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

October 23, 2016

HOME WORK #2

Problem	Marks
1	
2	
3	
4	
5	
6	
7	
Total	

Problem 1. Conditional entropy

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

1.b)
Since the cryptosystem provides perfect secrecy, $p(x|y) = p(x)$.
Then $p(M) = \frac{1}{|M|}$ (each M is equiprobable)

$$\sum p(M)log_2(\frac{1}{p(M)})$$
$$= \frac{1}{|M|}log_2(\frac{1}{p(M)}) + \frac{1}{|M|}log_2(\frac{1}{p(M)}) + ... + \frac{1}{|M|}log_2(\frac{1}{p(M)}) \text{ (}|M| \text{ total terms)}$$
$$= |M| * \frac{1}{|M|}log_2(\frac{1}{p(M)})$$
$$= log_2(\frac{1}{p(M)})$$

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

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,

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

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

$\longrightarrow \mathcal{A}$nswer

Problem 2. Binary polynomial arithmetic

2.a.i)
x^3
$x^3 + 1$
$x^3 + x$
$x^3 + x + 1$
$x^3 + x^2$
$x^3 + x^2 + 1$
$x^3 + x^2 + x$
$x^3 + x^2 + x + 1$

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

2.a.iii)
Let $A(x)$ be a degree 3 polynomial. If $A(x)$ 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 $P_1 = x + 1$ 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
$\quad A_1(0) = 0 + 0 + 1 = 1$ and $A_1(-1) = -1 - 1 + 1 = -1$

Let $A_2(x) = x^3 + x^2 + 1$, then
$\quad A_2(0) = 0 + 0 + 1 = 1$ 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)
Since $x^4 + x + 1 \equiv 0 \pmod{x^4 + x + 1}$
$x^4 \equiv 1 + x \pmod{x^4 + x + 1}$
$x^5 \equiv x + x^2 \pmod{x^4 + x + 1}$

$f(x)g(x) = (x^2 + 1)(x^3 + x^2 + 1)$
$= x^5 + x^3 + x^4 + x^2 + x^2 + 1$
$= x^5 + x^4 + x^3 + 2x^2 + 1$
$= (x + x^2) + (1 + x) + x^3 + 2x^2 + 1$
$= x^3 + 3x^2 + 2x + 2$
$= x^3 + x^2$
is GF2 4 binary? i think so
ii)

d)

$\longrightarrow$ $\mathcal{A}$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) $(01)(b) = 1(b_7 x^7 ... + b_1 x + b_0)$
$d_i = b_i$

b.ii)
$x^8 \equiv x^4 + x^3 + x + 1 \pmod{x^8 + x^4 + x^3 + x + 1}$
$(02)(b) = x(b_7 x^7 + ... + b_1 x + b_0)$
$= b_7 x^8 + b_6 x^7 ... + b_1 x^2 + b_0 x)$
$= b_7 (x^4 + x^3 + x + 1) + b_6 x^7 + ... + b_1 x^2 + b_0 x)$
$d = b_6 x^7 + b_5 x^6 + b_4 x^5 + (b_7 + b_3)x^4 + (b_7 + b_2)x^3 + b_1 x^2 + (b_7 + b_0)x + b_7$
$d_7 = b_6 x^7$

$d_6 = b_5 x^6$
$d_5 = b_4 x^5$
$d_4 = (b_7 \oplus b_3)x^4$
$d_3 = (b_7 \oplus b_2)x^3$
$d_2 = b_1 x^2$
$d_1 = (b_7 \oplus b_0)x$
$d_0 = b_7$

b.iii)
$(03)(b) = (x + 1)(b_7 x^7 + ... + b_1 x + b_0)$
$= (b_7 x^8 + b_6 x^7 + ... + b_1 x^2 + b_0 x) + (b_7 x^7 + ... + b_1 x + b_0)$
$= b_7(x^4 + x^3 + x + 1) + (b_6 \oplus b_7)x^7 + ... + (b_0 \oplus b_1)x + b_0)$
$d_7 = b_6 \oplus b_7$
$d_6 = b_5 \oplus b_6$
$d_5 = b_4 \oplus b_5$
$d_4 = b_3 \oplus b_4 \oplus b_7$
$d_3 = b_2 \oplus b_3 \oplus b_7$
$d_2 = b_1 \oplus b_2$
$d_1 = b_0 \oplus b_1 \oplus b_7$
$d_0 = b_0 \oplus b_7$

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

$t(x) = c(y)s(y) \pmod{y^4 + 1}$
$= [(03)y^3 + (01)y^2 + (01)y + (02)](s_3 y^3 + s_2 y^2 + s_1 y + s_0) \pmod{y^4 + 1}$
$= (03)(s_3 y^6 + s_2 y^5 + s_1 y^4 + s_0 y^3)$
$+(01)(s_3 y^5 + s_2 y^4 + s_1 y^3 + s_0 y^2)$
$+(01)(s_3 y^4 + s_2 y^3 + s_1 y^2 + s_0 y)$
$+(02)(s_3 y^3 + s_2 y^2 + s_1 y + s_0)$

$= (03)s_3 y^6$
$+((03)s_2 + (01)s_3)y^5$
$+((03)s_1 + (01)s_2 + (01)s_3)y^4$
$+((03)s_0 + (01)s_1 + (01)s_2 + (02)s_3)y^3$
$+((01)s_0 + (01)s_1 + (02)s_2)y^2$
$+((01)s_0 + (02)s_1)y$
$+(02)s_0$

$= (03)s_3 y^2$
$+((03)s_2 + (01)s_3)y$
$+((03)s_1 + (01)s_2 + (01)s_3)$
$+((03)s_0 + (01)s_1 + (01)s_2 + (02)s_3)y^3$
$+((01)s_0 + (01)s_1 + (02)s_2)y^2$
$+((01)s_0 + (02)s_1)y$
$+(02)s_0$

$$= ((03)s_0 + (01)s_1 + (01)s_2 + (02)s_3)y^3$$
$$+((01)s_0 + (01)s_1 + (02)s_2 + (03)s_3)y^2$$
$$+((01)s_0 + (02)s_1 + (03)s_2 + (01)s_3)y$$
$$+((02)s_0 + (03)s_1 + (01)s_2 + (01)s_3)$$

$$t(x) = t_3 y^3 + t_2 y^2 + t_1 y + t_0$$

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

a)
i)
ECB: Only P_i is affected since each block is handled independently.
ii)
CBC: P_i and P_{i+1} are affected since any C_i block only affects the plaintext of the block following it.
iii)
OFB: Only P_i is affected since OFB does not use C_i in the decryption of P_{i+1} (only during encryption)...or rather it relies on purely on the IV.
iv)
CFB: P_i to $P_i + k$ are affected since only the last k ciphertext blocks are kept in the register for decrypting.
v)
CTR: Only P_i is affected CTR_i is simply a counter and is not dependent on the value of C_i.

b)
ECB: Only P_i
CBC: All of them
OFB: All of them
CFB: Only P_i
CTR: Only P_i

$\longrightarrow \mathcal{A}$nswer

Submitted by Brian Yee - 00993104 on October 23, 2016.