Mid Sem II   Number Theory and Cryptography (B. Tech.)   Max:20 Marks

1. If the input to the following algorithm is an odd, composite, non-Carmichael number; then show that $\Pr(Error) \leqslant \frac{1}{2}$. $\boxed{4}$

Algorithm 1 Fermat's Test

```
procedure IsPrime(n)
    Select a ∈ {1, 2, ... n − 1} uniformly at random
    if a^(n−1) ≡ 1 (mod n) then
        print "Prime"
    else
        print "Composite"
    end if
end procedure
```

> **Solution:** Proved in the class.

2. If n is an odd Carmichael number then show that $n = p_1 \cdot p_2 \cdots p_t$ for some primes $p_1, p_2, \ldots p_t$ satisfying $(p_i - 1)$ divides $(n - 1)$ for $i = 1, 2, \ldots t$. $\boxed{4}$

> **Solution:** Proved in the class.

3. What is the order of 538 in $\mathbb{Z}^*_{1287}$? $\boxed{3}$

> **Solution:** We know that the group $(\mathbb{Z}^*_{1287}, \times)$ is isomorphic to the group $(\mathbb{Z}^*_9 \times \mathbb{Z}^*_{11} \times \mathbb{Z}^*_{13}, \times)$. [Here $f\colon \mathbb{Z}^*_{1287} \to \mathbb{Z}^*_9 \times \mathbb{Z}^*_{11} \times \mathbb{Z}^*_{13}$, defined by $f(a) = (a \bmod 9, a \bmod 11, a \bmod 13)$, is the isomorphism function.]
>
> Since f is an isomorphism, the order of 538 in $\mathbb{Z}^*_{1287}$ is same as the order of $f(538)$ [which is equal to $(-2, -1, 5)$] in $(\mathbb{Z}^*_9 \times \mathbb{Z}^*_{11} \times \mathbb{Z}^*_{13}, \times)$.
>
> Calculating the powers of $(-2, -1, 5)$, we get $(-2, -1, 5)^1 = (-2, -1, 5)$, $(-2, -1, 5)^2 = (4, 1, -1)$, $(-2, -1, 5)^3 = (-8, -1, -5) = (1, -1, -5)$, $(-2, -1, 5)^4 = (4, 1, -1)^2 = (-2, 1, 1)$ and so on. We find that 12 is the smallest exponent e such that $(-2, -1, 5)^e = (1, 1, 1)$; and so the order is 12.

4. For $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, we used the isomorphism between $(\mathbb{Z}^*_n, \times)$ and $(\mathbb{Z}^*_{p_1^{e_1}} \times \mathbb{Z}^*_{p_2^{e_2}} \times \cdots \times \mathbb{Z}^*_{p_t^{e_t}}, \times)$ to calculate the value of $\varphi(n)$. Can we use the same technique to calculate the value of $\varphi(p_i^{e_i})$ for $i = 1, 2, \ldots t$. Justify your answer. $\boxed{2}$

> **Solution:** For $n = n_1 \cdot n_2 \cdots n_t$, the Chinese Remainder Theorem requires n_i to be pairwise co-prime. Therefore, we cannot say that $(\mathbb{Z}^*_{p_i^{e_i}}, \times)$ is isomorphic to $(\mathbb{Z}^*_{p_i} \times \mathbb{Z}^*_{p_i} \times \cdots \times \mathbb{Z}^*_{p_i}, \times)$

5. If $n = 2 \cdot p^e$ for some odd prime p, then show that $\mathbb{Z}^*_n$ is cyclic. $\boxed{3}$

Solution: We know that $\mathbb{Z}_{p^e}^*$ is cyclic for all primes p. Therefore it has a generator. Let g be a generator of $\mathbb{Z}_{p^e}^*$.

The order of $(1, g)$ in $(\mathbb{Z}_2^* \times \mathbb{Z}_{p^e}^*, \times)$ is same as the order of g in $(\mathbb{Z}_{p^e}^*, \times)$, which is equal to $p^{e-1}(p-1)$. Since $(\mathbb{Z}_2^* \times \mathbb{Z}_{p^e}^*, \times)$ is isomorphic to $(\mathbb{Z}_{2p^e}^*, \times)$, the order of $(1, g)$ in $(\mathbb{Z}_2^* \times \mathbb{Z}_{p^e}^*, \times)$ is same as the order of $f^{-1}(1, g)$ in $(\mathbb{Z}_{2p^e}^*, \times)$. [Here $f \colon \mathbb{Z}_{2p^e}^* \to \mathbb{Z}_2^* \times \mathbb{Z}_{p^e}^*$ is the isomorphism function]. Therefore, the order of $f^{-1}(1, g)$ in $(\mathbb{Z}_{2p^e}^*, \times)$ is $p^{e-1}(p-1)$.

Since the size of $(\mathbb{Z}_{2p^e}^*, \times)$ is $\varphi(2p^e) = 2p^e(1 - \frac{1}{2})(1 - \frac{1}{p}) = p^{e-1}(p-1)$, therefore $f^{-1}(1, g)$ is the generator of $(\mathbb{Z}_{2p^e}^*, \times)$. Hence $(\mathbb{Z}_{2p^e}^*, \times)$ is a cyclic group.

6. Give a subgroup of $\mathbb{Z}_{323}^*$ of size 18. $\boxed{4}$

Solution: We know that the group $(\mathbb{Z}_{323}^*, \times)$ is isomorphic to the group $(\mathbb{Z}_{17}^* \times \mathbb{Z}_{19}^*, \times)$. [Here $f \colon \mathbb{Z}_{323}^* \to \mathbb{Z}_{17}^* \times \mathbb{Z}_{19}^*$ is the isomorphism function.]

It is easy to see that $(\{1\} \times \mathbb{Z}_{19}^*, \times)$ is a subgroup of $(\mathbb{Z}_{17}^* \times \mathbb{Z}_{19}^*, \times)$ of size 18. Since the group $(\mathbb{Z}_{323}^*, \times)$ is isomorphic to the group $(\mathbb{Z}_{17}^* \times \mathbb{Z}_{19}^*, \times)$, therefore $\left(f^{-1}(\{1\} \times \mathbb{Z}_{19}^*), \times\right)$ is a subgroup of $(\mathbb{Z}_{323}^*, \times)$ of size 18. [Here $f^{-1}(\{1\} \times \mathbb{Z}_{19}^*)$ denotes the set $\{x \in \mathbb{Z}_{323}^* \mid f(x) \in \{1\} \times \mathbb{Z}_{19}^*\}$].

By Chinese Remainder Theorem, we get $f^{-1}(\{1\} \times \mathbb{Z}_{19}^*) = \{17x + 1 \mid 0 \leqslant x < 18\}$.