbol{x = -1}$ or $\boldsymbol{x = 0}$. If $\boldsymbol{A(x)}$ is reducible with $\boldsymbol{P_1}$ as a factor, then $\boldsymbol{A(-1) = 0}$. If $\boldsymbol{A(x)}$ is reducible with $\boldsymbol{P_2}$ as a factor, then $\boldsymbol{A(0) = 0}$. Otherwise $\boldsymbol{A(x)}$ is irreducible.

Let $\boldsymbol{A_1(x) = x^3 + x + 1}$, then
$\boldsymbol{A_1(0) = 0 + 0 + 1 = 1}$ and $\boldsymbol{A_1(-1) = -1 - 1 + 1 = -1}$

Let $\boldsymbol{A_2(x) = x^3 + x^2 + 1}$, then
$\boldsymbol{A_2(0) = 0 + 0 + 1 = 1}$ and $\boldsymbol{A_2(-1) = -1 + 1 + 1 = 1}$

Neither $\boldsymbol{A_1(x)}$ or $\boldsymbol{A_2(x)}$ have $\boldsymbol{P_1}$ or $\boldsymbol{P_2}$ as factors, and are therefore irreducible.

2.b.i)
Since $x^4 + x + 1 \equiv 0 \pmod{x^4 + x + 1}$
$x^4 \equiv x + 1 \pmod{x^4 + x + 1}$
$x^5 \equiv x^2 + x \pmod{x^4 + x + 1}$
$x^6 \equiv x^3 + x^2 \pmod{x^4 + x + 1}$

$f(x)g(x) = (x^2 + 1)(x^3 + x^2 + 1)$
$= x^5 + x^3 + x^4 + x^2 + x^2 + 1$
$= x^5 + x^3 + x^4 + 1$
$= (x^2 + x) + (x + 1) + x^3 + 1$
$= x^3 + x^2$

2.b.ii)
Since $x^4 + x + 1 \equiv 0 \pmod{x^4 + x + 1}$
$x^4 + x \equiv 1 \pmod{x^4 + x + 1}$
$x(x^3 + 1) \equiv 1 \pmod{x^4 + x + 1}$

So given $f(x) = x$, then $f^-1(x) = (x^3 + 1)$

d.i)
$y * (ay^3 + by^2 + cy + d)$
$\equiv ay^4 + by^3 + cy^2 + dy$
$\equiv by^3 + cy^2 + dy + a \pmod{y^4 + 1}$ (since $y^4 \equiv 1 \pmod{y^4 + 1}$)

d.ii)
For any $i \geq 0$, we can rewrite y^i as follows:

$y^i \equiv y^{j+4m} \pmod{y^4 + 1}$ where $j, m \in \mathbb{Z}$, $0 \leq j \leq 3$, and $m = \lfloor \frac{i}{4} \rfloor$

Note: $i = j + 4m \iff i - 4m = j \iff j = i \pmod 4$

Then $y^i \equiv y^{j+4m} \equiv y^j(y^4)^m \equiv y^j \pmod{y^4 + 1}$ (since $y^4 \equiv 1 \pmod{y^4 + 1}$)
Therefore, $y^i \equiv y^j \pmod{y^4 + 1}$ where $j \equiv i \pmod 4$ and $0 \leq j \leq 3$.

d.iii)
Let $b = ay^3 + by^2 + cy + d$ represent any 4-byte vector as polynomial.
Since we have d.ii, this can be split into 4 cases.

Case $y^i \equiv y^0 \pmod{y^4 + 1}$:
$y^i * b = y^0(ay^3 + by^2 + cy + d) \equiv ay^3 + by^2 + cy + d \pmod{y^4 + 1}$
This is a left circular shift of $j = 0$ bytes.

Case $y^i \equiv y^1 \pmod{y^4 + 1}$:
$y^i * b = y^1(ay^3 + by^2 + cy + d)$
$\equiv by^3 + cy^2 + dy + a$ (by d.i)
This is a left circular shift of $j = 1$ bytes.

Case $y^i \equiv y^2 \pmod{y^4 + 1}$:
$y^i * b = y^2(ay^3 + by^2 + cy + d)$

$= y^1(y^1(ay^3 + by^2 + cy + d))$
$\equiv y^1(by^3 + cy^2 + dy + a)$ (by d.i)
$\equiv cy^3 + dy^2 + ay + b \pmod{y^4 + 1}$ (by d.i)
This is a left circular shift of $j = 2$ bytes.

Case $y^i \equiv y^3 \pmod{y^4 + 1}$:
$y^i * b = y^3(ay^3 + by^2 + cy + d)$
$= y^1y^1(y^1(ay^3 + by^2 + cy + d))$
$\equiv y^1(y^1(by^3 + cy^2 + dy + a))$ (by d.i)
$\equiv y^1(cy^3 + dy^2 + ay + b)$ (by d.i)
$\equiv dy^3 + ay^2 + by + c \pmod{y^4 + 1}$ (by d.i)
This is a left circular shift of $j = 3$ bytes.

In all cases, it is shown that multiplying any 4-byte vector by y^i ($i \geq 0$) is a circular left shift of j bytes where $j \equiv i \pmod 4$ and $0 \leq j \leq 3$ (d.ii).

$\longrightarrow \mathcal{A}$nswer

Problem 3. Arithmetic with the constant polynomial of MixColumns in AES

3.a)
$c(1) = 1$
$c(2) = x$
$c(3) = x + 1$

b.i) $(01)(b) = 1(b_7x^7 ... + b_1x + b_0)$
$d_i = b_i$

b.ii)
$x^8 \equiv x^4 + x^3 + x + 1 \pmod{x^8 + x^4 + x^3 + x + 1}$
$(02)(b) = x(b_7x^7 + ... + b_1x + b_0)$
$= b_7x^8 + b_6x^7 ... + b_1x^2 + b_0x)$
$= b_7(x^4 + x^3 + x + 1) + b_6x^7 + ... + b_1x^2 + b_0x)$
$d = b_6x^7 + b_5x^6 + b_4x^5 + (b_7 + b_3)x^4 + (b_7 + b_2)x^3 + b_1x^2 + (b_7 + b_0)x + b_7$
$d_7 = b_6$
$d_6 = b_5$
$d_5 = b_4$
$d_4 = b_7 + b_3$
$d_3 = b_7 + b_2$
$d_2 = b_1$
$d_1 = b_7 + b_0$
$d_0 = b_7$

b.iii)

$$\begin{aligned}
&\mathbf{(03)}(\boldsymbol{b}) = (\boldsymbol{x}+1)(\boldsymbol{b_7 x^7} + \ldots + \boldsymbol{b_1 x} + \boldsymbol{b_0})\\
&= (b_7x^8 + b_6x^7 + \ldots + b_1x^2 + b_0x) + (b_7x^7 + \ldots + b_1x + b_0)\\
&= b_7(x^4 + x^3 + x + 1) + (b_6 + b_7)x^7 + \ldots + (b_0 + b_1)x + b_0)\\
&d_7 = b_6 + b_7\\
&d_6 = b_5 + b_6\\
&d_5 = b_4 + b_5\\
&d_4 = b_3 + b_4 + b_7\\
&d_3 = b_2 + b_3 + b_7\\
&d_2 = b_1 + b_2\\
&d_1 = b_0 + b_1 + b_7\\
&d_0 = b_0 + b_7
\end{aligned}$$

c.i)

$$\begin{aligned}
&y^4 \equiv 1 \pmod{y^4+1}\\
&y^5 \equiv y \pmod{y^4+1}\\
&y^6 \equiv y^2 \pmod{y^4+1}
\end{aligned}$$

$$\begin{aligned}
&t(y) = c(y)s(y) \pmod{y^4+1}\\
&= [(03)y^3 + (01)y^2 + (01)y + (02)](s_3y^3 + s_2y^2 + s_1y + s_0) \pmod{y^4+1}\\
&= (03)(s_3y^6 + s_2y^5 + s_1y^4 + s_0y^3)\\
&+(01)(s_3y^5 + s_2y^4 + s_1y^3 + s_0y^2)\\
&+(01)(s_3y^4 + s_2y^3 + s_1y^2 + s_0y)\\
&+(02)(s_3y^3 + s_2y^2 + s_1y + s_0) \pmod{y^4+1}
\end{aligned}$$

$$\begin{aligned}
&= (03)s_3y^6\\
&+((03)s_2 + (01)s_3)y^5\\
&+((03)s_1 + (01)s_2 + (01)s_3)y^4\\
&+((03)s_0 + (01)s_1 + (01)s_2 + (02)s_3)y^3\\
&+((01)s_0 + (01)s_1 + (02)s_2)y^2\\
&+((01)s_0 + (02)s_1)y\\
&+(02)s_0 \pmod{y^4+1}
\end{aligned}$$

$$\begin{aligned}
&= (03)s_3y^2\\
&+((03)s_2 + (01)s_3)y\\
&+((03)s_1 + (01)s_2 + (01)s_3)\\
&+((03)s_0 + (01)s_1 + (01)s_2 + (02)s_3)y^3\\
&+((01)s_0 + (01)s_1 + (02)s_2)y^2\\
&+((01)s_0 + (02)s_1)y\\
&+(02)s_0 \pmod{y^4+1}
\end{aligned}$$

$$\begin{aligned}
&= ((03)s_0 + (01)s_1 + (01)s_2 + (02)s_3)y^3\\
&+((01)s_0 + (01)s_1 + (02)s_2 + (03)s_3)y^2\\
&+((01)s_0 + (02)s_1 + (03)s_2 + (01)s_3)y\\
&+((02)s_0 + (03)s_1 + (01)s_2 + (01)s_3) \pmod{y^4+1}
\end{aligned}$$

c.ii)

$$\boldsymbol{C} = \begin{bmatrix} \boldsymbol{t_0} \\ \boldsymbol{t_1} \\ \boldsymbol{t_2} \\ \boldsymbol{t_3} \end{bmatrix} = \begin{bmatrix} \mathbf{2} & \mathbf{3} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{3} & \mathbf{1} & \mathbf{1} & \mathbf{2} \end{bmatrix}$$

⟶ Answer

Problem 4. Error propagation in block cipher modes

Let $\boldsymbol{C_i}$ denote the encryption of the i-th message block, $\boldsymbol{M_i}$.
Let $\boldsymbol{P_i}$ denote the plaintext obtained from the decryption of $\boldsymbol{C_i}$.

a.i)
ECB: Only $\boldsymbol{P_i}$ is affected since the decryption of each block is just a simple block substitution(independent of each other).
ii)
CBC: $\boldsymbol{P_i}$ and $\boldsymbol{P_{i+1}}$ are affected since $\boldsymbol{P_{i+1}}$ is the result of $\boldsymbol{C_i} \oplus \boldsymbol{C_{i+1}}$ but $\boldsymbol{P_{i+2}}$ is the result of $\boldsymbol{C_{i+1}} \oplus \boldsymbol{C_{i+2}}$(does not depend on $\boldsymbol{C_i}$).
iii)
OFB: Only $\boldsymbol{P_i}$ is affected since any given decryption state has been generated exclusively from the previous state (which eventually originates from the IV).
iv)
CFB: Only $\boldsymbol{P_i}$ and $\boldsymbol{P_{i+1}}$ are affected. $\boldsymbol{C_i}$ is involved in decrypting $\boldsymbol{P_{i+1}}$ (when it gets combined with the key to create the next cipher block) but $\boldsymbol{C_{i+1}}$ will take its place (in creating the next cipher block) for decrypting $\boldsymbol{P_{i+2}}$.
v)
CTR: Only $\boldsymbol{P_i}$ is affected since $\boldsymbol{CTR_i}$ (the source of the output block that gets XORed with $\boldsymbol{C_i}$) is simply an independent counter value.

b)
The error happens before any encryption takes place, so the entire plaintext would be encrypted and decrypted normally, as if the plaintext had no errors in it. Thus, only $\boldsymbol{M_i}$ would be affected.

⟶ Answer

Submitted by Brian Yee - 00993104 on October 28, 2016.