UNIT 1 – 2 MARKS

1. **Define cryptography**

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

2. **Define cryptanalysis.**

Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of **cryptanalysis**. Cryptanalysis is what the layperson calls "breaking the code."

3. **Define security Attack, mechanism and service**

• **Security attack:** Any action that compromises the security of information owned by an organization.

• **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

• **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

4. **Distinguish Threat and Attack**

Threat -A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability.

Attack -An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

5. **Differentiate active attacks and passive attacks.**

A passive attack attempts to learn or make use of information from the system but does not affect system resources. Two types of passive attacks are the release of message contents and traffic analysis.

An active attack attempts to alter system resources or affect their operation. It can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

6. **Specify the components of encryption algorithm**

- Plaintext
- Encryption algorithm
- Secret key
- Cipher text
- Decryption algorithm

7. **Describe security mechanism.**

• **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

8. Differentiate block and stream cipher

A *block cipher* processes the input one block of elements at a time, producing an output block for each input block. A *stream cipher* processes the input elements continuously, producing output one element at a time, as it goes along.

9. **What are the essential ingredients of a symmetric cipher?**

• **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input.

• **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.

• **Secret key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

• **Cipher text:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different cipher texts. The cipher text is an apparently random stream of data and, as it stands, is unintelligible.

• **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plaintext.

10. Specify four categories of security threats

- Interruption
- Interception
- Modification
- Fabrication

11. What is brute-force attack?

The attacker tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

12. List the types of cryptanalysis attack

- Cipher text only
- Known plain text
- Chosen plaintext
- Chosen cipher text
- Chosen text

13. Compare Substitution and Transposition techniques.

➔ **A substitution technique** is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.1 If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

Example: Caesar cipher, monoalphabetic cipher, Playfair cipher,

➔ A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

Example: rail fence

14. Define Steganography.

A plaintext message may be hidden . The methods of **steganography** conceal the existence of the message

Example Techniques: character marking, invisible ink, pin punctures, type writer correction ribbon

15. Quote Euler's theorem.

Euler's theorem states that for every and that are relatively prime:

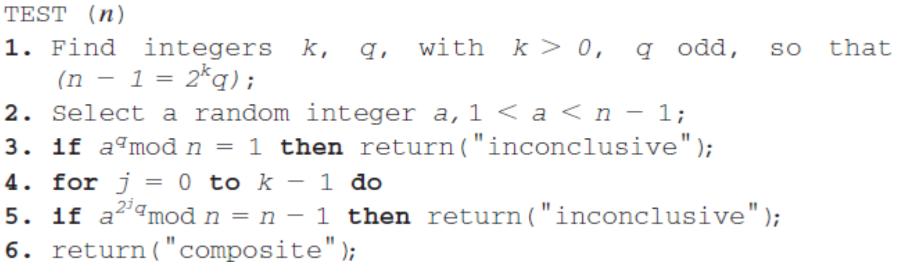
$$a^{\phi(n)} \equiv 1(\bmod n)$$

16. Quote Fermat's theorem.

If ***p*** is prime and **a** is a positive integer not divisible by ***p*** , then

$$a^{p-1} \equiv 1 (\bmod p)$$

17. Write algorithm for testing for primality



```
TEST ($n$)
Find integers $k$, $q$, with $k > 0$, $q$ odd, so that
    ($n - 1 = 2^k q$);
Select a random integer $a$, $1 < a < n - 1$;
if $a^q \bmod n = 1$ then return("inconclusive");
for $j = 0$ to $k - 1$ do
    if $a^{2^j q} \bmod n = n - 1$ then return("inconclusive");
return("composite");
```

18. Define primitive root.

it is said that the base integer ***a*** generates (via powers) the set of nonzero integers modulo 19. Each such integer is called a primitive root of the modulus 19.More generally, we can say that the highest possible exponent to which a number can belong (mod n) is pie(n). If a number is of this order, it is referred to as a **primitive root** of n.

19. Find GCD(24140,16762)

20. Fine GCD(4655,12075)

21. Using the extended Euclidean algorithm, find the multiplicative inverse of

a) 1234 mod 4321

b) 24140 mod 40902

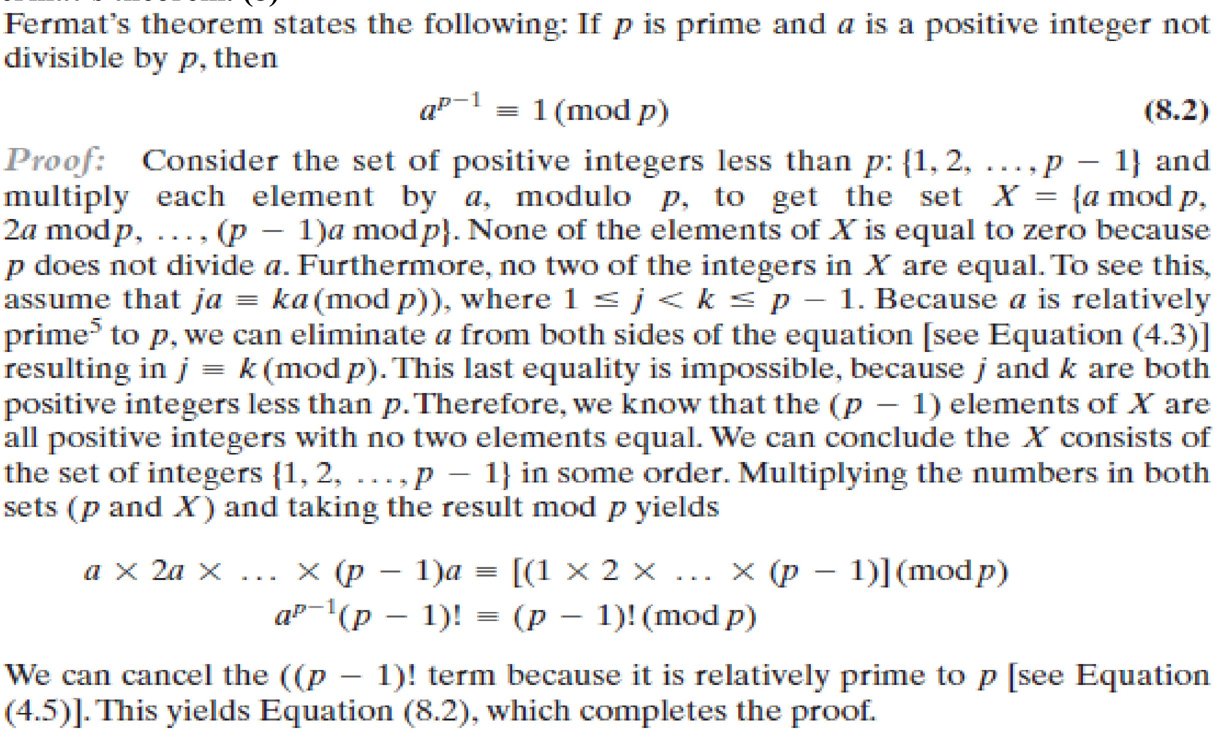
c) 550 mod 1769

22. Using Fermat's theorem, find 3^201 mod 11

16 MARKS

1. **State and Describe**

(i) Fermat's theorem. (8)



Fermat's theorem states the following: If p is prime and a is a positive integer not divisible by p, then

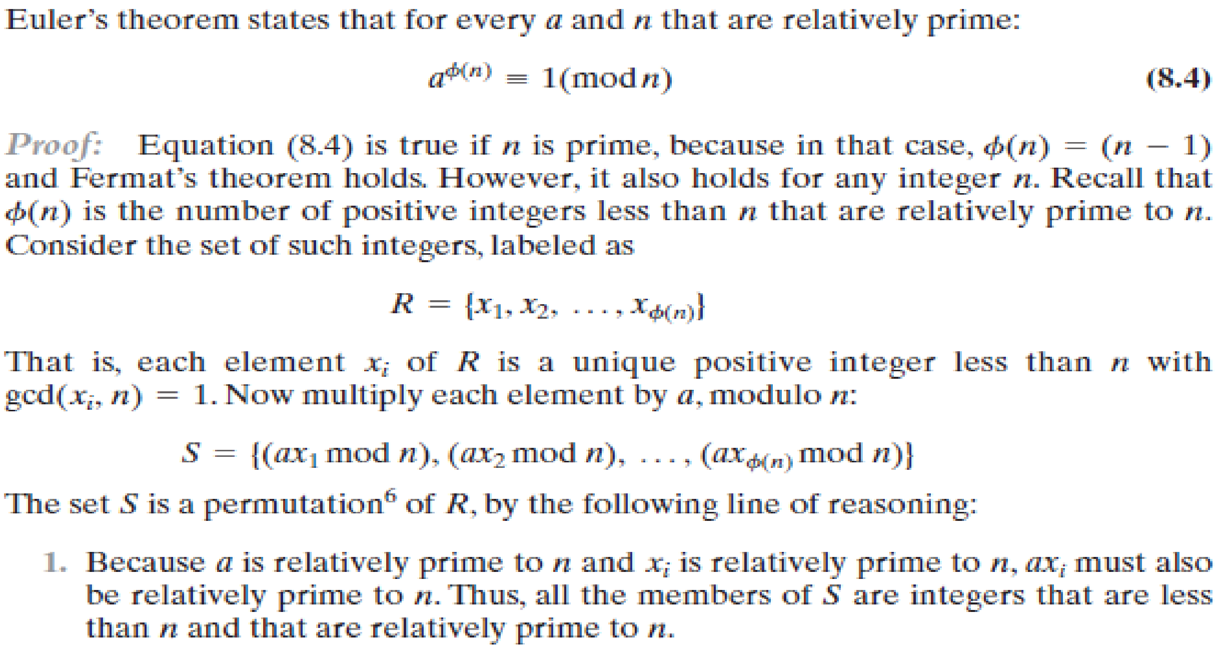
$$a^{p-1} \equiv 1 \, (\text{mod } p) \qquad \textbf{(8.2)}$$

Proof: Consider the set of positive integers less than p: $\{1, 2, \ldots, p - 1\}$ and multiply each element by a, modulo p, to get the set $X = \{a \bmod p, 2a \bmod p, \ldots, (p - 1)a \bmod p\}$. None of the elements of X is equal to zero because p does not divide a. Furthermore, no two of the integers in X are equal. To see this, assume that $ja \equiv ka (\text{mod } p))$, where $1 \le j < k \le p - 1$. Because a is relatively prime[5] to p, we can eliminate a from both sides of the equation [see Equation (4.3)] resulting in $j \equiv k (\text{mod } p)$. This last equality is impossible, because j and k are both positive integers less than p. Therefore, we know that the $(p - 1)$ elements of X are all positive integers with no two elements equal. We can conclude the X consists of the set of integers $\{1, 2, \ldots, p - 1\}$ in some order. Multiplying the numbers in both sets (p and X) and taking the result mod p yields

$$a \times 2a \times \ldots \times (p - 1)a \equiv [(1 \times 2 \times \ldots \times (p - 1)] (\text{mod } p)$$
$$a^{p-1}(p - 1)! \equiv (p - 1)! \, (\text{mod } p)$$

We can cancel the $((p - 1)!$ term because it is relatively prime to p [see Equation (4.5)]. This yields Equation (8.2), which completes the proof.

(ii) Euler's theorem. (8)



Euler's theorem states that for every a and n that are relatively prime:

$$a^{\phi(n)} \equiv 1 (\text{mod } n) \qquad \textbf{(8.4)}$$

Proof: Equation (8.4) is true if n is prime, because in that case, $\phi(n) = (n - 1)$ and Fermat's theorem holds. However, it also holds for any integer n. Recall that $\phi(n)$ is the number of positive integers less than n that are relatively prime to n. Consider the set of such integers, labeled as

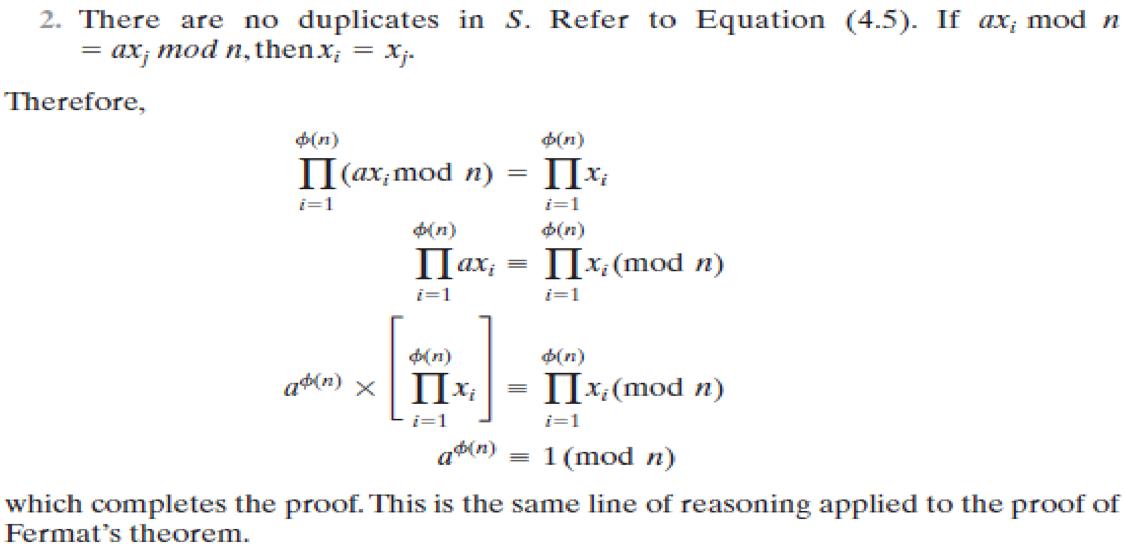
$$R = \{x_1, x_2, \ldots, x_{\phi(n)}\}$$

That is, each element x_i of R is a unique positive integer less than n with $\gcd(x_i, n) = 1$. Now multiply each element by a, modulo n:

$$S = \{(ax_1 \bmod n), (ax_2 \bmod n), \ldots, (ax_{\phi(n)} \bmod n)\}$$

The set S is a permutation[6] of R, by the following line of reasoning:

1. Because a is relatively prime to n and x_i is relatively prime to n, ax_i must also be relatively prime to n. Thus, all the members of S are integers that are less than n and that are relatively prime to n.



2. There are no duplicates in S. Refer to Equation (4.5). If $ax_i \bmod n = ax_j\ mod\ n$, then $x_i = x_j$.

Therefore,

$$\prod_{i=1}^{\phi(n)}(ax_i \bmod n) = \prod_{i=1}^{\phi(n)}x_i$$
$$\prod_{i=1}^{\phi(n)}ax_i \equiv \prod_{i=1}^{\phi(n)}x_i (\bmod n)$$
$$a^{\phi(n)} \times \left[\prod_{i=1}^{\phi(n)}x_i\right] \equiv \prod_{i=1}^{\phi(n)}x_i (\bmod n)$$
$$a^{\phi(n)} \equiv 1 (\bmod n)$$

which completes the proof. This is the same line of reasoning applied to the proof of Fermat's theorem.

2. (i) Tabulate the substitution Techniques in detail. (12)

Definition , example and disadvantages

- Caesar cipher
- monoalphabetic cipher
- playfair cipher
- hill cipher
- polyalphabetic ciphers –vigenere and vernam cipher
- one time pad

(ii) Describe the Transposition Techniques in detail. (4)

Rail fence

3. (i) List the different types of attacks and explain in detail.(8)

1. A passive attack attempts to learn or make use of information from the system but does not affect system resources. Two types of passive attacks are

- The release of message contents and
- traffic analysis.

2. **An active attack** attempts to alter system resources or affect their operation. It can be subdivided into four categories:

- masquerade,
- replay,
- modification of messages, and
- denial of service.
-

(ii) Describe in detail about the types of cryptanalytic attack. (8)

- Cipher text only
- Known plain text
- Chosen plaintext

- Chosen cipher text

Chosen text

4. (i) Evalute3^21 mod 11 using Fermat's theorem. (6)

(ii) State Chinese Remainder theorem and find X for the given set of congruent equations using CRT. (10)

X=2(mod 3)
X=3(mod 5)
X=2(mod 7)

5. (ii) Discuss about the Groups, Rings and Field (8)

6. (i) Solve using playfair cipher. Encrypt the word "Semester Result" with the keyword "Examination". List the rules used. (8)

(ii) Demonstrate the encryption of the message "PAY" using hill cipher with the following key matrix and show the decryption. (8)

|17 17 5|
K= |21 18 21|
|2 2 19|