Assignment III - B.E. VI Semester

Five students can submit one assignment

1. What is one-way function? what is trapdoor one-way function?
2. State and prove the correctness of RSA Cryptosystem.
3. Find the computational cost (in terms of bit operation) of key generation in RSA algorithm.
4. For RSA with parameters: $e = 7$ and $n = 17 * 31$.
   (a) Encrypt the message block $M = 2$.
   (b) Compute a private key corresponding to the given above public key.
   (c) Perform the decryption of the obtained ciphertext using the method which is four times faster than usual method(Using CRT).
5. Let N is product of two primes. Prove formally that hardness of factorization of N implies hardness of finding $\phi(N)$ given N.
6. Let (N, e) be an RSA public key. Given the private key d, show that one can efficiently factor the modulus N.
7. Alice and Bob have the same modulus n for RSA, and encryption exponents e_A and e_B with $gcd(e_A, e_B) = 1$. Charles sends them the same message m encrypted with these keys, resulting in the ciphertexts c_A and c_B. Adversary intercepts both c_A and c_B. How can she find m?
8. Solve the equation $x^2 + 4x + 1 = 0$ in Z_{23}.
9. What is the 11th root of 2 in Z_{19}? (i.e. what is $2^{1/11} in Z_{19}$)
10. Solve the following system of congruences:
    $x \equiv 12 (mod\ 25)$
    $x \equiv 9 (mod\ 26)$
    $x \equiv 23 (mod\ 27)$
11. Let p be an odd prime. Then show that there are exactly $(p-1)/2$ quadratic residues modulo p and exactly $(p-1)/2$ quadratic non residues modulo p.
12. Let g is the generator of the cyclic group Z_p. Show that g is quadratic non residue mod p.

13. Solve following quadratic congruent equation.
(i)$b^2 \equiv\ 44(mod\ 83)$-
(ii)$b^2 \equiv\ 11(mod\ 29)$
(iii)$b^2 \equiv\ 15(mod\ 59)$

14. Using only CRT show that if $x \cong y\ mod\ p\ \ and\ \ x \cong y\ mod\ q\ \ then\ \ x \cong y\ mod\ N$. (5)

15. Prove that an element $s \in Z_N^*$ is a Q.R. mod N if and only if s is a Q.R. *mod* p and s is a Q.R. *mod* q. Hence, the number of Q.R. in Z_N is $\frac{p-1}{2}\frac{q-1}{2}$

16. Show that computing the square root of a QR in Z_N is as hard as factoring N. (Hint: When the factorization of $N = pq$ is known one computes the square root of $x \in Z_N^*$ by first computing the square root in Z_p of $x\ mod\ p$ and the square root in Z_q of $x\ mod\ q$ and then using the CRT to obtain the square root of x in Z_N).

17. Show that computing the square root of a QR in Z_N is as hard as factoring N. (Hint: When the factorization of $N = pq$ is known one computes the square root of $x \in Z_N^*$ by first computing the square root in Z_p of $x\ mod\ p$ and the square root in Z_q of $x\ mod\ q$ and then using the CRT to obtain the square root of x in Z_N).

18. Given $n = 11 * 19$. Find the square root of 9 mod n.

19. Using the algorithm(discussed in class), find Jacobi of following.
(i) (3053/6823) (ii) (7411/9283)

20. Let sender A sends the same message M to three different receivers using their respective public keys that have same $e = 3$ but different value of n. Let's assume you can intercept all three transmission. Can you find plaintext M in feasible time.

21. Show that text-RSA is vulnerable under following security notions.
(i) IND-CPA(semantic security) (ii) IND-CCA

22. If m is chosen from a small list of possible values ($m < 2^l,\ m\ has\ l - bits$). Show that attacker can compute message m in time $O(l2^\alpha), l/2 < \alpha < l$ which is better than brute force method. (Meet in middle attack)

23. Let (Gen,E,D) be a chosen ciphertext secure public-key encryption system with message space $\{0,1\}^{128}$. Which of the following is also chosen ciphertext secure?

(i)(Gen, E', D') where $E'(pk, m) = E(pk, m \oplus 1^{128})$ and $D'(sk, c) = D(sk, c) \oplus 1^{128}$
(ii)(Gen, E', D') where $E'(pk, m) = (E(pk, m), E(pk, 0^{128}))$ and $D'(sk, (c1, c2)) = D(sk, c1)$.
(iii)(Gen, E', D') where $E'(pk, m) = (E(pk, m), E(pk, m))$ and $D'(sk, (c1, c2)) = D(sk, c1)$.

24. Alice and Bob wish to resolve a dispute over telephone. We can encode the possibilities of the dispute by a binary value. For this they engage a protocol:
(i). $Alice \rightarrow Bob$: Alice picks up randomly an x, which is a 200 bit number and computes the function f(x). Alice sends f(x) to Bob.
(ii). $Bob \rightarrow Alice$: Bob tells Alice whether x was even parity or odd parity.
(iii). $Alice \rightarrow Bob$: Alice then sends x to Bob, so that Bob can verify whether his guess was correct. If Bob's guess was right, Bob wins. Otherwise Alice has the dispute solved in her own way. They decide upon the following function, $f : X \rightarrow Y$, where X

is a random variable denoting a 200 bit sequence and Y is a random variable denoting a 100 bit sequence. The function f is defined as follows: $f(x) =$ (the most significant 100 bits of x) $\vee$ (the least significant 100 bits of x), $\forall x \in X$ Here $\vee$ denotes bitwise OR. Answer the following questions in this regard:
(i). Suppose Bob's strategy to guess the even or odd of x is that if least significant bit of $f(x)$ is zero then x is even else x is odd. If Alice is honest, what is the probability of Bob to be successful in guessing whether x is even or odd correctly?
(ii). What is Alice's probability of cheating Bob?
(iii). What happens when the above function ($\vee$) is replaced by bit-wise XOR? Rework the above sub-parts for this change,

25. Given a positive rational number $\frac{a}{b}$, Find a finite Continued Fraction expansion and the Convergents of continued expansion of the following.
(i) $\frac{33}{95}$ (ii) $\frac{34}{99}$.

26. Write Wiener's algorithm. Suppose that $n = 317940011$ and $b = 77537081$ in the RSA cryptosystem. Using Wiener's algorithm, attempt to factor it.