A **0200MAT266042501** **Pages: 3**

Reg No.:_______________ Name:__________________________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

B.Tech Degree S4 (R,S) Exam April 2025 (2019 Scheme)

Course Code: MAT266

Course Name: MATHEMATICAL FOUNDATIONS FOR SECURITY SYSTEMS

Max. Marks: 100 Duration: 3 Hours

PART A

(Answer all questions; each question carries 3 marks) Marks

1	Define a ring with a suitable example.	3
2	Does there exist a field of order 2025? Justify your answer.	3
3	Prove that $p(x) = x^2 + x + 2$ is an irreducible polynomial in $GF(3)$.	3
4	Show that {(1,0,1),(0,1,1),(1,1,0)} form a basis of R^3.	3
5	Is 271 a prime number?	3
6	Find the Euler totient function of 240 and 101.	3
7	Using the divisibility test determine whether 943 is a prime or not.	3
8	Factorize $n = 2419$, using Fermat's method.	3
9	The probability that there will be 0,1,2,3 defective light bulbs in a randomly selected batch of bulbs produced in a factory are 0.6, 0.3, 0.08, 0.02 respectively. Find the mean and variance of the number of defective bulbs in a randomly selected batch	3
10	Determine the binomial distribution for which mean is 4 and variance is 3	3

PART B

(Answer one full question from each module, each question carries 14 marks)

Module -1

156

11	a)	Define a ring. Show that $<Z_6, +, \cdot>$ is a ring.	7
	b)	Show that $GF(4)$ is a subfield of $GF(256)$. Let α be a primitive element in $GF(256)$. Find a positive integer k for which $\beta = \alpha^k \in GF(4)$.	7
12	a)	Find the power representation and polynomial representation of elements in the extension field $GF(2^4)$ using the primitive polynomial $p(x) = x^4 + x + 1$.	7
	b)	Illustrate the subfields of GF (2^{24}).	7

Module -2

13	a)	Is $f(x) = x^4 + x + 1$ a primitive polynomial. Justify your answer	7
	b)	Show that the intersection of two subspaces of a vector space V is a subspace of V. What about their union? Justify your answer.	7
14	a)	What is the dimension of the vector space spanned by the vectors {(1,1,0,1,0,1), (0,1,0,1,1,1), (1,1,0,0,1,1), (0,1,1,1,0,1), (1,0,0,0,0,0)} over GF (2).	7
	b)	Determine all the conjugacy classes in $GF(2^4)$ w.r.t $GF(2)$.	7

Module -3

15	a)	Find the gcd (841,160), and also express 'gcd' as an integer linear combination of 841 & 160.	7
	b)	State Fermat's Little theorem. Using it, find the following; (i) 145^{102} mod 101 (ii) 27^{-1} mod 41.	7
16	a)	Solve (a) $6^{24}(mod\ 35)$ (b) $71^{-1}(mod\ 100)$ using Euler's theorem.	7
	b)	Define Euler's totient function $\phi(n)$, for a positive integer n. Explain the rules to calculate $\phi(n)$ for a given positive integer n and calculate $\phi(2025)$.	7

Module -4

17	a)	Does the number 341 pass Fermat's primality test to the base 2? Justify your answer.	7

b) Solve the following system of linear congruences using Chinese remainder theorem; 7

$x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$

18 a) Solve the following quadratic congruences; 7

(i) $x^2 \equiv 2 \pmod{23}$ ii) $x^2 \equiv 6 \pmod{19}$ iii)) $x^2 \equiv 7 \pmod{11}$

b) Using pollard (P-1) method, Find a non-trivial factor of $n = 2813$. 7

Module -5

19 a) A random variable X has the following probability distribution; 7

x	-2	-1	0	1	2	3
$p(x)$	0.1	k	0.2	$2k$	0.3	k

Find i) the value of k ii) $E(X)$ iii) $E(X^2)$ iv) $V(X)$ v) $E(2X+3)$ vi) $V(2X+3)$.

b) Define entropy of a random variable. Compute the entropy of the random variable which counts the number of heads in flipping three fair coins. 7

20 a) State and prove Markov's inequality 7

b) Gracefully estimate the probability that in 100 flips of a fair coin the number of heads will be at least 40 and no more than 60. 7

***