5\. (a) Let S be a set of r elements. Give a map f from S to S and an element $x_0 \in S$, let $x_{j+1} = f(x_j)$ for $j = 0,1,2,\ldots$. Let λ be a positive real number, and let $l = 1 + \sqrt{2\lambda r}$. Then prove that proportion of pairs (f, x_0) for which $x_0, x_1, \ldots\ldots, x_l$ are distinct, where f runs over all maps from S to S and x_0 runs over all elements of S, is less than $e^{-\lambda}$.

OR

(b) Use generalized Fermat factorization to factor: (i) 19578079, (ii) 17018759

6\. (a) Using quadratic sieve method to factor $n = 1042387$, taking the bounds $P = 50$ and $A = 500$.

OR

(b) Write down the algorithm of continued fraction method.

M.A./M.Sc.-Math.-IVS-(CC-403)

2017

Time : **3** hours

Full Marks : **80**

The figures in the right hand margin indicate marks.
Answer from both the Sections as directed.

(NUMBER THEORETIC CRYPTOGRAPHY – II)

SECTION – A

1\. *Answer any **four** of the following :* *(4x4=16)*

(a) Find the discrete log of 153 to the base 2 in F_{181}^{*} using the Silver-Pohlig-Hellman algorithm.

(b) If $n \equiv 3 \; mod \; 4$, then prove that n is a strong pseudo prime to the base b if and only if it is an Euler pseudo prime to the base b.

(c) Use Fermat factorization to factor: (i) 8633, (ii) 809009.

(d) Let $x > 1$ be a real number whose continued fraction expansion has convergent b_i/c_i. Then prove that for all i: $|b_i^2 - x^2 c_i^2| < 2x$.

(e) Factor 4087 using $f(x) = x^2 + x + 1$ and $x_0 = 2$ by rho method.

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

(Turn over)

OR

2. *Answer **all** questions :* *(2x8=16)*

(a) Define discrete logarithm of y to the base b.

(b) What is the discrete logarithm of 7 to the base 2 in F_{19}^{*}.

(c) Define a pseudo prime to the base b.

(d) Prove that the number 91 is a pseudo prime to the base 3.

(e) Prove that 561 is a Carmichael number.

(f) Factor 200819.

(g) Prove that: $log n! - (n log n - n) = O(\log n)$.

(h) Define factor bases.

SECTION - B

*Answer **all** questions* *(16x4=64)*

3. (a) Write down the algorithm for finding the discrete log in the finite field.

OR

(b) Suppose that plaintext message units are single letters in the usual 26-letter alphabet with A – Z corresponding to 0 – 25. You receive the sequence of ciphertext message units 14, 25, 89, 3, 65, 24, 3, 49, 89, 24, 41, 25, 68, 41, 71. The public key is the sequence {57,14,3,24,8} and the secret key is b = 23, m = 61. Try to decipher the message without using the deciphering key; check by using the deciphering key and the algorithm for a superincreasing knapsack problem

4. (a) Using oblivious transfer, construct a non-interactive zero-knowledge proof for possession of a discrete logarithm. (Suppose that the order N of the group is known to everyone.)

OR

(b) Let n be an odd composite integer. Then prove that

(i) n is a pseudoprime to the base b, where $g.c.d.(b, n) = 1$, if and only if the order of b in $(\mathbb{Z}/n\mathbb{Z})*$ (i.e, the least positive power of b which is = 1 mod n) divides $n - 1$.

(ii) If n is a pseudoprime to the bases b_1 and b_2 (where $g.c.d.(b_1, n) = g.c.d.(b_2, n) = 1$), then n is a pseudoprime to the base $b_1 b_2$ and also to the base $b_1 b_2^{-1}$ (where b_2^{-1} is an integer which is inverse to b_2 modulo n).