

**COMP90043: Cryptography and security: Week 5: Extra Exercises**

(1) Simplify the following expressions:

- (a)  $100003 \pmod{100} =$
- (b)  $64 \pmod{10} =$
- (c)  $2^{145} 3^{777} 9^{777} \pmod{4} =$
- (d)  $4^8 \pmod{15} =;$
- (e)  $3^{123} 5^{456} 7^{789} \pmod{4} =$

(2) Verify the following identities.

$$((x \pmod{m}) + (y \pmod{m})) \pmod{m} = (x + y) \pmod{m},$$

$$((x \pmod{m}) \times (y \pmod{m})) \pmod{m} = (x \times y) \pmod{m},$$

where  $x$ ,  $y$  and  $m$  are integers.

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

(4) Find  $x^5 \pmod{10}$ , where  $x$  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

(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.

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

**Reduced set of residues** is the set of all residues modulo  $n$  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  $n = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$ , then there are  $\phi(n)$  elements in its reduced set of residues and,

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