The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/6360 Data Security

GAME 2 Solutions

14th March 2019

Number of Questions: 5
Time allowed: 50min
Total mark: 5

In order to score marks you need to show all the workings and not just the end result.

	Student Number	***Student Name***
Student 1		
Student 2		
Student 3		
Student 4		
Student 5		
Student 6		
Student 7		

Question 1	***Question 2***	***Question 3***	***Question 4***	***Question 5***	***TOTAL***

1. Find the GCD of 2,735 and 1,971.

<u>Solution:</u> We use Euclid's algorithm:

```
Algorithm gcd(a,n)
//n ≥ a
begin
g0 := n;
g1 := a;
i := 1;
while gi ≠ 0 do
   begin
      gi+1 := gi-1 mod gi;
      i := i + 1
   end;
gcd := gi-1
end
```

When we run the algorithm on 2,735 and 1,971 we get:

i	g_i
0	2,735
1	1,971
2	764
3	443
4	321
5	122
6	77
7	45
8	32
9	13
10	6
11	1
12	0

Therefore, GCD(*2,735*, *1,971*)=1

2. Find the inverse of 7 modulo 101.

<u>Solution:</u>

$$
\begin{aligned}
x &= 7100 - 1 \; mod \; 101 \\
&= 799 \; mod \; 101 \\
&= 7 \times 798 \; mod \; 101 \\
&= 7 \times (72)49 \; mod \; 101 \\
&= 7 \times 49 \times (49)48 \; mod \; 101 \\
&= 40 \times (492)24 \; mod \; 101 \\
&= 40 \times (782)12 \; mod \; 101 \\
&= 40 \times (242)6 \; mod \; 101 \\
&= 40 \times (712)3 \; mod \; 101 \\
&= 40 \times 92 \times 922 \; mod \; 101 \\
&= 40 \times 92 \times 81 \; mod \; 101 = 29
\end{aligned}
$$

3. For the equation $\Phi(x) = y$, $y=1$ has two solutions: $x=1$ and $x=2$. Find all solutions for each of the following.

a. $y=2$

b. $y=4$

c. $y=31$

Solution:

a. $x \in \{3, 4, 6\}$

b. $x \in \{5,8,10,12\}$

c. no solution

4. Calculate Φ(98).

Solution:

$98 = 2 \times 72$

$\Phi(98) = (2 - 1) \times 7^{2-1} (7 - 1) = 42$

5. Suppose there are 5 possible messages, A, B, C, D and E, with the probabilities p(A)= p(B)= 1/10,p(C)= 2/5, p(D)= p(E)= 1/5. What is the expected number of bits needed to encode these messages in optimal encoding? (That is, find H(M).) Provide optimal encoding. Calculate the average number of bits per message for your encoding.

<u>Solution:</u>

$$H(M) = \sum_{i=1}^{n} p(M_i)\, lg\, \frac{1}{p(M_i)}$$

$$= 2 \times \frac{1}{10}\, lg10 + \frac{2}{5}\, lg\frac{5}{2} + 2 \times \frac{1}{5}\, lg5$$

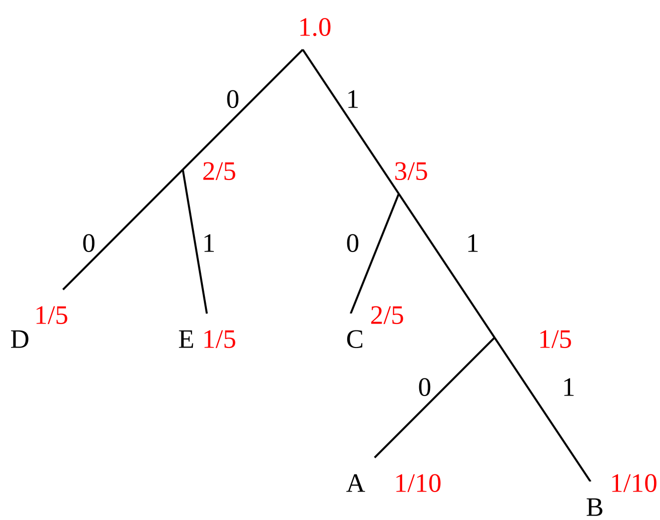
$$= \frac{1}{5}\lg(2 \times 5) + \frac{2}{5}\, lg\frac{5}{2} + \frac{2}{5}\, lg5$$

$$= \frac{1}{5}(lg2 + \lg 5) + \frac{2}{5}\,(lg5 - lg2) + \frac{2}{5}\, lg5$$

$$= \frac{1}{5}(1 + lg5) + \frac{2}{5}\,(lg5 - 1) + \frac{2}{5}\, lg5$$

$$= \frac{1}{5} + \frac{1}{5}lg5 + \frac{2}{5}lg5 - \frac{2}{5} + \frac{2}{5}lg5$$

$$= -\frac{1}{5} + lg5 \cong -\frac{1}{5} + 2.32 = 2.12 bits$$



Gives the encoding:

$$A = 110, B = 111, C = 10, D = 00, E = 01$$

$$NAVG = 2 \times 3 \times \frac{1}{10} + 2 \times \frac{2}{5} + 2 \times 2 \times \frac{1}{5} = 11/5 = 2.2\, bits$$