factoring a com integer. What is the largest number can test using the following primali ting methods ? (20)

(a) Fermat

(b) Pollard rho

(c) Quadratic sie

(d) Trial division

Roll No. .....

23541

M. Tech. 1st Sem. (Cyber Forensics and Information Security) Examination– December, 2016

MATHEMATICAL FOUNDATIONS OF INFORMATION SECURITY

Paper : MTCF-101

Time : 3 hours ***Max. Marks : 100***

Before answering the questions, candidates should ensure that they have been supplied the correct and complete question paper. No complaint in this regard will be entertained after the examination.

Note: Question no. **one** is compulsory. Attempt **five** questions in total selecting **one** question from each section.

1. (a) Application of Chinese Remainder Theorem. (5)

(b) Differentiate symmetric and asymmetric crypto system. (5)

(c) Explain Diffie-Hellman key agreement. (5)

(d) Write pseud de for Pollard rho method. Also j s complexity. (5)

Se **ı-A**

2. Define quadrati ɔngruence and the importance of Q nd QNRs in solving equations. (20)

3. (a) What is Eucli Algorithm ? Use it to find ged of foll ; pairs : (4+6)

(i) 88 and 22

(ii) 300 and 4

(iii) 24 and 32

(b) Define : (10)

(i) Congruenc l its properties

(ii) Residue cl ıd a least residue.

Se **ı-B**

4. (a) Use the vige cipher with keyword "Health" to en r the message "Life is full of Surpise (10)

(b) Use hill ciphe ncipher the message, "we live in ar cure world". Use the following key : (10)

K = 03 02
05 07

5. (a) Distinguish between a modern and a traditional symmetric key cipher. (10)

(ii) List out the components of modern block ciphers. (10)

Section-C

6. Explain in detail about EI gamal crypto system. (20)

7. (a) Explain the taxonomy of attacks on RSA. (10)

(b) In RSA, given n = 12091 and e = 13. Encrypt the message "This is tough" using the 00 to 26 encoding scheme. Decrypt the cipher text to find the original message. (10)

Section-D

8. Explain in detail about elliptic curve crypto system. (20)

9. Assume that you have a computer performing 1 million bit operation per second. You want to spend only one hour on