

CPSC 418 / MATH 318 — Introduction to Cryptography

ASSIGNMENT 2

Name: Artem Golovin

Student ID: 30018900

Problem 1 — Binary polynomial arithmetic, 20 marks

- a.
 - i.
 - 1. $x^3 + x^2 + x + 1$
 - 2. $x^3 + x^2 + x$
 - 3. $x^3 + x^2 + 1$
 - 4. $x^3 + x^2$
 - 5. $x^3 + x + 1$
 - 6. $x^3 + x$
 - 7. $x^3 + 1$
 - 8. x^3
 - ii.
 - 1. $x^3 + x^2 + x + 1$
 - 2. $x^3 + x^2 + x$
 - 3. $x^3 + x^2$
 - 4. $x^3 + x$
 - 5. $x^3 + 1$
 - 6. x^3
 - iii.
 - 1. $x^3 + x^2 + 1$
 - 2. $x^3 + x + 1$