Malaviya National Institute of Technology	2016-17
Department of Computer Science and Engineering	B-Tech
CST-204 : Discrete mathematics	Semester - IV
Home Assignment	**Deadline: After End Exam**

Problem 1: Answer all the following questions.

1 In RSA encryption, the two prime numbers p and q as p=17, q=29. Let the public encryption exponent choose as 9

   (a) Compute the private decryption exponent

   (b) Encrypt the message m=14

2 Prove that every integer greater than 1 is a product of prime numbers

3 For what values of n is $2^n > n^2$? Use mathematical induction to show that your answer is correct.

4 For any integer $n \geq 1$, prove that there always exist n consecutive composite numbers. (Hint: You might want to use the factorial function.)

5 Find all solutions for $x^2 \equiv 1 \,(mod\, 144)$.

6 What is $18! \pmod{437}$?
`[Hint:` $437 = 19 \cdot 23$. `Use Wilson's Theorem and the Chinese Remainder Theorem.]`

7 (4 Marks) Alice, Bob, Charlie, and Mallory use RSA to communicate with one another on a regular basis. You may assume that everyone knows everyones public keys. One day Mallory notices that Alice and Bob have chosen the same RSA modulus N but different exponents e_a, e_b. Mallory knows that the next day Charlie will be sending Alice and Bob a message M containing the location of a secret meeting among the three of them. In particular, the same message will be sent to both Alice and to Bob, but the version sent to Alice will be encrypted with Alices public key and the one sent to Bob will be encrypted with Bobs public key. If Mallory can intercept both ciphertexts C_a and C_a, can Mallory uncover the location of the secret meeting? Explain

8 Let a and $n > 1$ be integers with $gcd(a, n) = 1$. The order of $a \,mod\, n$ is the smallest positive integer r such that $a^r = 1 \,(mod\, n)$. We denote $r = ord_n(a)$.

   (a) Show that $r < \phi(n)$.

   (b) Show that if $m = rk$ is a multiple of r, then $a^m = 1 \,(mod\, n)$.

   (c) Suppose $a^t = 1 \,(mod\, n)$. Write $t = qr + 5$ with $0 < s < r$ (this is just division with remainder). Show that $a^s = 1 \,(mod\, n)$.

   (d) Using the definition of r and the fact that $0 < s < r$, show that $s = 0$ and therefore $r|t$. This, combined with part (b), yields the result that $a^t = 1 \,(mod\, n)$ if and only if $ord_n(a)|t$.

(e) Show that- $ord_n(a)|\phi(n)$.

9 This problem illustrates the point that the Diffie-Hellman protocol is not secure without the step where you take the modulus; i.e. the "In-discrete Log Problem is not a hard problem! You are Eve and have captured Alice and Bob and imprisoned them. You overhear the following dialog.
Bob: Oh, lets not bother with the prime in the Diffie-Hellman protocol, it will make things easier.
Alice: Okay, but we still need a base to raise things to.How about g = 3?
Bob: All right, then my result is 27.
Alice: And mine is 243.

(a) What is Bobs secret X_B and Alices secret X_A ?

(b) What is their secret combined key?

10 If n is composite and passes the Miller-Rabin test for the base , then is called a $strong - pseudo - prime$ to the base a . Show that 2047 is a $strong - pseudo - prime$ to the base 2

11 The RSA system was used to encrypt the message M into the cipher-text C = 6. The public key is given by n = $p \times q$ = 187 and e = 107. In the following, we will try to crack the system and to determine the original message M.

(a) What parameters comprises the public key and what parameters the private key?

(b) What steps are necessary to determine the private key from the public key?

(c) Determine the private key for the given system.

(d) What is the original message M?

12 In the discussion of MixColumns and InvMixColumns, it was stated that $b(x) = a^{-1}(x) mod(x^4 + 1)$ where a(x) = $\{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$ and $b(x) = \{0B\}x^3 + \{0D\}x^2 + \{09\}x + \{0E\}$. Show that this is true.

13 Determine all primes p such that p + 2 and p + 4 are also prime.

14 Let p be a prime number, different from 2 and 5. Show that there exists a natural number whose decimal writing contains only the digit 1 (that is a number in the list 1, 11, 111, 1111, etc.) which is divisible by p.

15 Let ϕ be the Eulers function. Show that $\phi(n^m) = n^{m-1}\phi(n)$ for every natural numbers n,m.

16 The Fibonacci sequence of numbers $F_0, F_1, F_2, \ldots$ is defined by the following recurrence: $F_0 = 0, F_1 = 1$ and $F_i = F_{i-1} + F_{i-2}$ for all $i > 1$. Thus, the first few Fibonacci numbers are

$$F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3, F_5 = 5, F_6 = 8, F_7 = 13, \ldots$$

- **Prove that** any two adjacent Fibonacci numbers F_i and F_{i+1} are relatively prime.
- **Prove** the identity $F_{i+1}F_{i-1} - F_i^2 = (-1)^i$. [*Hint: Use Induction. Show your work.*] Using the identity, compute $F_i^{-1} \pmod{F_{i+1}}$.

17 Solve the following equations for x and y or show that no solution exists. Show your work (in particular, what division must you carry out to solve each case).
(a) 5x+23 $\equiv$ 6 (mod 47)
(b) 9x+80 $\equiv$ 2 (mod 81)
(c) The system of simultaneous equations
30x+3y $\equiv$ 0 (mod 37) and y $\equiv$ 4+13x (mod 37)

18 if gcd(m,x) = 1 then there are m distinct elements in the set { mod(ax,m) : a $\in$ {0,....,m-1} }. If gcd(m,x) $>$ 1, how many distinct elements are there? Prove your answer.

19 Let $N = pq$ be a product of two distinct primes p and q. Suppose I give you N and the inverse of 3 mod $\phi(N)$. That is, I give you N and $d = 3^{-1} \pmod{\phi(N)}$, but I don't tell you what $\phi(N)$ is. Using this information, show a fast way to find the prime factors of N.

20 I have a number of apples, I know that I don't have more than 1000 of them, but I don't have fewer than 900 either. When I arrange them in groups of 11, I have three left over. When I arrange them in groups of 13, I have five left over. How many apples do I have?

21 Answer all the following questions.

(a) 17^{492} mod 83
(b) $\frac{7}{12}$ mod 45
(c) $12\sqrt{23}$ mod 81
(d) $986 \times 987 \times 992 \times 999$ mod 990
(e) $8^2 \times 9^{15}$ mod 70
(f) $\frac{5}{17}$ mod 60
(g) $5\sqrt{49}$ mod 44
(h) Bob receives the encrypted message 8 from Alice. He has picked p = 5, q = 11 and k = 13. What is Alice's secret number?
(i) Compute n $\frac{4}{6}$ mod 8 and $\frac{2}{3}$ mod 8. How do they compare?
(j) Eve intercepts the message 19 sent from Alice to Bob. She knows that k = 831 and N = 3337. What is the message?
(k) Alice has the secret number 18 that she wants to send Bob. She knows k = 19 and N - 527. What encrypted message should she send Bob?
(l) How many numbers mod 16 have a unique 3rd root?
(m) How many numbers from 89 to 187 are odd?
(n) Compute the multiplicative inverse of a (mod n) for the following values of a and n (if it exists), using Extended Euclid. Show your work.
    i. a = 2011, n = 2012.
(o) A student has been asked to solve the following seemingly simple problem: x $\equiv$ 2^{1990}mod 1990. Help her to get the solution by approaching the problem as follows:

i. Factorize 1990 into prime factors.

ii. For all the prime factors, p_i (or its power as may be the case), express the given congruence as x $\equiv a_i mod p_i$. (Hint: Apply Fermats little Theorem, if p is prime, for any positive integer a, $a^{p-1} \equiv 1$ mod p.)

iii. Apply Chinese Remainder Theorem (CRT) to get the solution of the original congruence.

(p) Prove that if $gcd(x, y) = 1$, then $gcd(x + y, x - y)$ is either 1 or 2.

(q) Given integer n =$p_1 \times p_2 \times p_3$ where p_1, p_2, p_3 are prime numbers larger then 2, prove that, there are exactly 8 integers x $\in$

$$1, n$$

satisfy $x^2 \equiv 1(modn)$.

(r) Let n = p $\times$ q with p and q being distinct large prime numbers of roughly equal size. Suppose, we know that for any a $<$ n and gcd(a,n) = 1. We have $a^{p+q} = a^{n+1}$ mod n. Prove that n can be factored in O($n^{(\frac{1}{4})}$ steps with high probability

22 Suppose for applying RSA, p = 11, q = 23, and e = 13. What is the value of d? Show how to encrypt the message 100 and then how to decrypt the resulting message.

23 a For all integers $n \geq 0$ $F_n = 2^{2^n} + 1$ is the n^{th} Fermat's number, then Find $gcd(F_n, F_m)$

b Show that in Z_p, with p prime, if a^i mod p = 1, then $a^n mod p = a^{n \, mod \, i} mod p$.

24 Using the Extended Euclidean algorithm find the multiplicative inverse.

a [5 Marks] 550 mod 1769

b [5 Marks] 1234 mod 4321

25 Prove that "RSA is a collection of strong one way trapdoor permutations, Under the strong RSA assumption".

26 Find integers x and y such that $17x + 101y = 1$.

27 Find all solutions of $12x = 28 \, (mod \, 236)$.

28 Let n = $p \times q$ with p and q being distinct large prime numbers of roughly equal size. Suppose, we know that for any $a < n$ and gcd(a,n) = 1. We have $a^{p+q} = a^{n+1}$ mod n. Prove that n can be factored in O($n^{(\frac{1}{4})}$ steps with high probability.

29 Arjun and Barack are communicating using the RSA algorithm with modulus n = 10573 = (97)(109). Arjun sends an encrypted message to Barack, which he decrypts with the exponent d = 2117 to discover the plaintext m = 221 (mod 10573). What was the encrypted message that Barack received?

30 Let's explore why in the RSA public key system each person has to be assigned a different modulus $N = pq$. Suppose we try to use the same modulus $N = pq$ for everyone. Each person is assigned a public exponent e_i and a private exponent d^i such that e^i . d^i = 1

mod φ(N). At first this appears to work fine: to encrypt to Bob, Alice computes c = $x^{e_{bob}}$ for some value x and sends c to Bob. An eavesdropper Eve, not knowing d_{bob} appears to be unable to invert Bob's RSA function to decrypt c. Let's show that using e_{eve} and d_{eve} Eve can very easily decrypt c.

a . Show that given e_{eve} and d_{eve} Eve can obtain a multiple of φ(N). Let us denote that integer by V .

b . Suppose Eve intercepts a ciphertext c = $x^{e_{bob}}$ mod N. Show that Eve can use V to efficiently obtain x from c. In other words, Eve can invert Bob's RSA function. Hint: First, suppose e_{bob} is relatively prime to V . Then Eve can find an integer d such that d . e_{bob} = 1 mod V . Show that d can be used to efficiently compute x from c. Next, show how to make your algorithm work even if e_{bob} is not relatively prime to V . Note: In fact, one can show that Eve can completely factor the global modulus N.

31 Find all four solutions to $x^2 \equiv 133\,(mod\,143)$. (Note that $143 = 11 \times 13$.)

32 Let $p = 3\,(mod 4)$ be prime. Show that $x^2 \equiv -1\,(mod\,p)$ has no solutions. (Hint: Suppose x exists. Raise both sides to the power $\frac{(p-l)}{2}$ and use Fermat's theorem.)

33 Give an example of integers $m \neq n$ with $gcd(m, n) > 1$ and integers $a \neq b$ such that the simultaneous congruences $x \equiv a\,(mod\,m)$, $x \equiv b\,(mod\,n)$ have a solution.

34 Suppose x = 2 (mod 7) and x = 3 (mod 10). What is x congruent to mod 70?

35 Your opponent uses RSA with $n = pq$ and encryption exponent e and encrypts a message m. This yields the ciphertext $c = m^e\,(mod\,n)$. A spy tells you that, for this message, m^{12345} = 1 (mod n). Describe how to determine m. Note that you do not know $p, q, \phi(n)$, or the secret decryption exponent d. However, you should find a decryption exponent that works for this particular ciphertext. Moreover, explain carefully why your decryption works (your explanation must include how the spys information is used).

"All roads that lead to success have to pass through hard work boulevard at some point" - **Eric Thomas**