CISC-203*
Test #3
November 1, 2018

Student Number (Required) _____

Name (Optional) _____

This is a closed book test. You may not refer to any resources.

This is a 50 minute test.

Please write your answers in ink. Pencil answers will be marked, but will not be reconsidered after the test papers have been returned.

The test will be marked out of 50.

Question 1	/10
Question 2	/10
Question 3	/10
Question 4	/15
Question 5	/5
TOTAL	/50

☐ By writing my initials in this box, I authorize Dr. Dawes to destroy this test paper if I have not picked it up by January 15, 2019.

Question 1 : (10 marks)

Find all integer solutions to the equivalence $(x+6)*4 \equiv 5 \quad (\%7)$

Show your work.

Note to 2020 students: this material will be covered on Monday February 10.

Question 2 : (10 Marks)

Prove that if a has an inverse in $\mathbb{Z}_n$ and a also has an inverse in $\mathbb{Z}_m$, then a has an inverse in $\mathbb{Z}_{n*m}$

(Hint: what must be true about a and n, in order for a^{-1} to exist in $\mathbb{Z}_n$?)

Question 3 : (10 Marks)

Show the steps of computing $187^{37}\%144$ using "repeated squaring". You are not required to work out the final value, just show the steps.

Note for 2020 students: this material will be covered on Monday Feb 10.

Question 4 : (15 Marks)

(a) [5 marks] Let n be any odd number > 1.

If $a^{-1} = b$ **in** $\mathbb{Z}_n$, **does** $(2 \otimes a)^{-1} = b \oslash 2$ **in** $\mathbb{Z}_n$ **?**

Show your work.

Question continues on next page

(b) [5 marks] **Show that in $\mathbb{Z}_n$ where $n \geq 2$,** $(n-1) \otimes (n-1) = 1$

(c) [5 marks]

Let n be a prime number. Let a, b and c be non-zero elements of $\mathbb{Z}_n$

Prove or disprove: $(a \otimes b) \oslash c = a \otimes (b \oslash c)$ **in** $\mathbb{Z}_n$

Question 5: (5 Marks)

this question was on cryptography ... not relevant for Test 2 in 2020