SET-I

M A/ M Sc Applied Mathematics, Central University of Jammu

Semester-IV, End Semester Examination 2016

Course number: MAMT-404

Course Title: Cryptography

Maximum Marks: 100

Time Allowed: 3 hours

Instructions for the candidates:

- The question paper consist of three sections, namely, **Section A**, **Section B** and **Section C**.
- The **section A** consist of 10 objective type questions, and all the questions are compulsory in this section.
- The **section B** consist of 8 short answer type questions, and the candidate has to attempt any 5 questions.
- The **section C** consist of 10 long answer type questions with 2 questions from each unit, and the candidate has to attempt 5 questions selecting one question from each unit.

Section A

(1) If ϕ denotes the Euler's phi function, then which of the following is false?
   (a) $\phi(m) = m - 1$, for $m=$ prime.
   (b) $\phi(m^2) = m(m-1)$, for $m=$ prime.
   (c) $\phi(10^n) = 4 \times 10^{n-1}$. 1
   (d) None of the above.

(2) The set of units of $\mathbb{Z}_{11}$ is
   (a) $\{2, 4, 6, 8, 10\}$.
   (b) $\{1, 3, 5, 7, 9\}$.
   (c) $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. 1
   (d) None of the above.

(3) Let g be a primitive root for $\mathbb{F}_p$ and h be a non-zero element of $\mathbb{F}_p$, then discrete logarithm problem (DLP) is the problem of finding
   (a) an exponent x such that $g^x \equiv h \mod p$.
   (b) an exponent x such that $h^x \equiv g \mod p$.
   (c) a base x such that $x^g \equiv h \mod p$. 1
   (d) None of the above.

(4) $\mathbb{F}_p^*$, the set of all non zero elements of a finite field $\mathbb{F}_p$
   (a) forms a multiplicative group.
   (b) forms a ring with respect to the operations defined in $\mathbb{F}_p$.
   (c) forms a field of cardinality $(p-1)$. 1
   (d) None of the above.

(5) For a fixed integer n, such that an integer a is a witness for n if
   (a) $a^n \equiv a \mod n$.
   (b) $a^n \not\equiv a \mod n$.
   (c) $a^{n-1} \not\equiv \mod n$. 1
   (d) None of the above.

(6) The Riemann zeta function $\zeta(s)$ is defined by $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ has an analytic continuation to the entire complex plane with a simple pole at
   (a) $s = 0$.

(b) $s \neq 1$
(c) $s = 1$ and no other poles.
(d) None of the above. 1

(7) Let p be an odd prime number and let a be a number with $p \nmid a$, then a is quadratic residue modulo p if
(a) $c^2 \equiv a \mod p$.
(b) $c^2 \not\equiv a \mod p$.
(c) $c \equiv a \mod p$.
(d) None of the above. 1

(8) Let a, a_1, a_2, b, b_1, b_2 be integers with b, b_1, b_2 are positive and odd, then
(a) $(\frac{a_1 a_2}{b}) = (\frac{a_1}{b})(\frac{a_2}{b})$.
(b) $(\frac{a_1 a_2}{b}) \neq (\frac{a_1}{b})(\frac{a_2}{b})$.
(c) $(\frac{a_1}{b}) = (\frac{a}{b_1})(\frac{a}{b_2})$.
(d) None of the above. 1

(9) In ElGamal digital signature scheme if primes p and q are such that $q \equiv 1 \mod p$, then the secret signing exponent s satisfying
(a) $1 \leq s \leq p-1$.
(b) $1 \leq s \leq p$.
(c) $0 \leq s \leq 1$.
(d) All of the above. 1

(10) In a digtal signature scheme a verification algorithm returns true if
(a) D^{sig} is a signature for D associated to the private key.
(b) D^{sig} is not a signature for D associated to the private key.
(c) the algorithm has no access to the public key.
(d) None of the above. 1

Section B

(1) State and prove Fermat-Little theorem. 6
(2) Describe Diffie-Hellman key exchange algorithm. 6
(3) Discuss Riemann hypothesis with detail. 6
(4) Prove that if a cryptosystem has perfect secrecy, then $\#K \geq \#M$. 6
(5) Define digital signature. Discuss the NTRU digital signatures in detail. 6
(6) Describe Random bit sequences and symmetric ciphers. 6
(7) Discuss the complexity theory of $\mathcal{P}$ versus $\mathcal{NP}$. 6
(8) Describe the redundancy and entropy of natural language. 6

Section - C

Unit - I

(9) (a) Describe cryptanalysis of simple substitution ciphers.
(b) Let $m \geq 1$ and a be any two integers, then prove that $a.b \equiv 1 \mod m$ for some integer b if and only if $gcd(a, m) = 1$. 6+6
(10) State and prove primitive root theorem. 12

Unit - II

(11) Describe the ElGamal public key cryptosystem with all details. 12
(12) State and prove Chinese remainder theorem. 12

Unit - III

(13) (a) State and prove Euler's formula for pq.
(b) Discuss the Miller Rabin test for composite numbers. 6 + 6

(14) Discuss the pollard's $(p-1)$ factorization algorithm. 12

Unit - IV

(15) Discuss Probablilistic encryption and the Goldwasser-Micali cryptosystem with all necessary details. 12

(16) If for a cryptosystem $\#K = \#M = \#C$ then system has perfect secrecy if and only if
(a) $\forall\ k \in K$ used with same probability.
(b) $\forall\ m \in M$ and $c \in C$ there is exactly one $k \in K$ that encrypts m to c. 12

Unit - V

(17) Give the ElGamal digital signatures algorithm with all details. 12
(18) Discuss the GGH lattice based digital signature scheme with all details. 12