

HOME WORK #2

Problem	Marks
1	
2	
3	
4	
5	
6	
7	
Total	

Problem 1. Conditional entropy

1.a)

$$H(M|C) = \sum_{c \in C} p(C) \sum_{m \in M} p(M|C) \log_2\left(\frac{1}{p(M|C)}\right)$$

$$H(M|C) = \sum p(C) \sum p(M|C) \log_2\left(\frac{1}{p(M|C)}\right)$$

$$= 4 * \frac{1}{4} \left(\frac{1}{2} \log_2(2) + \frac{1}{2} \log_2(2) \right)$$

$$= 1$$

1.b)

$$H(M|C) = \sum p(C) \sum p(M|C) \log_2\left(\frac{1}{p(M|C)}\right)$$

Since the cryptosystem provides perfect secrecy, $p(M|C) = p(M)$.

$$= \sum p(C) \sum p(M) \log_2\left(\frac{1}{p(M)}\right)$$

We know $\sum p(M) \log_2\left(\frac{1}{p(M)}\right) = \log_2\left(\frac{1}{p(M)}\right)$, when a cryptosystem provides perfect secrecy.

$$= \sum p(C) \log_2 \left(\frac{1}{p(M)} \right)$$

With perfect secrecy, every M is equiprobable, so every C is equiprobable. Since $|C| = |M|$ (as every unique C comes from encrypting some unique M), so we have $p(C) = p(M)$.

Thus,

$$= \sum p(M) \log_2 \left(\frac{1}{p(M)} \right) \\ = H(M)$$

1.c)

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

→ Answer

Problem 2. Binary polynomial arithmetic

2.a.i)

$$\begin{aligned} x^3 \\ x^3 + 1 \\ x^3 + x \\ x^3 + x + 1 \\ x^3 + x^2 \\ x^3 + x^2 + 1 \\ x^3 + x^2 + x \\ x^3 + x^2 + x + 1 \end{aligned}$$

2.a.ii)

$$\begin{aligned} x^3 &= x * x * x \\ x^3 + 1 &= (x + 1)(x^2 - x + 1) \\ x^3 + x &= x(x^2 + 1) \\ x^3 + x + 1 &= \text{irreducible} \\ x^3 + x^2 &= x^2(x + 1) \\ x^3 + x^2 + 1 &= \text{irreducible} \\ x^3 + x^2 + x &= x(x^2 + x + 1) \\ x^3 + x^2 + x + 1 &= (x + 1)(x^2 + 1) \end{aligned}$$

2.a.iii)

Let $A(x)$ be a degree 3 polynomial. If $A(x)$ is reducible, then it must be 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 $P_1 = x + 1$ and $P_2 = x$. If A is reducible, then either P_1 or P_2 is a factor of A. Notice P_1 and P_2 are respectively equal to zero when $x = -1$ or $x = 0$. If $A(x)$ is reducible with P_1 as a factor, then $A(-1) = 0$. If $A(x)$ is reducible with P_2 as a factor, then $A(0) = 0$. Otherwise $A(x)$ is irreducible.

Let $A_1(x) = x^3 + x + 1$, then

$$A_1(0) = 0 + 0 + 1 = 1 \text{ and } A_1(-1) = -1 - 1 + 1 = -1$$

Let $A_2(x) = x^3 + x^2 + 1$, then

$$A_2(0) = 0 + 0 + 1 = 1 \text{ and } A_2(-1) = -1 + 1 + 1 = 1$$

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

2.b.i)

$$\text{Since } x^4 + x + 1 \equiv 0 \pmod{x^4 + x + 1}$$

$$x^4 \equiv x + 1 \pmod{x^4 + x + 1}$$

$$x^5 \equiv x^2 + x \pmod{x^4 + x + 1}$$

$$x^6 \equiv x^3 + x^2 \pmod{x^4 + x + 1}$$

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

$$= x^5 + x^3 + x^4 + x^2 + x^2 + 1$$

$$= x^5 + x^3 + x^4 + 1$$

$$= (x^2 + x) + (x + 1) + x^3 + 1$$

$$= x^3 + x^2$$

2.b.ii)

$$\text{Since } x^4 + x + 1 \equiv 0 \pmod{x^4 + x + 1}$$

$$x^4 + x \equiv 1 \pmod{x^4 + x + 1}$$

$$x(x^3 + 1) \equiv 1 \pmod{x^4 + x + 1}$$

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

d.i)

$$y * (ay^3 + by^2 + cy + d)$$

$$\equiv ay^4 + by^3 + cy^2 + dy$$

$$\equiv by^3 + cy^2 + dy + a \pmod{y^4 + 1} \quad (\text{since } y^4 \equiv 1 \pmod{y^4 + 1})$$

d.ii)

$$\text{Since } 1 \equiv y^4 \pmod{y^4 + 1},$$

$$y^i \equiv y^i y^4 \equiv y^{i+4} \equiv y^j \pmod{y^4 + 1} \text{ where } j \equiv i + 4 \equiv i \pmod{4} \text{ and } 0 \leq j \leq 3.$$

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 $y^i \equiv y^1 \pmod{y^4 + 1}$:

$$y^i * b = y^1(ay^3 + by^2 + cy + d)$$

$$\equiv by^3 + cy^2 + dy + a \quad (\text{by d.i})$$

This is a left circular shift of $j = 1$ bytes.

Case $y^i \equiv y^2 \pmod{y^4 + 1}$:

$$\begin{aligned} y^i * b &= y^2(ay^3 + by^2 + cy + d) \\ &= y^1(y^1(ay^3 + by^2 + cy + d)) \\ &\equiv y^1(by^3 + cy^2 + dy + a) \quad (\text{by d.i}) \\ &\equiv cy^3 + dy^2 + ay + b \pmod{y^4 + 1} \quad (\text{by d.i}) \end{aligned}$$

This is a left circular shift of $j = 2$ bytes.

Case $y^i \equiv y^3 \pmod{y^4 + 1}$:

$$\begin{aligned} y^i * b &= y^3(ay^3 + by^2 + cy + d) \\ &= y^1y^1(y^1(ay^3 + by^2 + cy + d)) \\ &\equiv y^1(y^1(by^3 + cy^2 + dy + a)) \quad (\text{by d.i}) \\ &\equiv y^1(cy^3 + dy^2 + ay + b) \quad (\text{by d.i}) \\ &\equiv dy^3 + ay^2 + by + c \pmod{y^4 + 1} \quad (\text{by d.i}) \end{aligned}$$

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).

→ Answer

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

3.a)

$$\begin{aligned} c(1) &= 1 \\ c(2) &= x \\ c(3) &= x + 1 \end{aligned}$$

$$\begin{aligned} \text{b.i) } (01)(b) &= 1(b_7x^7 + \dots + b_1x + b_0) \\ d_i &= b_i \end{aligned}$$

b.ii)

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

b.iii)

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

c.i)

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

$$\begin{aligned}
t(y) &= c(y)s(y) \pmod{y^4 + 1} \\
&= [(03)y^3 + (01)y^2 + (01)y + (02)](s_3y^3 + s_2y^2 + s_1y + s_0) \pmod{y^4 + 1} \\
&= (03)(s_3y^6 + s_2y^5 + s_1y^4 + s_0y^3) \\
&\quad + (01)(s_3y^5 + s_2y^4 + s_1y^3 + s_0y^2) \\
&\quad + (01)(s_3y^4 + s_2y^3 + s_1y^2 + s_0y) \\
&\quad + (02)(s_3y^3 + s_2y^2 + s_1y + s_0) \pmod{y^4 + 1} \\
&= (03)s_3y^6 \\
&\quad + ((03)s_2 + (01)s_3)y^5 \\
&\quad + ((03)s_1 + (01)s_2 + (01)s_3)y^4 \\
&\quad + ((03)s_0 + (01)s_1 + (01)s_2 + (02)s_3)y^3 \\
&\quad + ((01)s_0 + (01)s_1 + (02)s_2)y^2 \\
&\quad + ((01)s_0 + (02)s_1)y \\
&\quad + (02)s_0 \pmod{y^4 + 1} \\
&= (03)s_3y^2 \\
&\quad + ((03)s_2 + (01)s_3)y \\
&\quad + ((03)s_1 + (01)s_2 + (01)s_3) \\
&\quad + ((03)s_0 + (01)s_1 + (01)s_2 + (02)s_3)y^3 \\
&\quad + ((01)s_0 + (01)s_1 + (02)s_2)y^2 \\
&\quad + ((01)s_0 + (02)s_1)y \\
&\quad + (02)s_0 \pmod{y^4 + 1} \\
&= ((03)s_0 + (01)s_1 + (01)s_2 + (02)s_3)y^3 \\
&\quad + ((01)s_0 + (01)s_1 + (02)s_2 + (03)s_3)y^2 \\
&\quad + ((01)s_0 + (02)s_1 + (03)s_2 + (01)s_3)y \\
&\quad + ((02)s_0 + (03)s_1 + (01)s_2 + (01)s_3) \pmod{y^4 + 1}
\end{aligned}$$

c.ii)

$$C = \begin{bmatrix} 3 & 1 & 1 & 2 \\ 1 & 1 & 2 & 3 \\ 1 & 2 & 3 & 1 \\ 2 & 3 & 1 & 1 \end{bmatrix}$$

→ Answer

Problem 4. Error propagation in block cipher modes

Let C_i denote the encryption of the i -th message block, M_i .

Let P_i denote the plaintext obtained from the decryption of C_i .

a.i)

ECB: Only P_i is affected since the decryption of each block is just a simple block substitution (independent of each other).

ii)

CBC: P_i and P_{i+1} are affected since P_{i+1} is the result of $C_i \oplus C_{i+1}$ but P_{i+2} is the result of $C_{i+1} \oplus C_{i+2}$ (does not depend on C_i).

iii)

OFB: Only 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: All plaintext blocks starting from P_i are affected since the C_i will be added to the register for encrypting P_{i+1} into C_{i+1} . As a result, even if the plaintext blocks after P_i are error-free, they will still be encrypted using ciphertext that was created from the errant plaintext block, P_i .

v)

CTR: Only P_i is affected since CTR_i (the source of the output block that gets XORed with 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 M_i would be affected.

→ Answer

Submitted by Brian Yee - 00993104 on October 27, 2016.