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

October 26, 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)
$\boldsymbol{H(M|C) = \sum p(C) \sum p(M|C) log_2(\frac{1}{p(M|C)})}$

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

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

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

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

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

Thus,

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

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

$\longrightarrow \mathcal{A}$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 $\boldsymbol{x^4 + x + 1 \equiv 0 \pmod{x^4 + x + 1}}$

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

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

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

$\boldsymbol{f(x)g(x) = (x^2 + 1)(x^3 + x^2 + 1)}$

$\boldsymbol{= x^5 + x^3 + x^4 + x^2 + x^2 + 1}$

$\boldsymbol{= x^5 + x^3 + x^4 + 1}$

$\boldsymbol{= (x^2 + x) + (x + 1) + x^3 + 1}$

$\boldsymbol{= x^3 + x^2}$

2.b.ii)

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

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

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

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

d.i)

$\boldsymbol{y * [ay^3 + by^2 + cy + d)]}$

$\boldsymbol{= ay^4 + by^3 + cy^2 + dy}$

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

d.ii)

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

$\boldsymbol{y^i \equiv y^i y^4 \equiv y^{i+4} \equiv y^j \pmod{y^4 + 1}}$ where $\boldsymbol{j \equiv i + 4 \equiv i \pmod{4}}$.

d.iii)

Let $\boldsymbol{ay^3 + by^2 + cy + d}$ represent any 4-byte vector as polynomial.

Base case:

$\boldsymbol{i = 0}$: $\boldsymbol{y^0(ay^3 + by^2 + cy + d) = ay^3 + by^2 + cy + d}$

No bytes have been shifted (ie. a circular left shift of 0 bytes). Using the proof from *d.ii* we get that this is a shift of $\boldsymbol{j = 0}$ bytes.

$\boldsymbol{i = 1}$: $\boldsymbol{y^1(ay^3 + by^2 + cy + d)}$ This is a left circular shift of $\boldsymbol{j = 1}$ bytes (proven by d.i and d.ii).

Induction Hypothesis:

Assume for $\boldsymbol{i \geq 0}$ that $\boldsymbol{y^i(ay^3 + by^2 + cy + d) = ay^{3+i} + by^{2+i} + cy^{1+i} + dy^i}$ is a left circular shift of $\boldsymbol{j}$ bytes where $\boldsymbol{j \equiv i \pmod{4}}$ and $\boldsymbol{0 \leq j \leq 3}$.

Suppose $\boldsymbol{k} \in \mathbb{Z}$ and $\boldsymbol{k \geq 1}$.

$\boldsymbol{y^{k+1}(ay^3 + by^2 + cy + d) = y^k(y^1(ay^3 + by^2 + cy + d))}$
$\boldsymbol{= y^k(ay^{3+1} + by^{2+1} + cy^{1+1} + dy^1)}$
$\boldsymbol{= ay^{3+(k+1)} + by^{2+(k+1)} + cy^{1+(k+1)} + dy^{k+1}}$ (by IH)

Since $\boldsymbol{k + 1 \geq 0}$ and $\boldsymbol{y^{k+1} = y^j}$ where $\boldsymbol{j \equiv k + 1 \pmod{4}}$ and $\boldsymbol{0 \leq j \leq 3}$ (proof d.ii), the multiplication of any 4-byte vector with $\boldsymbol{y^{k+1}}$ is a left circular shift of $\boldsymbol{j}$ bytes.

⟶ $\mathcal{A}$nswer

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

3.a)
$\boldsymbol{c(1) = 1}$
$\boldsymbol{c(2) = x}$
$\boldsymbol{c(3) = x + 1}$

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

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

b.iii)
$\boldsymbol{(03)(b) = (x + 1)(b_7x^7 + ... + b_1x + b_0)}$
$\boldsymbol{= (b_7x^8 + b_6x^7 + ... + b_1x^2 + b_0x) + (b_7x^7 + ... + b_1x + b_0)}$
$\boldsymbol{= b_7(x^4 + x^3 + x + 1) + (b_6 \oplus b_7)x^7 + ... + (b_0 \oplus b_1)x + b_0)}$
$\boldsymbol{d_7 = b_6 \oplus b_7}$
$\boldsymbol{d_6 = b_5 \oplus b_6}$
$\boldsymbol{d_5 = b_4 \oplus b_5}$
$\boldsymbol{d_4 = b_3 \oplus b_4 \oplus b_7}$
$\boldsymbol{d_3 = b_2 \oplus b_3 \oplus b_7}$

$d_2 = b_1 \oplus b_2$
$d_1 = b_0 \oplus b_1 \oplus b_7$
$d_0 = b_0 \oplus b_7$

c.i)
$y^4 \equiv 1 \pmod{y^4+1}$
$y^5 \equiv y \pmod{y^4+1}$
$y^6 \equiv y^2 \pmod{y^4+1}$

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

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

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

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

c.ii)

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

$\longrightarrow \mathcal{A}$nswer

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 $\boldsymbol{C_i}$ will be combined with $\boldsymbol{P_{i+1}}$ via an exclusive-OR.
iii)
OFB: Only $\boldsymbol{P_i}$ is affected since any given decryption state has been generated exclusively from the previous state (eventually originating from the IV).
iv)
CFB: When using only one register, $\boldsymbol{P_i}$ and $\boldsymbol{P_{i+1}}$ are affected since only the last $\boldsymbol{k}$ previous ciphertext blocks (in this case $\boldsymbol{k = 1}$) are kept in the register for decryption.
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)
All message blocks following (and including) $\boldsymbol{M_i}$ are affected, since in CBC mode $\boldsymbol{C_i}$ is used in the encryption of $\boldsymbol{C_{i+1}}$ (and then $\boldsymbol{C_{i+1}}$ gets used when encrypting $\boldsymbol{C_{i+2}}$ and so on).

$\longrightarrow$ $\mathcal{A}$nswer

Submitted by Brian Yee - 00993104 on October 26, 2016.