List of Tables

Table 1: Permuted Choice 1 (PC-1) ............................................................... 57
Table 2: Subkey Rotation Table ................................................................. 58
Table 3: Permuted Choice 2 (PC-2) ............................................................ 58
Table 4: Initial Permutation (IP) ................................................................. 59
Table 5: Inverse Initial Permutation (IP⁻¹) .................................................. 59
Table 6: E-Bit Selection Table ................................................................. 62
Table 7: Permutation (P) ................................................................. 62
Table 8: Substitution Box 1 (S-Box 1) ..................................................... 63
Table 9: Substitution Box 2 (S-Box 2) ..................................................... 63
Table 10: Substitution Box 3 (S-Box 3) .................................................... 63
Table 11: Substitution Box 4 (S-Box 4) .................................................... 63
Table 12: Substitution Box 5 (S-Box 5) .................................................... 64
Table 13: Substitution Box 6 (S-Box 6) .................................................... 64
Table 14: Substitution Box 7 (S-Box 7) .................................................... 64
Table 15: Substitution Box 8 (S-Box 8) .................................................... 64
Table 16: Comparison of Symmetric and public-key cryptosystem ............ 82
Table 17: Comparison of various cryptographic hash functions ............... 124
Table 18: Time consumed (sec.) in 512-bit, 1024-bit and 2048-bit RSA key-pair generation on testing machines ........................................ 161
Table 19: Encryption Time, Encrypted File Size and Decryption time of file sizes from 1KB to 10KB ......................................................... 164
Table 20: Time taken in digital signature generation of various text files ... 166
Table 21: Time taken in digital signature verification of various text files ... 168
Table 22: Test results on System A ......................................................... 171
Table 23: Test results on System B ......................................................... 172
Table 24: Test results on System C ......................................................... 173
Table 25: Test results on System D ......................................................... 174
1

Introduction

“Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.”

- Eric Hughes.

1.1 Meaning of Cryptography

The word “cryptography” comes from the Latin root “kryptos” which means “hidden, secret” and “graphein” means “writing”. Hence, cryptography refers to secret writing. Similarly the word “cryptology” is a combination of two Greek words kryptos and logia which means “study” so cryptology means the study of hiding information.

Generally, in English cryptology and cryptography are used interchangeably, but cryptology is the combined study of cryptography and cryptanalysis while cryptography means to use and practice of cryptographic techniques. Cryptanalysis is the study of methods for breaking the encryption algorithms and deciphers the encrypted information without knowledge of the key which is normally required to do so.

![Figure 1: Branches of Cryptology](image-url)
Until modern era, cryptography was exclusively referred to as encryption. It is the process of converting messages from a comprehensive form into an incomprehensive one at one end and which reverses the process at the other end so that the message is unreadable by interceptors or eavesdropper without the secret knowledge.

1.2 History of Cryptography

In this fast-paced technological world the importance of information and communication systems is escalating with the increasing significance and quantity of data that is transmitted. Unfortunately systems and data are increasingly vulnerable to a variety of threats, such as unauthorized access and use, misappropriation, alteration, and destruction, any organization has an obligation to protect its secret and sensitive data from them. Cryptography is the foundation of all data as well as information security aspects. Cryptography is the science of encrypting and decrypting information. In telecommunications, cryptography is necessary when data communicating over any untrusted channel. It is implemented in many day-to-day applications such as the security of ATM card, computer passwords, e-commerce, military, etc.

Writing about cryptography from a novice's standpoint seems to be a foolhardy (and facetious) endeavor to say the least, given the ready availability of excellent resources both online and in print. However, no understanding of cryptography and its importance in today's information society is complete without at least a cursory knowledge of how it came about and why it is what it is today.

Before modern era, cryptography was solely used to mean any method of encryption or concealment of meaning at one end and decode it at another end. The earliest forms of secret writing was the first phase of cryptography and it required little more than local pen and paper period analogs as most people could not read. In this period, the methods used for maintaining the
secrecy were not so difficult, since messages were decoded by hand. The two important classical ciphers used in that period are: substitution cipher and transposition cipher. In transposition cipher, the letters in a message are rearranged so that the message “poet” would be encoded as “etpo”. In substitution cipher, a letter or groups of letters are replaced by another letter or groups of letters respectively. One of the earliest substitution ciphers was the Caesar Cipher, in which the letter in the plaintext was replaced by shifting each letter forward by fixed number of positions. It was named after Julius Caesar (100-44 B.C.) who used a simple substitution cipher with the normal alphabet in government communications. He used a shift by three so that the message “digital” would be encoded as “gljlwdo” as in excess-3 in Boolean algebra. The first documented example of written cryptography dates to as far back as 1900 B.C. when an Egyptian scribe first used non-standard hieroglyphics of the day to communicate on stone. In 1467, Leon Battista Alberti invented first automatic cipher device, a wheel. Later Arnaldus de Bruxella (1473-1490) used five lines of cipher to conceal the crucial part of the operation of making a philosopher's stone.

Early 20th century was the second phase of cryptography known as “mechanical era”. Many mechanical cipher devices were invented and some were patented. The most important was rotor machines-famously including the Enigma developed by Arthur Scherbius which was used to generate the code. The Germans figured the Enigma code was unbreakable. British code breaking organization employed over 10,000 people breaking these codes, but the level of effort was very high, the Germans had anticipated. Thomas Jefferson in the 1790s, possibly aided by Dr. Robert Patterson (a mathematician at U. Penn.), who invented his wheel cipher which would be redeveloped as the Strip Cipher, M-138-A, used by the US Navy during World War II.

Claude E. Shannon is considered by many to be the father of mathematical cryptography. Shannon worked for several years at Bell Labs,
and during his time there, he produced an article entitled “A mathematical theory of cryptography” [1]. This article was written in 1945 and eventually was published in the Bell System Technical Journal in 1949. Shannon continued his work by producing another article entitled “A mathematical theory of communication” [2]. Shannon was inspired during the war to address “[t]he problems of cryptography [because] secrecy systems furnish an interesting application of communication theory”. It is commonly accepted that this paper, published in 1949, was the starting point for development of modern cryptography. Shannon provided the two main goals of cryptography: secrecy and authenticity. His focus was on exploring secrecy and thirty-five years later, G.J. Simmons would address the issue of authenticity. “A mathematical theory of communication” highlights one of the most significant aspects of Shannon’s work: cryptography’s transition from art to science. In his works, Shannon described the two basic types of systems for secrecy. The first are those designed with the intent to protect against hackers and attackers who have infinite resources with which to decode a message (theoretical secrecy, now unconditional security), and the second are those designed to protect against hackers and attacks with finite resources with which to decode a message (practical secrecy, now computational security). Most of Shannon’s work focused around theoretical secrecy; here, Shannon introduced a definition for the “unbreakability” of a cipher. If a cipher was determined “unbreakable”, it was considered to have “perfect secrecy”. In proving “perfect secrecy”, Shannon determined that this could only be obtained with a secret key whose length given in binary digits was greater than or equal to the number of bits contained in the information being encrypted. Furthermore, Shannon developed the “unicity distance”, defined as the “amount of plaintext that… determines the secret key. [1,2,3]

The biggest wave of change yet seen in the field of cryptography owes its beginnings to the scientific mobilization of World War II. A leading figure in cryptographic discourse, William Frederick Friedman, founder of
Riverbank Laboratories; cryptanalyst for the US government, and lead code breaker of Japan’s World War II Purple Machine (invented in response to techniques discovered by Herbert O. Yardley), is “honored as the father of U.S. cryptanalysis”. In another significant development during the war, the Germans’ cryptographic workhorse, the Enigma machine was broken by the Polish mathematician Marian Rejewski, based on captured ciphertext and one list of three months worth of daily keys obtained through a spy. Major code breaking developments during the war was continued by Alan Turing, Gordon Welchman and others at Bletchley Park in England.

After the war, the locus of cryptographic activity centered in the National Security Agency (NSA), a branch of the Department of Defense located at Fort Meade, Maryland. Created in 1952 at the behest of President Harry Truman, the NSA took on the role of a centralized intelligence agency whose twin purposes were to protect U.S. military and executive communications from hostile interception and intercepting and decoding communications belonging to other governments.

### 1.3 Modern Cryptography

This is the third phase of cryptography known as “modern era” [4]. The revolution in computers and electronic technology/communications drove the need for civilian research in cryptography, as companies and individuals began to sense the same need for encryption and privacy protection that the government had long recognized. This revolution made possible much more complex ciphers. Computers allowed for the encryption of any kind of data representable in any binary format, but classical ciphers used to encrypt only written language texts which were the new and remarkable achievement in cryptography.

Initially computers were used as standalone devices but the advent of new technologies and as business grew dramatically all over the world, began
to realize that information could only be useful when it can be shared and this led to the concept of networking. A computer network is a network of geographically distributed multiple computers connected in a manner to enable meaningful transmission and exchange of information among them. Sharing of information, sharing of resources both hardware & software and sharing of processing load are some major objectives of a computer network. But work doesn’t end after a network is built because networks require administration to function correctly and steps are needed when expanding the functionalities of the network. Learning this yields a great milestone leading to many new possibilities in making your IT business flourish. One of the possibilities may open the way to that network becoming a voice and data communications network. This is a special type of network which has units that are capable of transmitting both voice and data packets as a form of communication. “External” devices are generally thought of as being independently powered circuitry that exists beyond the chassis of a computer or other digital message source. It is highly desired to communicate in computer network with high security & privacy. Computer security deals with the managerial procedures and technological safeguards applied to computer hardware, software, and data to assure against accidental or deliberate unauthorized access to and the dissemination of computer system data. Computer privacy, on the other hand, is concerned with the moral and legal requirements to protect data from unauthorized access and dissemination. The issues involved in computer privacy are therefore political decisions regarding who may have access to what and who may disseminate what, whereas the issues involved in computer security are procedures and safeguards for enforcing the privacy decisions. To cope with the security and privacy attacks and to achieve the security services such as Authentication, Confidentiality, Integrity, Non-Repudiation and Availability, given new direction to cryptography. Classical cryptosystems is very easy to understand, easily implemented and very easy to be broken. New forms of cryptography came
after the widespread development of computer communications. Hence, more formally, cryptography is the branch of mathematics to study techniques related to aspect of information security services. It is deployed with cryptographic algorithms for hiding message and retrieving hidden messages.

Extensive research was done in the early 1970s. Shannon’s work influenced further cryptography research in the 1970s, as the public-key cryptography developers, M. E. Hellman and W. Diffie cited Shannon’s research as a major influence. His work also impacted modern designs of secret-key ciphers. At the end of Shannon’s work with cryptography, progress slowed until Hellman and Diffie introduced their paper involving “public-key cryptography” [5]. Some of the famous algorithms were: DSA; Whitefield Diffie and Martin Hellman key exchange algorithm, RSA etc. Since then, cryptography has been used as a tool in communications, information security etc. In the 1970s, Dr. Horst Feistel led a cryptography research group at IBM's Watson Research Laboratory and developed the Lucifer cipher, the precursor to today’s U.S. Data Encryption Standard (DES) and other product ciphers, known collectively as the ‘Feistel ciphers’.

In the present scenario the cryptographic techniques have become the immediate solution to protect information against third parties. These techniques required that data and information should be encrypted with some sort of mathematical algorithm where only the party that shares the information could possible decrypt to use the information.

*Cryptographic goals:* Within the context of any communication, there is some specific security requirements include: [6]

1. **Authentication** which means the process of providing one’s identity. It is a service related to identification. This function applies to both entities and information itself. Two parties entering into a communication should identify each other. Information delivered over a channel should be authenticated as to origin, date of origin, data
content, time sent, etc. For these reasons this aspect of cryptography is usually subdivided into two major classes: entity authentication and data origin authentication. Data origin authentication implicitly provides data integrity (for if a message is modified, the source has changed).

(2) **Confidentiality** that ensures no one can read the message except the intended receiver. It is a service used to keep the content of information from all but those authorized to have it. Secrecy is a term synonymous with confidentiality and privacy. There are numerous approaches to providing confidentiality, ranging from physical protection to mathematical algorithms which render data unintelligible.

![Figure 2: Cryptographic Goals](image)

(3) Integrity for assuring the receiver, the received message has not been altered in any way from the original. It is a service which addresses the unauthorized alteration of data. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution.

(4) Non-repudiation is a mechanism to prove that the sender really send this message. It is a service which prevents an entity from denying previous commitments or actions. When disputes arise due to an entity denying that certain actions were taken, a means to resolve the
situation is necessary. For example, one entity may authorize the purchase of property by another entity and later deny such authorization was granted. A procedure involving a trusted third party is needed to resolve the dispute.

In cryptography, the message which is to be kept secret is called as plaintext. The process of hiding its content is called encryption and the encrypted message is called ciphertext. The process of receiving the content of plaintext from the ciphertext is called decryption. A cryptographic algorithm or cipher [7] is a mathematical function used in the encryption and decryption processes. A modern cryptographic algorithm always includes a key. Cryptographic algorithms, plaintexts, ciphertexts, and keys are collectively called cryptosystem. It works in combination with a key to encrypt the plaintext and to decrypt the ciphertext. Figure 3 depicts the flow of information in a cryptographic, or cipher, system. A message (plaintext) M is to be communicated over an insecure communication channel C. K is the key and $T_K$ is the transformation. [8] We may represent the enciphering, deciphering, and cryptanalytic operations as:

\[
C = f(M, K) = T_K(M) \\
M = g(C, K) = T_K^{-1}(C) \\
M' = h(C)
\]

While cryptography is the science of secure data, cryptanalysis is the science of analyzing and breaking secure communication. An attempted cryptanalysis is called attack and its practitioner is called an attacker. The branch of mathematics which encompasses both cryptography and cryptanalysis is called cryptology and its practitioner is generally called
cryptologist. A fundamental assumption in cryptanalysis was first stated by the Dutchman A. Kerkhoff [9]. It is usually referred as Kerkhoff’s principle. It states that the secrecy must reside entirely in the key even though the adversary knows the details of the cryptosystem, including algorithms and their implementations. The fundamental and classical task of cryptography is not only providing mechanism for encryption but also to provide the security services requirements like authentication, confidentiality, integrity, and non-repudiation defined by ITU-T X.800 (International Telecommunication Union-Security Recommendations) [10]. The service confidentiality protects the content of information from unauthorized entity. Data integrity is the service which gives the assurance that data received are exactly as sent by an authorized entity. The service authentication applies to the communicating parties as well as the information. It is divided into peer entity and data origin authentication. Peer entity authentication is used with a logic connection to provide confidence in the identity of the entities connected and data entity authentication implicitly provides data integrity. Similarly, non-repudiation is a service which prevents protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. To provide such security services, three classes of cryptographic algorithms which are shown in Figure 4, namely – (1) Symmetric (or Private-Key) Algorithm: two parties have an encryption and decryption method for which they share a secret key; (2) Asymmetric (or Public-Key) Algorithm: a user possesses a secret key (private key) as in symmetric cryptography but also a public key and; (3) Hybrid Cryptography: symmetric and asymmetric algorithms (and often also hash functions) are all used together.