The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/COMP6360 Data Security

Week 2 Workshop Solutions – 7th and 8th March 2019

1. Apply Chinese Remainder Theorem to find x in the range [0,59] such that

x mod 4 = 3
x mod 3 = 2
x mod 5 = 4

Solution:
Chinese Remainder Theorem: Let $d_1, d_2, ..., d_t$ be pairwise relatively prime, and let $n = d_1 \times d_2 \times \cdots \times d_t$. Then the system of equations

$$x \bmod d_i = x_i, i = 1, \ldots, t$$

has a common solution x in the range $[0, n-1]$.The common solution is

$$x = \left(\sum_{i=1}^{t} \frac{n}{d_i} y_i x_i \right) \bmod n$$

where y_i is a solution of $\frac{n}{d_i} y_i \bmod d_i = 1, i = 1, \ldots, t$.

We have $x_1 = 3, x_2 = 2, x_3 = 4$. Further, we have $d_1 = 4, d_2 = 3, d_3 = 5$ and so $n = 4 \times 3 \times 5$.

We first need to find y_1, y_2 and y_3 such that

$$\frac{60}{4} y_1 \bmod 4 = 1$$
$$\frac{60}{3} y_2 \bmod 3 = 1$$
$$\frac{60}{5} y_3 \bmod 5 = 1$$

We get:

$$15 y_1 \bmod 4 = 1$$
$$20 y_2 \bmod 3 = 1$$
$$12 y_3 \bmod 5 = 1$$

that is,

$$3y_1 \bmod 4 = 1$$
$$2y_2 \bmod 3 = 1$$
$$2y_3 \bmod 5 = 1$$

We get $y_1 = 3, y_2 = 2$ and $y_3 = 3$.

We now get the solution:

$$x = (15\times 3\times 3 + 20\times 2\times 2 + 12\times 3\times 4) \bmod 60 =$$
$$((15\times 3\times 3) \bmod 60 + (20\times 2\times 2) \bmod 60 + (12\times 3\times 4) \bmod 60) \bmod 60 =$$
$$(15 + 20 + 24) \bmod 60 = 59$$

2. Using Chinese Remainder Theorem solve for x in the range [0, n-1].

a) 5x mod 17 = 1
b) 19x mod 26 = 1
c) 17x mod 100 = 1
d) 2x mod 57 =1

Solution:

a) $5x \bmod 17 = 1$

As 17 is a prime number, we cannot apply Chinese Remainder Theorem. We can use Extended Euclid's Algorithm, or Euler's Totient function (you should do both of these for practice), but since the modulus (17) is fairly small, we can simply apply a brute force strategy to find the multiplicative inverse:

5×1 mod 17 = 5
5×2 mod 17 = 10
5×3 mod 17 = 15
5×4 mod 17 = 3
5×5 mod 17 = 8
5×6 mod 17 = 13
5×7 mod 17 = 1

Thus the multiplicative inverse of 5 modulo 17 is 7.

b) $19x \bmod 26 = 1$

We have

26 = 2×13, d1 = 2, d2 = 13

19x1 mod 2 = 1 → x1 mod 2 = 1, x1 = 1
19x2 mod 13 = 1 → 6x2 mod 13 = 1, x2 = 11

x mod 2 = 1
x mod 13 = 11

We now need to find y_1 and y_2 such that

$$(26/2)\ y_1 \bmod 2 = 1$$
$$(26/13)\ y_2 \bmod 13 = 1$$

$$13y_1 \bmod 2 = y_1 \bmod 2 = 1$$
$$2y_2 \bmod 13 = 1$$

We get $y_1 = 1$ and $y_2 = 7$.

We now get the solution

$$x = (13\times1\times1 + 2\times7\times11) \bmod 26 = 11$$

Thus the multiplicative inverse of 19 modulo 26 is 11.

c) $17x \bmod 100 = 1$

We have

$$100 = 2^2\times5^2,\ d_1 = 2^2,\ d_2 = 5^2$$

$$17x1 \bmod 4 = 1 \rightarrow x1 \bmod 4 = 1,\ x1 = 1$$
$$17x2 \bmod 25 = 1 \rightarrow x2 = 3$$

$$x \bmod 4 = 1$$
$$x \bmod 25 = 3$$

We now need to find y1 and y2 such that

$$(100/4)\ y_1 \bmod 4 = 1$$
$$(100/25)\ y_2 \bmod 25 = 1$$

$$25y_1 \bmod 4 = 1 \rightarrow y_1 \bmod 4 = 1$$
$$4y_2 \bmod 25 = 1$$

We get $y_1 = 1$ and $y_2 = 19$.

We now get the solution

$$x = (25\times1\times1 + 4\times19\times3) \bmod 100 = 53$$

Thus the multiplicative inverse of 17 modulo 100 is 53.

d) $2x \bmod 57 = 1$

We have

$57 = 3 \times 19$, $d_1 = 3$, $d_2 = 19$

$2x1 \bmod 3 = 1 \rightarrow x_1 = 2$
$2x2 \bmod 19 = 1 \rightarrow x_2 = 10$

$x \bmod 3 = 2$
$x \bmod 19 = 10$

We now need to find y1 and y2 such that

$(57/3)\, y_1 \bmod 3 = 1$
$(57/19)\, y_2 \bmod 19 = 1$

$19y_1 \bmod 3 = 1 \rightarrow y_1 \bmod 3 = 1$
$3y_2 \bmod 19 = 1$

We get $y_1 = 1$ and $y_2 = 13$.
We now get the solution

$x = (19\times1\times2 + 3\times13\times10) \bmod 57 = 29$

Thus the multiplicative inverse of 2 modulo 57 is 29.

3. Using extended Euclid's algorithm, find the solution to the equation 17x mod 100 = 1 in the range [0, 99].

<u>Solution:</u>
We need to find the multiplicative inverse of 17 mod 100 using extended Euclid's algorithm. We already know that the result is 53 (see exercise 2.c).

```
Algorithm inv(a,n)
begin
        g0 := n; g1 := a; u0 = 1; v0 := 0; u1 := 0; v1 := 1; i := 1;
        while gi ≠ 0 do "gi = ui × n + vi × a"
                begin
                        y := gi-1 div gi ; gi+1 := gi-1 - y × gi ;
                        ui+1 := ui-1 - y × ui ; vi+1 := vi-1 - y × vi ;
                        i := i + 1
                end;
        x := vi -1
        if x ≥ 0 then inv := x else inv := x+n
end
```

i	y	u	v	g
0		1	0	100
1		0	1	17
2	5	1	-5	15
3	1	-1	6	2
4	7	8	**-47**	1
5	2	-17	100	0

$x = -47 \bmod 100 = 53$ (Remember when $x_0<0$ add n)

Note that u_4 gives is the multiplicative inverse of 100 mod 17, that is, the solution of 100y mod 17 = 1. Checking:

$y=u_4 = 8 \bmod 17$,

$100 \times 8 \bmod 17 = 15 \times 8 \bmod 17 = 120 \bmod 17 = 1$

4. Using Euler's theorem and fast exponentiation, solve the following equation for x in the range [0, n-1].

a) 5x mod 17 = 1
b) 19x mod 26 = 1
c) 17x mod 100 = 1
d) 2x mod 57 =1

Solution:

a) We can use Euler's theorem:

$5^{\Phi(17)-1} \bmod 17 = x$

$5^{16-1} \bmod 17 = x$

Using fast exponentiation we get

$x = 5^{15} \bmod 17 = 5\times5^{14} \bmod 17$
$= 5\times25^7 \bmod 17 = 5\times8^7 \bmod 17$
$= 5\times8\times8^6 \bmod 17 = 6\times8^6 \bmod 17$
$= 6\times64^3 \bmod 17 = 6 \times 13^3 \bmod 17$
$= 6\times13\times13^2 \bmod 17 = 10\times13^2 \bmod 17$
$= 10\times16 \bmod 17 = \mathbf{7}$

b) Euler's theorem:

$19^{\Phi(26)-1} \bmod 26 = x$

$26 = 2\times13$

$\Phi(26) = (2-1) \times (13-1) = 12$

$x = 19^{12-1} \bmod 26 = 19^{11} \bmod 26$

$= 19 \times 19^{10} \bmod 26$
$= 19 \times 361^5 \bmod 26 = 19 \times 23^5 \bmod 26$
$= 19 \times 23 \times 23^4 \bmod 26 = 21 \times 23^4 \bmod 26$
$= 21 \times 9^2 \bmod 26$
$= 21 \times 81 \bmod 26 = 21 \times 3 \bmod 26 = 63 \bmod 26 =$ **11**

c) $100 = 2^2 \times 5^2$
$\Phi(100) = (2\text{-}1) \times 2 \times (5\text{-}1) \times 5 = 40$
$x = 17^{39} \bmod 100 = 17 \times 17^{38} \bmod 100 = 17 \times (17^2)^{19} \bmod 100 =$
$= 17 \times 289^{19} \bmod 100 =$
$= 17 \times 89^{19} \bmod 100 = 17 \times 89 \times 89^{18} \bmod 100 = 13 \times (89^2)^9 \bmod 100 =$
$= 13 \times 7921^9 \bmod 100 = 13 \times 21^9 \bmod 100 = 13 \times 21 \times 21^8 \bmod 100 =$
$= 73 \times (21^2)^4 \bmod 100 = 73 \times 41^4 \bmod 100 = 73 \times (41^2)^2 \bmod 100 =$
$= 73 \times 81^2 \bmod 100 = 73 \times 61 \bmod 100 =$ **53**

d) $2x \bmod 57 = 1$
$n = 57 = 3 \times 19$
$\Phi(n) = 2 \times 18 = 36$

Using Euler's theorem we get
$x = 2^{35} \bmod 57 = 29$

Working:
$2^{35} \bmod 57 = 2 \times 2^{34} \bmod 57 = 2 \times (2^2)^{17} \bmod 57 = 2 \times 4^{17} \bmod 57 =$
$= 2 \times 4 \times 4^{16} \bmod 57 = 8 \times (4^2)^8 \bmod 57 = 8 \times 16^8 \bmod 57 = 8 \times (16^2)^4 \bmod 57 =$
$= 8 \times 256^4 \bmod 57 = 8 \times 28^4 \bmod 57 = 8 \times (28^2)^2 \bmod 57 = 8 \times 784^2 \bmod 57 =$
$= 8 \times 43^2 \bmod 57 = 8 \times 1849 \bmod 57 = 8 \times 25 \bmod 57 =$ **29**

5. Find the inverse of 5 mod 31.

Solution:
$n = 31$
$\phi(n) = 30$

Using Euler's theorem we get
$x = 5^{\phi(31)-1} \bmod 31 = 5^{29} \bmod 31 = 25$
Working:
$5^{29} \bmod 31 = 5 \times 5^{28} \bmod 31 = 5 \times (5^2)^{14} \bmod 31 = 5 \times 25^{14} \bmod 31 =$
$= 5 \times (25^2)^7 \bmod 31 = 5 \times 625^7 \bmod 31 = 5 \times 5^7 \bmod 31 = 5 \times 5 \times 5^6 \bmod 31 =$
$25 \times 25^3 \bmod 31 = 25 \times 25 \times 25^2 \bmod 31 = 5 \times 5 \bmod 31 =$ **25**

6. Find all solutions to the equation 15x mod 25 = 10 in the range [0, 24].

Solution:

gcd(15,25)=5

Since 5 divides 10, the equation 15x mod 25 = 10 has 5 solutions of the form

$x = (2x_0 + 5t) \bmod 25$, t=0,1,2,3,4 where x_0 is the solution to 3x mod 5 =1.

We have $x_0 = 2$ and x = (4+5t) mod 25, t=0,1,2,3,4:
$x_1 = 4$
$x_2 = 9$
$x_3 = 14$
$x_4 = 19$
$x_5 = 24$

7. Let X be an integer variable represented with 32 bits. Suppose that the probability is ½ that X is in the range $[0, 2^8-1]$, with all such values being equally likely, and ½ that X is in the range $[2^8, 2^{32}-1]$, with all such values being equally likely. Compute H(X).

Solution: There are 2^8 numbers in the range $[0, 2^8 - 1]$ and they are all equally likely; thus the probability for each such number is $1/2 \times 1/2^8 = 1/2^9$. Similarly, there are $2^{32} - 2^8$ numbers in the range $[2^8, 2^{32} - 1]$ and they are also all equally likely; thus the probability for each such number is $1/2 \times 1/(2^{32} - 2^8) = 1/(2^{33} - 2^9)$. Then entropy H(X) is:

$H(X) = \Sigma\, p(X) \log_2 1/p(X) = 2^8 \times 1/2^9 \times \log_2 2^9 + (2^{32} - 2^8) \times 1/(2^{33} - 2^9) \times \log_2 (2^{33} - 2^9) = 9/2 + 1/2 \times \log_2 (2^{33} - 2^9) \approx 9/2 + 1/2 \times \log_2 2^{33} = 9/2 + 33/2 = 42/2 = 21$ *bits*.

8. Let X be one of the 6 messages: A, B, C, D, E and F, where:
p(A)=p(B)=p(C)=1/4
p(D)=1/8
p(E)=p(F)=1/16
Compute H(X) and find an optimal binary encoding of the message.

Solution:

$H(X) = \Sigma\, p(X) \log_2 1/p(X)$ = 19/8 bits

X	p(X)	1/p(X)	$\log_2 (1/p(X))$	$p(X) \log_2 (1/p(X))$
A	1/4	4	2	1/2

B	1/4	4	2	1/2
C	1/4	4	2	1/2
D	1/8	8	3	3/8
E	1/16	16	4	1/4
F	1/16	16	4	1/4

$H(X) = \Sigma\, p(X) \log_2 1/p(X) = 3 \times 1/4 \times \log_2 4 + 1/8 \times \log_2 8 + 2 \times 1/16 \times \log_2 16 = 6/4 + 3/8 + 8/16 = 19/8 = 2.375$ bits.

We now need to find an optimal encoding for these messages. We use Huffman code. We start to build a Huffman tree; we first insert a leaf for each message and we label it with the probability corresponding to that leaf. We then combine two nodes with the smallest probabilities by adding a parent node and connecting it to both nodes; the probability of the parent node is the sum of probabilities of the two nodes. We continue this process until we introduce a node with probability 1 – that is the root of the tree and we are done.

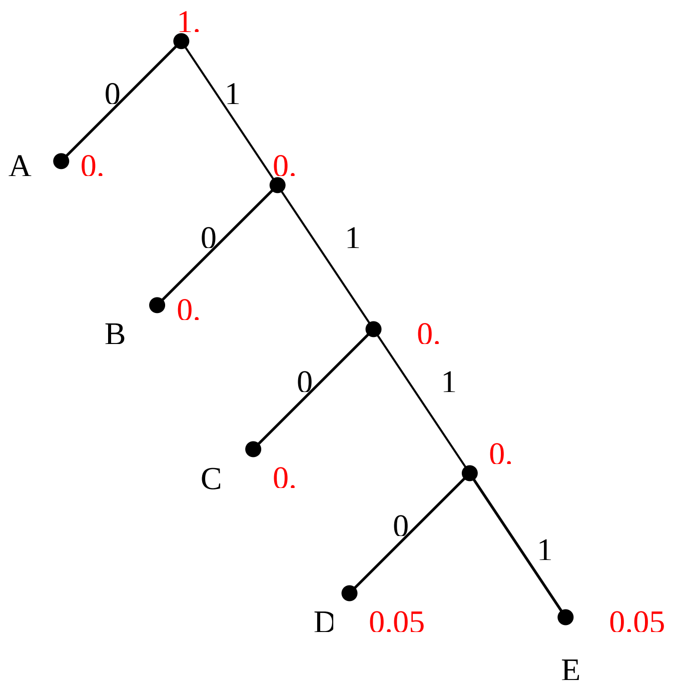
We then label edges of the Huffman tree with labels 0 and 1, such that from each internal node (that is, non-leaf), one edge is labelled 1 and the other edge is labelled 0 (note that this is a binary tree and so each internal tree has two edges connecting it to its children nodes). Then for each message, we find the encoding by reading off the labels of all the edges between the root and the leaf corresponding to that message.

<table>
<tr><td>A</td><td>1/4</td><td>1/4</td><td>1/4</td><td>1/4</td><td rowspan="2">1/2</td><td rowspan="6">1</td></tr>
<tr><td>B</td><td>1/4</td><td>1/4</td><td>1/4</td><td>1/4</td></tr>
<tr><td>C</td><td>1/4</td><td>1/4</td><td>1/4</td><td rowspan="4">1/2</td><td rowspan="4">1/2</td></tr>
<tr><td>D</td><td>1/8</td><td>1/8</td><td rowspan="3">1/4</td></tr>
<tr><td>E</td><td>1/16</td><td rowspan="2">1/8</td></tr>
<tr><td>F</td><td>1/16</td></tr>
</table>

9. Suppose there are 5 possible messages, A, B, C, D and E, with the probabilities p(A)= 0.5, p(B)= 0.3,p(C)= 0.1, p(D)= 0.05 and p(E)= 0.05. What is the expected number of bits needed to encode these messages in optimal encoding? (That is, find H(M).) Provide optimal encoding.

Solution:

$$H(M) = \Sigma\, p(M) \log_2 1/p(M)$$
$$= 1/2 \log_2 2 + 3/10 \log_2 10/3 + 1/10 \log_2 10 + 2 * 1/20 \log_2 20$$
$$= 1/2 + 3/10 (\log_2 10 - \log_2 3) + 1/10 \log_2 10 + 1/10(\log_2 10 - \log_2 2)$$
$$= 5/10 + 3/10 \log_2 10 – 3/10 \log_2 3 + 1/10 \log_2 10 + 1/10 \log_2 10 + 1/10$$
$$= 6/10 + 5/10 \log_2 10 – 3/10 \log_2 3$$
$$= 0.6 + 0.5 \log_2 10 – 0.3 \log_2 3$$
$$= 1.785 \text{ Bits}$$



Hence the encoding is
A = 0, B = 10, C = 110, D = 1110 and E = 1111
But how optimal?

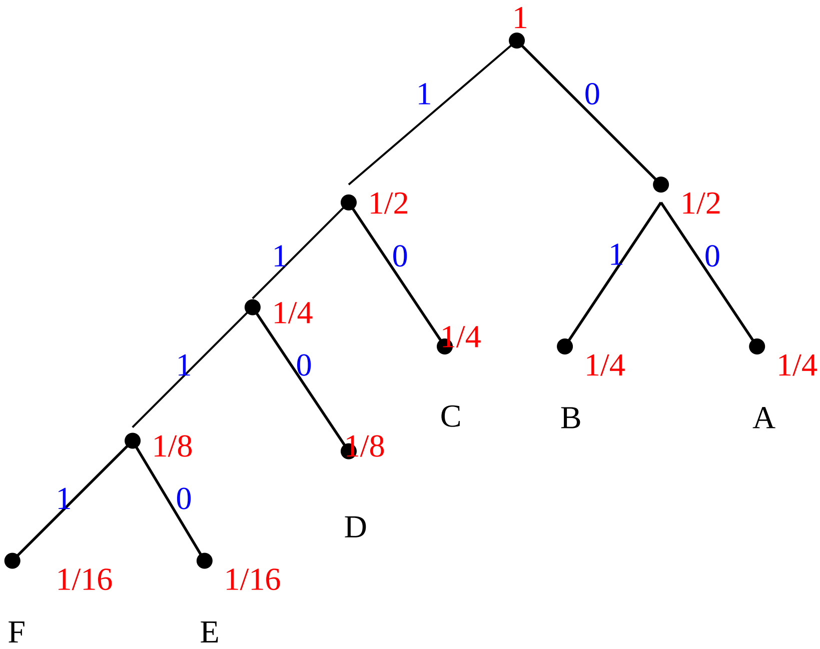
For each possible message we multiply the probability of the message occurring and the number of bits used to encode that message, and sum for all messages.

So the average number of bits N_{AVG} for the above encoding would be.

$$N_{AVG} = (p(A)*1) + (p(B) *2) + (p(C) *3) + (p(D)*4) + (p(E)*4)$$

$$= (0.5 *1) + (0.3 *2) + (0.1*3) + 2(0.05*4) = 1.8 \text{ Bits.}$$

This is slightly higher than the entropy of 1.785 Bits.



A=00, B=01, C=10, D=110, E=1110, F=1111.