 MA/M.Sc.—Math-IVS(403)

2018

Time : 3 hours

Full Marks : 80

Answer from **both** the Sections as directed

The figures in the right-hand margin indicate marks

Candidates are required to answer in their own words as far as practicable

(NUMBER THEORETIC CRYPTOGRAPHY-II)

SECTION – A

1. Answer any *four* of the following : 4 × 4

   (*a*) Define discrete logarithm. Give an example.

   (*b*) If n is a strong pseudoprime to the base b, then prove that it is an Euler pseudoprime to the base b.

   (*c*) Show that p^2 (with p prime) is a pseudoprime to the base b if and only if $b^{p-1} \equiv 1 \bmod p^2$.

(Turn Over)

(*d*) What is rho method of factorization ? Explain.

(*e*) Factor 17873.

(*f*) If $n \equiv 3 \bmod 4$, then n is a strong pseudoprime to the base b if it is an Euler pseudoprime to the base b.

Or

2. Answer *all* questions : 2 × 8

(*a*) What is pseudo-prime of a given base ?

(*b*) Prove that a Carmichael number must be the product of at least three distinct primes.

(*c*) Find all bases b for which 15 is a pseudoprime.

(*d*) What is the expected value of $\log j$ for a randomly chosen integer j between 1 and y ?

(*e*) What is the probability that 5 randomly chosen set of K vectors in F_2^n is linearly independent $(K \leq n)$?

(*f*) Prove that 561 is the smallest Carmichael number.

(*g*) What is map coloring ? Explain with example.

(*h*) Using the Silver-Pohling-Hellman algorithm, find the discrete log of 153 to the base 2 in F^*_{181}. (2 is generator of F^*_{181}).

SECTION – B

Answer all questions : 16 × 4

3. (*a*) For $n > m \geq 1$, let $P_p(n, m)$ denote the probability, that a random monic polynomial over F_p of degree at most n is a product of irreducible factors all of degree $\leq m$.

(*i*) Find an explicit expression for $P(n, 2)$.

(*ii*) Compute $P(n, 2)$ exactly for all $n \leq 7$.

Or

(*b*) Show that any sequence of positive integers (v_i) with $v_{i+1} \geq 2v_i$ for all i is superincreasing.

4. (*a*) In the zero-knowledge proof of possession of a discrete logarithm, if picara does not realy know the discrete log, then what are the odds against her successfully fooling Vivates for T repetitions of steps (1) – (3) ?

Or

(*b*) Prove that for any fixed prime number n there are only finitely many Carmichael numbers of the form npq (with p and q primes).

5. (*a*) Let $n = 2701$. Use the B-numbers 52^2, 53^2 mod n for a suitable factor-base B to factor 2701. What are $\vec{\epsilon}$ is corresponding to 52 and 53 ?

Or

(*b*) Use the rho-method with $F(x) = x^2 + 1, x_0 = 1$, $n = 8051$ and x_0 to factor the given n. Also compare x_k only with x_j for which $j = 2^h - 1$, where k is an $(h + 1)$-bit integer.

6. (*a*) Write down the algorithm of the quadratic sieve method.

Or

(*b*) In the continued fraction algorithm, explain why there is no need to include in the factor base B any prime p such that

$$\left(\frac{n}{p}\right) = -1.$$