Introduction to Cryptography: Assignment 7

Group number 57

Elwin Tamminga
s1013846

Lucas van der Laan
s1047485

1

(a)
$$\begin{array}{r}
397551 \\
17\,\overline{)6758371} \\
\underline{51} \\
165 \\
\underline{153} \\
128 \\
\underline{119} \\
93 \\
\underline{85} \\
87 \\
\underline{85} \\
21 \\
\underline{17} \\
4
\end{array}$$

(b) $q = 397551, r = 4$ because $6758371 = 397551 \cdot 17 + 4$

(c) $6758371 \mod 17 = 4$, as modulo is the remainder of a division.

2

(a) No, because the group contains a 0 and the number 0 does not have an inverse. There is no other number that can be modular multiplied with 0 to get 1.

(b) No, because it does not follow the inverse element property, there are elements in the set (for example 2) that cannot be used to do a modular multiplication with another element to get to 1.

(c) $A = \{0, 2, 3, 6, 8, 9\}$, because these values do not have an inverse in the set.

(d) The order of the group is 4, because the group contains the elements $\{1, 5, 7, 11\}$.

3

(a) 3, because $4 \cdot 3 \mod 12 = 0$

(b) 12, because $n/\gcd(n,5) = 12/\gcd(12,5) = 12/1 = 12$

(c) No, because A does not contain a neutral element.

(d) Yes, because B contains a neutral element (0) and each element has an inverse.

(e) No, because C is not a group as it does not apply the inverse property. The 1 in the group can not be added to another element to get 0.

(f) $\{0,4,8\}$, because the only reason A is not a subgroup of $\mathcal{G}$ was because it did not contain the element 0.

(g) $\{0,1,2,4,8,10,11\}$, because now 1 has an inverse element 11.

(h) The smallest subgroup of $\mathcal{G}$ containing B is B.
This is a cyclic group because the generator <2> would lead to the creation of this group.
This is done like so: $2,4,6,8,10,(12 \mod 12 = 0),2...$