 MA/M.Sc.—Math-IIIS(CC-302)

2019

(January)

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 - I)

SECTION – A

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

(*a*) Using the big-O notation, estimate in terms of a simple function of n the number of bit operations required to compute 3^n in binary.

(*b*) Let n be a positive odd integer. Prove that there is a 1 to 1 correspondence between the divisors of n which are $< \sqrt{n}$ and those that are $> \sqrt{n}$.

(*c*) Find the inverse of

$$A=\begin{pmatrix}2 & 3\\ 7 & 8\end{pmatrix}\in M_2(z/26z)$$

(*d*) Find $\left(\frac{91}{167}\right)$ using quadratic reciprocity.

(*e*) Find all solutions $\begin{pmatrix}x\\ y\end{pmatrix}$ modulo N, writing x and y as non-negative integers less than N.

$$x+4y\equiv 1 \bmod 9$$
$$5x+7y\equiv 1 \bmod 9$$

Or

2. Answer *all* questions : 2×8

(*a*) Multiply $(212)_3$ by $(212)_3$.

(*b*) If a is not divisible by p and if $n\equiv m \bmod (p-1)$, then $a^n\equiv a^m \bmod p$.

(*c*) Prove that $\left(\frac{-2}{p}\right)=1$ if $p\equiv 1$ or $3 \bmod 8$.

(*d*) What is deciphering ?

(*e*) Working in the 26-letter alphabet, use the matrix A in ex-1 to encipher the message unit "NO".

(*f*) What is RSA ?

(*g*) What do you mean by cryptography ?

(*h*) What is Legendre symbol ?

SECTION – B

Answer **all** questions : 16×4

3. (*a*) (*i*) Describe a subtraction-type bit operation in the same way as was done for an addition-type bit operation in the text.

(*ii*) Find a 3-digit (decimal) number which leaves a remainder of 4 when divided by 7, 9 or 11.

Or

(*b*) State and prove Fermat's little theorem.

4. (*a*) (*i*) Prove that there exists a sequence of primes p such that the probability that a

random $g \in F^*p$ is a generator approaches zero.

(*ii*) Prove that

$$(a+b)^p = a^p + b^p$$

in any field of characteristic p.

Or

(*b*) Prove that

$$G^2 = (-1)^{(q-1)/2} q.$$

5. (*a*) (*i*) How many different shift transformations are there with an N-letter alphabet?

(*ii*) Find a formula for the number of different affine enciphering transformations there are with an N-letter alphabet.

(*iii*) How many affine transformation are there when $N = 26, 27, 29, 30$?

Or

(*b*) Prove that if a non-invertible $A \in M_2(Z/NZ)$ is used to encipher digraph vectors by means

of the formula $C = AP$, then every cipher text one sends can be deciphered as coming from at least two different possible plain texts.

6. (*a*) Let n be any square free integer (i.e. product of distinct primes). Let d and e be positive integers such that de-1 is divisible by $p-1$ for every prime divisor p of n. Prove that $a^{de} \equiv a \bmod n$ for any integer 'a'.

Or

(*b*) Explain the following :

(*i*) Public key cryptography

(*ii*) Key exchange

(*iii*) Probabilistic encryption.