COMP90043: Cryptography and security: Week 5: Extra Exercises: Suggested Solution

(1) Simplify the following expressions:
   (a) $100003 \ (\ mod \ 100) = 3$
   (b) $64 \ (mod \ 10 \ ) = 4$
   (c) $2^{145} \ 3^{777} \ 9^{777} \ (mod \ 4) = 0$
   (d) $4^8 \ (mod \ 15) = 1;$
   (e) $3^{123} \ 5^{456} \ 7^{789} \ (mod \ 4) = 1$

(2) Verify the following identities.

$$((x \ mod \ m) + (y \ mod \ m)) \ mod \ m = (x + y) \ mod \ m,$$

$$((x \ mod \ m) \times (y \ mod \ m)) \ mod \ m = (x \times y) \ mod \ m,$$

where x, y and m are integers.

```
It is possible to apply basic principles of divisibility properties
and Euclid's algorithm to prove the identities with rigour.
In this subject, it is sufficient you realize the identities with
some examples.
```

(3) Write an efficient algorithm for computing exponentiation in a finite structure (a group, modulo p, finite field etc).

```
Exponentiation:=function(a, exp, n);
p:=1; j:=exp; base:=a;
while (j > 0)
    if even (j)
        base = base^2; j := j div 2;
    else
        p :=p*base; j:=j-1;
end while;
return p;
end function;
```

(4) Find $x^5 \ (mod \ 10)$, where is x is an integer and
   (a.) $0 \leq x < 10$
   (b.) $x \geq 10$.

(5) Express the following numbers as a product of primes and prime powers. $32, 63, 64, 79, 81, 124, 141, 234, 512$

```
For x > 10, first take x mod 10, and then use
the results in (a.) to find the answer.
```

(6) Using the results of the above question, find gcd of the following sequences of numbers.

(a) 32, 63
(b) 141, 81
(c) 81, 124
(d) 79, 141
(e) 512,81
(f) 124, 512.

```
For example  32 = 2^5; 63 = 3^2*7; 63 = 3^2 * 7; 64 = 2^6;
Similarly you need to work out the rest.
```

(7) Set of residues modulo n, denoted by Z_n, is given by $\{0, 1, \cdots, n-1\}$.

Reduced set of residues is the set of all residues moulo n which are relatively prime to n.

How many elements are there in the reduced set of residues:

(a) modulo 11;

```
10; they are 1,2,3,4,5,6,7,8,9,10
```

(b) modulo 35;
(c) modulo 26;
(d) modulo 29;
(e) modulo 77.

In general, if a number n can be expressed using its prime factors such that $n = {p_1}^{a_1}{p_2}^{a_2} \cdots {p_n}^{a_n}$, then there are $\phi(n)$ elements in its reduced set of residues and,

$$\phi(n) = {p_1}^{a_1-1}(p_1 - 1){p_2}^{a_2-1}(p_2 - 1) \cdots {p_n}^{a_n-1}(p_n - 1)$$