5. (*a*) Prove that, if $n$ has a factor that is with in $\sqrt[4]{n}$ of $\sqrt{n}$, then Fermat factorization works on the first try.

*Or*

(*b*) Use the rho method with $F(x) = x^2 - 1$, $x_0 = 2$, $n = 91$ factor $n$. Also compare $x_k$ only with $x_j$ for which $j = 2^h - 1$, where $k$ is an $(h + 1)$ – bit integer.

6. (*a*) Expand $e$ in a continued fraction and try to guess a pattern in the integer $a_i$.

*Or*

(*b*) Explain the algorithm of continued fraction method with example.

---





**MA/M.Sc.—Math-IVS (403)**

**2019**

*Time* : 3 hours

*Full Marks* : 80

Answer from **both** the Sections as per direction

*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*) In $F_9^*$ with $\alpha$ a root of $x^2 - x - 1$, Find the discrete logarithm of $-1$ to the base $\alpha$.

(*b*) Define vertices of a graph with example.

(*c*) Find the smallest pseudoprime to the base 5.

(*d*) Factor 4087 using $f(x) = x^2 + x + 1$ and $x_0 = 2$.

(*e*) Find the continued fraction representation of the following ration numher 45/89.

*Or*

2. Answer *all* questions : $2 \times 8$

(*a*) What is Silver-Pohling-Hellmann algorithm ?

(*b*) Give an example of discrete logarithm.

(*c*) Define pseudoprime.

(*d*) Find all bases for which 01 is a pseudoprime.

(*e*) Using Format factorization factor 4601.

(*f*) Find the continued fraction representation of the rational number 55/89.

(*g*) Define factor base.

(*h*) Find the smallest pseudoprime to the base 2.

## SECTION – B

Answer **all** questions : $16 \times 4$





3. (*a*) What is the percent likelihood that a random polynomial over $F_2$ of degree exactly 10 factors into a product of polynomials of degree $\leq 2$ ? What is the likelihood that a random nonzero polynomial of degrees at most 10 factors into such a product ?

*Or*

(*b*) Show that the superincreasing sequence with smallest $v_i s$ is the one with $v_i = 2^i$.

4. (*a*) Explain why being able to extract square roots modulo $n = pq$ is essentially equivalent to knowing the factorization of $n$.

*Or*

(*b*) Let $b$ be any integer greater than 1, let $p$ be an odd prime not dividing $b$, $b - 1$ or $b + 1$, Set $n = (b^{2p} - 1)/(b^2 - 1)$

(*i*) Show that $n$ is composite

(*ii*) Show that $2p/n - 1$.