NATIONAL INSTITUTE OF TECHNOLOGY, WARANGAL
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
Minor-I Examination, SEPETEMBER 2022
CRYPTOGRAPHY & NETWORK SECURITY

Time: 1 hr Date: 10.09.2022 Max. Marks: 10

Answer Key

1. Define the type of security attack in each of the following cases: **[1M]**

a. A student breaks into a professor's office to obtain a copy of the next day's test.
Ans: confidentiality attack.

b. A student gives a cheque for $10 to buy a used book. Later she finds that the cheque was cashed for $100.
Ans: Integrity attack.

2. Determine the following **[1M]**

a. -7 mod -3
Ans: -1 Explanation $2 \times -3 + -1 = -7$

b. 7 mod -3
Ans: -2 Explanation $-3 \times -3 + -2 = 7$

3. Using Fermat's Theorem calculate 5^{302} mod 11 **[2M]**

Ans : $a^{p-1} \equiv 1 \pmod p$
a=5, p=11, p-1=10, $(5^{300+2}) \bmod 11 = (5^{10})^{30+2 \bmod} 11 = 1^{30}.5^2 \bmod 11 = 3$

4. Perform polynomial multiplication of $(6x^2+x+3)$ and $(5x^2+2)$ with coefficients in Z_{10} **[1M]**

5. Is x^3+x^2+1 reducible over GF(2)?Explain **[1M]**
Ans: No. The polynomial can't be factored. It doesn't have roots.

6. Calculate Euler's totient function for n=108 **[1M]**
Ans: $n= 108= 2^2.3^3$
$Ø(n)=(2^{2-1}).(2-1).(3^{3-1}).(3-1) = 36$

7. Determine gcd(72345,43215) using Euclid algorithm. Write steps **[1M]**

72345 ÷ 43215 = 1 R 29130 (72345 = 1 × 43215 + 29130)
43215 ÷ 29130 = 1 R 14085 (43215 = 1 × 29130 + 14085)
29130 ÷ 14085 = 2 R 960 (29130 = 2 × 14085 + 960)
14085 ÷ 960 = 14 R 645 (14085 = 14 × 960 + 645)
960 ÷ 645 = 1 R 315 (960 = 1 × 645 + 315)
645 ÷ 315 = 2 R 15 (645 = 2 × 315 + 15)
315 ÷ 15 = 21 R 0 (315 = 21 × 15 + 0)
When remainder R = 0, the GCD is the divisor, b, in the last equation. GCD = 15

(or) recursive solution

gcd(72345,43215)= gcd(43215,29130)=
gcd(29130,14085)=gcd(14085,960)=gcd(960,645)=gcd(645,315)=gcd(315,15)=gcd(15,0)
gcd=15

8. An old woman goes to market and a horse steps on her basket and crashes the eggs. The rider offers to pay the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out 5 at a time, there was one egg left. The same happened when she picked 6

at a time, but when she took 7 at a time, no eggs are left over. What is the smallest number of eggs she could have had? Explain the method. **[2M]**

$x \cong 1 \bmod 5$

$x \cong 1 \bmod 6$

$x \cong 0 \bmod 7$

$a_1=1, a_2=1, a_3=0, m_1=5, m_2=6, m_3=7$

$M = m_1 x m_2 x m_3 = 5x6x7 = 210$

$M_1 = M/m_1 = 210/5 = 42$

$M_2 = M/m_2 = 210/6 = 35$

$M_3 = M/m_3 = 210/7 = 30$

$M_1 M_1^{-1} = 1 \bmod m_1$

$42\ M_1^{-1} = 1 \bmod 5$

$2\ M_1^{-1} = 1 \bmod 5$

$M_1^{-1} = 3$

$M_2 M_2^{-1} = 1 \bmod m_2$

$35 M_2^{-1} = 1 \bmod 6$

$5\ M_2^{-1} = 1 \bmod 6$

$M_2^{-1} = 5$

$M_3 M_3^{-1} = 1 \bmod m_3$

$30 M_3^{-1} = 1 \bmod 7$

$2\ M_3^{-1} = 1 \bmod 7$

$M_3^{-1} = 4$

$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$

$x = (1x42x3 + 1x35x5 + 0x30x4) \bmod 210 = 91$

****