The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260 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 1,496 and 1,989

Solution: 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 1,496, 1,989 we get:

i	g_i
0	1,496
1	1,989
2	493
3	17
4	0

Therefore, GCD(1,496, 1,989)=17

2. Find the inverse of 3 modulo 101.

Solution:

$x = 3^{100-1} \bmod 101 = 3^{99} \bmod 101 = 3 \times 3^{98} \bmod 101 = 3 \times (3^2)^{49} \bmod 101 = 3 \times 9 \times (9)^{48} \bmod 101 = 27 \times (9^2)^{24} \bmod 101 = 27 \times (81^2)^{12} \bmod 101 = 27 \times (97^2)^6 \bmod 101 = 27 \times (16^2)^3 \bmod 101 = 27 \times 54 \times 54^2 \bmod 101 = 27 \times 54 \times 88 \bmod 101 = 34$

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=8
c. y=29

Solution:

a. $x \in \{3, 4, 6\}$
b. $x \in \{15, 16, 20, 24, 30\}$
c. no solution

4. Calculate $\Phi(45)$.

Solution:

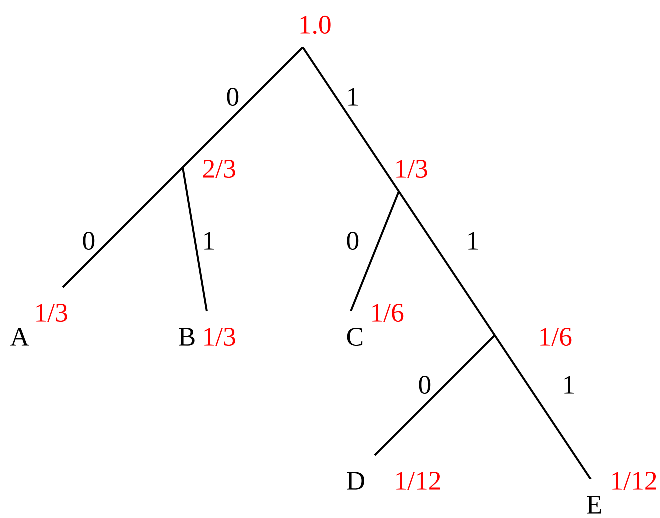
$45 = 3^2 \times 5$

$\Phi(45) = 3^{2-1} \times (3-1) \times (5-1) = 24$

5. Suppose there are 5 possible messages, A, B, C, D and E, with the probabilities p(A)= p(B)= 1/3,p(C)= 1/6, p(D)= p(E)= 1/12. What is the expected number of bits needed to encode these messages in optimal encoding? (That is, find H(M).) Provide optimal encoding.

Solution:

$$
\begin{aligned}
H(M) &= \text{Sigma } p(M) \log_2 1/p(M) \\
&= 2 * 1/3 \log_2 3 + 1/6 \log_2 6 + 2 * 1/12 \log_2 12 \\
&= 4/6 \log_2 3 + 1/6 \log_2 3 + 1/6 \log_2 2 + 1/6 \log_2 3 + 1/6 \log_2 4 \\
&= \log_2 3 + 1/6 + 2/6 \\
&= ½ + \log_2 3 \\
&= 2.085 \text{ Bits}
\end{aligned}
$$



Gives the encoding:

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

$N_{AVG} = 2\ (2 * 1/3) + (2 * 1/6\ ) + 2\ (3 * 1/12) = 13/6 = 2.17$ bits