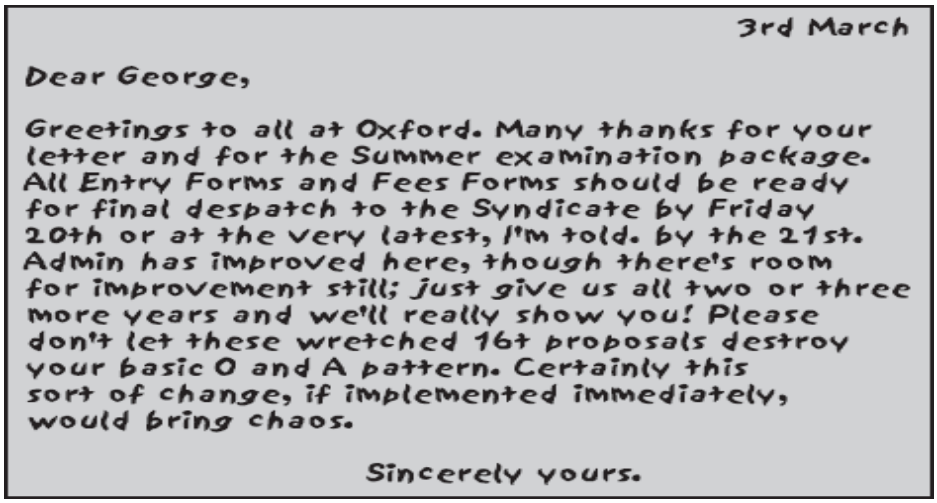
1.7STEGANOGRAPHY

A plaintext message may be hidden in one of two ways. The methods of **steganography** conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text.

A simple form of steganography, but one that is time-consuming to construct, is one in which an arrangement of words or letters within an apparently innocuous text spells out the real message. For example, the sequence of first letters of each word of the overall message spells out the hidden message. Figure shows an example in which a subset of the words of the overall message is used to convey the hidden message.



3rd March

Dear George,

Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final despatch to the Syndicate by Friday 20th or at the very latest, I'm told. by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16+ proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours.

Various other techniques have been used historically; some examples are the following:

Character marking: Selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light.

Invisible ink: A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.

Pin punctures: Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light.

Typewriter correction ribbon: Used between lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light

Steganography has a number of drawbacks when compared to encryption. It requires a lot of overhead to hide a relatively few bits of information, although using a scheme like that proposed in the preceding paragraph may make it more effective. Also, once the system is discovered, it becomes virtually worthless. This problem, too, can be overcome if the insertion method depends on some sort of key.

The advantage of steganography is that it can be employed by parties who have something to lose should the fact of their secret communication (not necessarily the content) be discovered. Encryption flags traffic as important or secret or may identify the sender or receiver as someone with something to hide.

1.6 Foundations of modern cryptography

Modern encryption is the key to advanced computer and communication security. This stream of cryptography is completely based on the ideas of mathematics such as number theory and computational complexity theory as well as concepts of probability.

Characteristics of Modern Cryptography

There are four major characteristics that separate modern cryptography from the classical approach.

Table 1.5 Differences between Traditional Encryption and Modern Encryption

Traditional Encryption	Modern Encryption
For making ciphertext, manipulation is done in the characters of the plaintext	For making ciphertext, operations are performed on binary bit sequence
The whole of the ecosystem is required to communicate confidentiality	Here, only the parties who want to execute secure communication possess the secret key
These are weaker as compared to modern encryption	The encryption algorithm formed by this encryption technique is stronger as compared to traditional encryption algorithms
It believes in the concept of security through obscurity	Its security depends on the publicly known mathematical algorithm

SNS COLLEGE OF ENGINEERING
Kurumbapalayam (Po), Coimbatore – 641 107
AN AUTONOMOUS INSTITUTION
Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

Cryptography

Cryptology, the study of cryptosystems, can be subdivided into two branches −

- Cryptography
- Cryptanalysis

Cryptography

Cryptography is the art and science of making a cryptosystem that is capable of providing information security. Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services.

Cryptanalysis

The art and science of breaking the cipher text is known as cryptanalysis. Cryptanalysis is the sister branch of cryptography and they both co-exist. The cryptographic process results in the cipher text for transmission or storage. It involves the study of cryptographic mechanism with the intention to break them. Cryptanalysis is also used during the design of the new cryptographic techniques to test their security strengths.

Note − Cryptography concerns with the design of cryptosystems, while cryptanalysis studies the breaking of cryptosystems.

Types of Modern Cryptography

Different algorithms have come up with powerful encryption mechanisms incorporated in them. It gave rise to two new ways of encryption mechanism for data security. These are:

- Symmetric key encryption
- Asymmetric key encryption

Key

It can be a number, word, phrase, or any code that will be used for encrypting as well as decrypting any ciphertext information to plain text and vice versa.

Symmetric and asymmetric key cryptography is based on the number of keys and the way these keys work. Let us know about both of them in details:

Symmetric key encryption

Symmetric key encryption technique uses a straight forward method of encryption. Hence, this is the simpler among these two practices. In the case of symmetric key encryption, the encryption is done through only one secret key, which is known as "Symmetric Key", and this key remains to both the parties.

The same key is implemented for both encodings as well as decoding the information. So, the key is used first by the sender prior to sending the message, and on the receiver side, that key is used to decipher the encoded message.

One of the good old examples of this encryption technique is Caesar's Cipher. Modern examples and algorithms that use the concept of symmetric key encryption are RC4, QUAD, AES, DES, Blowfish, 3DES, etc.

Asymmetric Key Encryption

Asymmetric Encryption is another encryption method that uses two keys, which is a new and sophisticated encryption technique. This is because it integrates two cryptographic keys for

implementing data security. These keys are termed as Public Key and Private Key.

The "public key", as the name implies, is accessible to all who want to send an encrypted message. The other is the "private key" that is kept secure by the owner of that public key or the one who is encrypting.

Encryption of information is done through public key first, with the help of a particular algorithm. Then the private key, which the receiver possesses, will use to decrypt that encrypted information. The same algorithm will be used in both encodings as well as decoding.

Examples of asymmetric key encryption algorithms are Diffie-Hellman and RSA algorithm.

Security Services of Cryptography

- Confidentiality of information.
- Data Integrity.
- Authentication.
  - Message authentication.
  - Entity authentication.
- Non-repudiation.

Cryptography Primitives

Cryptography primitives are nothing but the tools and techniques in Cryptography that can be selectively used to provide a set of desired security services −

- Encryption
- Hash functions
- Message Authentication codes (MAC)
- Digital Signatures

The following table shows the primitives that can achieve a particular security service on their own.

Table 1.6 Primitives and Security Service

Primitives ⇨ / ⇩ Service	Encryption	Hash Function	MAC	Digital Signature
Confidentiality	Yes	No	No	No
Integrity	No	Sometimes	Yes	Yes
Authentication	No	No	Yes	Yes
Non Reputation	No	No	Sometimes	Yes

1.6.1 Perfect Security

Perfect Secrecy (or information-theoretic secure) means that the ciphertext conveys no information about the content of the plaintext.....However, part of being provably secure is that

you need as much key material as you have plaintext to encrypt.

1.6.2 Information Theory

Information theory studies the quantification, storage, and communication of information. It was originally proposed by Claude Shannon in 1948 to find fundamental limits on signal processing and communication operations such as data compression.

Its impact has been crucial to the success of the Voyager missions to deep space, the invention of the compact disc, the feasibility of mobile phones, the development of the Internet, the study of linguistics and of human perception, the understanding of black holes, and numerous other fields. The field is at the intersection of mathematics, statistics, computer science, physics, neurobiology, information engineering, and electrical engineering.

The theory has also found applications in other areas, including statistical inference, natural language processing, cryptography, neurobiology, human vision, the evolution and function of molecular codes (bioinformatics), model selection in statistics, thermal physics, quantum computing, linguistics, plagiarism detection, pattern recognition, and anomalydetection.

Important sub-fields of information theory include source coding, algorithmic complexity theory, algorithmic information theory, information-theoretic security, Grey system theory and measures of information.

Applications of fundamental topics of information theory include lossless data compression (e.g. ZIP files), lossy data compression (e.g. MP3s and JPEGs), and channel coding (e.g. for DSL).

Information theory is used in information retrieval, intelligence gathering, gambling, and even in musical composition.

A key measure in information theory is entropy. Entropy quantifies the amount of uncertainty involved in the value of a random variable or the outcome of a random process. For example, identifying the outcome of a fair coin flip (with two equally likely outcomes) provides less information (lower entropy) than specifying the outcome from a roll of a die (with six equally likely outcomes). Some other important measures in information theory are mutual information, channel capacity, error exponents, and relative entropy.

1.6.3 Product Cryptosystems

A product cipher combines two or more transformations in a manner intending that the resulting cipher is more secure than the individual components to make it resistantto cryptanalysis.

The product cipher combines a sequence of simple transformations suchas substitution (S-box), permutation (P-box), and modular arithmetic. For transformation involving reasonable number of n message symbols, both of the foregoing cipher systems (the S-box and P-box) are by themselves wanting.

The combination could yield a cipher system more powerful than either one alone. This approach of alternatively applying substitution and permutation transformation has been used by IBM in the Lucifer cipher system, and has become the standard for national data encryption standards such as the Data Encryption Standard and the Advanced Encryption Standard. A product cipher that uses only substitutions and permutations is called a SP-network. Feistel ciphers are an important class of product ciphers.

1.7 CRYPTANALYSIS

Cryptanalysis is the art of trying to decrypt the encrypted messages without the use of the key that was used to encrypt the messages. Cryptanalysis uses mathematical analysis & algorithms to decipher the ciphers.

The success of cryptanalysis attacks depends

- Amount of time available
- Computing power available
- Storage capacity available

The following is a list of the commonly used Cryptanalysis attacks;

Brute force attack- this type of attack uses algorithms that try to guess all the possible logical combinations of the plaintext which are then ciphered and compared against the original cipher.

Dictionary attack– this type of attack uses a wordlist in order to find a match of either the plaintext or key. It is mostly used when trying to crack encrypted passwords.

Rainbow table attack– this type of attack compares the cipher text against pre- computed hashes to find matches.

Other Attacks using Cryptanalysis

Known-Plaintext Analysis (KPA): Attacker decrypts ciphertext with known partial plaintext.

Chosen-Plaintext Analysis (CPA): Attacker uses ciphertext that matches arbitrarily selected plaintext via the same algorithm technique.

Ciphertext-Only Analysis (COA): Attacker uses known ciphertext collections.

Man-in-the-Middle (MITM) Attack: Attack occurs when two parties use message or key sharing for communication via a channel that appears secure but is actuallycompromised. Attacker employs this attack for the interception of messages that pass through the communications channel. Hash functions prevent MITM attacks.

Adaptive Chosen-Plaintext Attack (ACPA): Similar to a CPA, this attack uses chosen plaintext and ciphertext based on data learned from past encryptions.