Micros, George

Assignment # 2

CS 463: Cryptography for Cybersecurity
Instructor: Ravi Mukkamala, Ph.D
Fall 2014

1 Question 1

1.1 Part a

$(234 * 145) \mod 10$
$(234 \mod 10) * (145 \mod 10) \mod 10$
$4 * 5 \mod 10 \equiv 0$

1.2 Part b

$7 * \frac{4}{11} \mod 10$
$7 * \frac{4+4*10}{11} \mod 10$
$7 * 4 \mod 10 \equiv 28 \mod 10 \equiv 8$

1.3 Part c

$8^{202} * 7^{103} \mod 10$
$(8^{202 \mod 100} \mod 10) * (7^{103 \mod 48} \mod 10) \mod 10$
$(64 \mod 10) * (7^{34 \mod 16} \mod 10) \mod 10$
$4 * (7^2 \mod 10) \mod 10 \equiv 4 * 4 \mod 10 \equiv 6$

2 Question 2

2.1 Part a

$\mathbb{Z}_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$
$\mathbb{Z}*_{12} = \{1,5,7,11\}$

2.2 Part b

$7^2 \mod 12 \equiv 1$
order(7) in $\mathbb{Z}*_{12} = 2$

2.3 Part c

The multiplicative inverse of 5 in $\mathbb{Z}*_{12}$ is itself
$5 * 5 \mod 12 \equiv 1$