McGraw Hill Education 大学计算机教育国外著名教材系列 影印版

Cryptography and Network Security

Second Edition

密码学与网络安全

（第2版）

Atul Kahate 著

清华大学出版社

大学计算机教育国外著名教材系列（影印版）

Cryptography and Network Security

Second Edition

密码学与网络安全

（第2版）

Atul Kahate

清华大学出版社
北京

Atul Kahate

Cryptography and Network Security, Second Edition

EISBN: 0-07-064823-9

图书在版编目(CIP)数据

密码学与网络安全：第 2 版 = Cryptography and Network Security, Second Edition: 英文 /（印）卡哈特（Kahate, A.）著. —影印本. —北京：清华大学出版社，2009.5

（大学计算机教育国外著名教材系列（影印版））

ISBN 978-7-302-19796-6

Ⅰ. 密…　Ⅱ. 卡…　Ⅲ. ①密码－理论－高等学校－教材－英文②计算机网络－安全技术－高等学校－教材－英文　Ⅳ. TN918.1　TP393.08

中国版本图书馆 CIP 数据核字（2009）第 045371 号

责任印制：孟凡玉

出版发行：清华大学出版社　　**地　　址：**北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编：**100084
社 总 机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969, c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015, zhiliang@tup.tsinghua.edu.cn
印 刷 者：清华大学印刷厂
装 订 者：三河市李旗庄少明装订厂
发 行 者：全国新华书店
开　　本：185×230　　**印张：**35
版　　次：2009 年 5 月第 1 版　　**印　　次：**2009 年 5 月第 1 次印刷
印　　数：1~3000
定　　价：53.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：010-62770177 转 3103　产品编号：029503-01

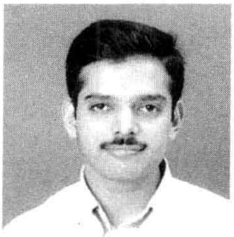
出版说明

进入21世纪，世界各国的经济、科技以及综合国力的竞争将更加激烈。竞争的中心无疑是对人才的竞争。谁拥有大量高素质的人才，谁就能在竞争中取得优势。高等教育，作为培养高素质人才的事业，必然受到高度重视。目前我国高等教育的教材更新较慢，为了加快教材的更新频率，教育部正在大力促进我国高校采用国外原版教材。

清华大学出版社从1996年开始，与国外著名出版公司合作，影印出版了“大学计算机教育丛书（影印版）”等一系列引进图书，受到国内读者的欢迎和支持。跨入21世纪，我们本着为我国高等教育教材建设服务的初衷，在已有的基础上，进一步扩大选题内容，改变图书开本尺寸，一如既往地请有关专家挑选适用于我国高校本科及研究生计算机教育的国外经典教材或著名教材，组成本套“大学计算机教育国外著名教材系列（影印版）”，以飨读者。深切期盼读者及时将使用本系列教材的效果和意见反馈给我们。更希望国内专家、教授积极向我们推荐国外计算机教育的优秀教材，以利我们把“大学计算机教育国外著名教材系列（影印版）”做得更好，更适合高校师生的需要。

清华大学出版社

About the Author



Atul Kahate has 12 years of experience in Information Technology in India and abroad in various capacities. He has done his Bachelor of Science degree in Statistics and his Master of Business Administration in Computer Systems. He has authored thirteen highly acclaimed books published by Tata McGraw-Hill and Pearson Education on various areas of Information Technology (including editions), titled *Web Technologies – TCP/IP to Internet Application Architectures*, *Fundamentals of Computers*, *Information Technology and Numerical Methods*, *Foundations of Information Technology*, *Operating Systems and Systems Programming*, *Operating Systems*, *Computer Communication Networks*, *Introduction to Database Management Systems*, *Object Oriented Analysis and Design*, and *Schaum's Series Outlines—Programming in C++*. Two of these are published as international editions worldwide by McGraw-Hill and have also been translated into Chinese. Several of his books are being used as course textbooks or sources of reference in a number of universities/colleges/IT companies all over the world.

Kahate has been writing articles in newspapers about cricket since the age of 12 and has also authored two books on cricket. He has written over 1000 articles on IT and cricket in all the leading newspapers and magazines/journals in India and abroad. He has deep interest in teaching, music and cricket, besides technology. He has conducted several training programmes in a number of educational institutions and IT organizations, including prestigious institutions such as IIT, Symbiosis, I^{2}IT, MET, Indira Institute of Management, Fergusson College, MIT, VIIT, MIT, Walchand Government Engineering College, etc., and numerous other colleges in India, on a wide range of technologies.

He has also worked as the official cricket statistician and scorer in a number of Test and Limited Overs International cricket matches. He has a rich collection of books on IT and cricket, and has developed his own database that can provide the latest cricket statistics at any moment. He has contributed to cricket websites, such as CricInfo and Cricket Archive. He is a member of the Association of Cricket Statisticians, England, and has written several articles for the Association of Cricket Statisticians and Scorers of India.

Kahate has won several awards, both in India and abroad. He has worked with Syntel, L&T Infotech, American Express and Deutsche Bank previously and is working with i-flex solutions limited as Project Manager for about six years now. He lives in Pune with his wife Anita, daughter Jui and son Harsh. He can be reached at *akahate@gmail.com*.

To,

My wife ***Anita*** *for her love, support, and patience*
My daughter ***Jui*** *for making every day the most beautiful day of my life*
My son ***Harsh*** *for being the naughtiest person at our home*

Preface to the Second Edition

Having worked in the area of Information Technology for about six years (in 2001), I had read a lot about information security, and how to achieve it. However, my concepts were vague, and I knew the technology of security in bits and pieces. This was quite annoying, as it never gave a feeling of satisfaction. It was as if I did not know the complete picture. For example, I did know that number systems played an important role in cryptography, but did not know how much I should know about them to understand the concepts thoroughly. Similarly, I knew that digital certificates and Public Key Infrastructure (PKI) were quite wonderful technologies, but knew only to some extent as to how they worked. Numerous other examples can be given.

Then I got an opportunity to lead an information security project in i-flex solutions limited. I knew that I could learn a lot simply by working on that project. However, I also felt very strongly that until I was thorough with all the aspects of computer security/cryptography myself, I would not be able to do true justice to this project. It was for this reason that I took up the task of studying each and every aspect of these technologies. Unfortunately, there were a lot of hurdles. The main hurdle was that there was not a single book that explained all that I wanted, and more importantly, in the manner that I wanted. My colleagues in the project also expressed this feeling on many occasions. The information available was scattered, quite complex to understand, and not explained to the level that makes one completely understand what is going on.

The struggle for learning was quite wonderful! However, it also convinced me that I should make an attempt to explain what I know, in a very simple manner, so that others who venture into this area do not have to struggle the way I did. This is perhaps the main intention behind this book. In simple terms, it is something, which makes me feel, 'if only such a book were available when I started exploring and learning about security/cryptography'. The biggest satisfaction will be if and when readers in similar situations, feel contented after reading this book.

The first edition of this book was published in early 2003. At that time, there were very few books on the subject, and the ones that existed were quite complex to comprehend. Hence, I had made a genuine attempt to simplify the subject to the maximum possible extent. I had not written the book with any specific aims of addressing the needs of some syllabi. I had written it in a manner that I felt made understanding the subject very easy, more than anything else. To my surprise, in the last four and half years, not only has the book been used in almost all syllabi in India and many other countries, but in addition, several syllabi/courses have been designed around this book. This has reinforced my belief that the sequencing and structuring of the contents of the book is largely correct. This belief has been graciously greeted by the readers of the first edition of the book, which has seen 8 reprints, an international edition, and a Chinese translation, too!

At the same time, security technology is moving rapidly to say the least; and four and half years is a very long time for revising the contents of the book. Several new technologies have emerged, new versions of existing technologies/protocols have been developed; and we must constantly look at these areas for incorporation in this book. Some of the major areas in this context are as follows:

- More detailed coverage of modern algorithms such as AES, SHA-256 and its variations, TLS, etc.
- Providing more mathematical base, wherever needed
- Expanding existing content wherever necessary
- Coverage of some of the topics mentioned in a few syllabi that were not a part of the original edition

With these changes, I am confident that the book is even better than the first edition in terms of meeting the reader's expectations.

The major changes are to make the contents more comprehensive, make them up-to-date wherever necessary, and try to simplify the coverage even further.

These changes are done to address the needs of various syllabi and the feedback received from hundreds of students, readers, professors, and IT professionals.

This book is targeted at two sets of readers: undergraduate/graduate/post-graduate students and IT professionals. To satisfy the diverse needs of both these categories, the book is designed very carefully. On one hand, it goes into the depth of every aspect, to satisfy the needs of the students, and on the other, it touches upon the aspects that the IT professionals like to know at a conceptual level.

A lot of care has been taken in organizing and sequencing the topics. As such, I would recommend that the reader does not skip any chapters altogether. However, for readers who are keener on getting a gist of the material without having to understand the whole thing in very minute details, the mathematical aspects can be skipped.

Students and teachers of the information security/cryptography courses would find the book very helpful. It discusses the technology in great detail, and there are over 425 diagrams which the teachers can use in classroom discussions. Each chapter contains:

- **Summary** of salient points
- List of **terms** and **concepts**
- Self-assessment questions - **Multiple-Choice Questions** (MCQ) and **Detailed Questions**
- **Design/Programming Exercises**

An attempt has been made to keep the presentation style lucid and the language simple.

The overall organization of the book is as follows:

Chapter 1 introduces the basic concepts of security. It discusses the need for security, the principles of security and the various types of attacks on computer systems and networks. We discuss both the theoretical concepts behind all these aspects, as well as the practical issues and examples of each one of them. This will cement our understanding of security. Without understanding why security is required, and what is under threat, there is no point in trying to understand how to make computer systems and networks secure. *Changes from the first edition:* A new section on the modern nature of security attacks is added. Discussions of trusted systems, security models, security management practices, and ethical/legal issues are added. A new section describes the types of attacks. New attacks such as phishing and pharming are covered.

Chapter 2 introduces the concept of cryptography, which is the fundamental building block of computer security. Cryptography is achieved by using various algorithms. All these algorithms are based on either substitution of plain text with some cipher text, or by using certain transposition techniques, or a combination of both. The chapter then introduces the important terms of encryption and decryption. *Changes from the first edition:* Playfair Cipher and Hill Cipher are covered in detail. Diffie–Hellman Key Exchange coverage is expanded. Types of attacks are covered in detail.

Chapter 3 discusses the various issues involved in computer-based symmetric key cryptography. We discuss stream and block cipher and the various chaining modes. We also discuss the chief symmetric key cryptographic algorithms in great detail, such as DES, IDEA, RC5 and Blowfish. *Changes from the first edition:* The Blowfish algorithm is covered in more detail. AES is significantly expanded.

Chapter 4 examines the concepts, issues and trends in asymmetric key cryptography. We go through the history of asymmetric key cryptography. Later, we discuss the major asymmetric key cryptographic algorithms, such as RSA, MD5, SHA, and HMAC. We introduce several key terms, such as message digests and digital signatures in this chapter. We also study how best we can combine symmetric key cryptography with asymmetric key cryptography. *Changes from the first edition:* Variations of the SHA-1 message digest algorithm are covered, with specific coverage of SHA-512.

Chapter 5 talks about the upcoming popular technology of Public Key Infrastructure (PKI). Here, we discuss what do we mean by digital certificates, how they can be created, distributed, maintained and used. We discuss the role of Certification Authorities (CA) and Registration Authorities (RA). We also introduce the Public Key Cryptography Standards (PKCS). *Changes from the first edition:* Covers the details of creating digital certificates in Java..

Chapter 6 deals with the important security protocols for the Internet. These protocols include SSL, SHTTP, TSP, SET and 3D-Secure. We also discuss how electronic money works, what are the dangers involved therein and how best we can make use of it. An extensive coverage of email security is provided, with a detailed discussion of the key email security protocols, such as PGP, PEM and S/MIME. We also discuss wireless security here. *Changes from the first edition:* The coverage of SSL is expanded, and it is compared with TLS. Coverage of PGP is expanded to explain key rings, PGP certificates, and trust management.

Chapter 7 tells us how to authenticate a user. There are various ways to do this. The chapter examines each one of them in significantly great detail and addresses their pros and cons. We discuss password-based authentication, authentication based on something derived from the password, authentication tokens, certificate-based authentication, and biometrics. We also study the popular Kerberos protocol. *Changes from the first edition:* Covers the concepts of security handshakes. It then covers one-way authentication and mutual authentication in detail.

Chapter 8 deals with the practical issues involved in cryptography. Currently, the three main ways to achieve this is to use the cryptographic mechanisms provided by Sun (in the Java programming language), Microsoft and third-party toolkits. We discuss each of these approaches. *Changes from the first edition:* The practical aspects of cryptography in Microsoft's .NET framework are also covered now. The aspects of operating systems security have been enhanced. Database security is covered in detail.

Chapter 9 is concerned with network layer security. Here, we examine firewalls, their types and configurations. Then we go on to IP security, and conclude our discussion with Virtual Private Networks (VPN). *Changes from the first edition:* Network Address Translation (NAT) is added. The concepts of intrusion and intrusion detection are covered in detail.

Chapter 10 contains a number of case studies in the area of cryptography and network security. It discusses how the concepts learnt in the earlier chapters can be put into actual practice. It also covers a few real-life security attacks that have happened, and how they have been dealt with. This presents the viewpoints of the attackers as well as those of the attacked party. *Changes from the first edition:* A couple of more case studies are added.

An Online Learning Center provides online content for the benefit of students and instructors alike. This will contain solutions to all exercises, sample question papers, additional programming exercises, web links, PowerPoint Slides, Cryptography Demos with AES and DES Applets, and real-life case studies. The contents of this website will be updated from time to time.

Without a doubt, Mr. Achyut Godbole has had the greatest influence on my life. I have learnt so much from him in so many ways, both personally and technically. He continues to provide constant encouragement, honest feedback and words of motivation. I cannot express my gratitude for him in words.

My parents and the whole family have been very understanding and supportive. I wish to thank them all besides all my great friends. Besides putting up with the household difficulties, my wife Anita has actually helped me with a number of reviews, which carry a lot of meaning, as she has been a software professional herself. Her sacrifices always allow me to use my spare time constructively. My little and wonderful daughter Jui and very naughty son Harsh have woken up and watched me curiously working on my laptop at 4 a.m. on many occasions. They have made me laugh even when the chips were sometimes down.

This book would not have been possible without the help and support of a number of individuals. My six years in my current organization (i-flex) have been made immensely memorable by people right from the top (Mr Rajesh Hukku, Mr Deepak Ghaisas, Mr Nandu Kulkarni, Mr N K Raman, Mr V Shankar, Mr Vivek Govilkar)to right up to the newest joined in the organization. I am very grateful for all their support, encouragement and words of wisdom. I cannot thank all my dear student friends enough, who always keep me motivated to learn something new. I would like to thank Bruce Schneier, Dan Conway and David Ireland for some of the programming exercises.

Hundreds of readers all over the world have sent such memorable emails about the first edition of the book that it actually makes all this effort seem nothing! I thank all of them profusely for taking their valuable time to appreciate something they have found a bit useful.

As ever, the team at McGraw-Hill (MGH) has been simply brilliant. This book would not have seen the light of day without the expertise and enthusiasm of Vibha Mahajan, Nilanjan Chakravarty, and the rest of the team. I would like to express my gratitude to all of them.

I am grateful to the following reviewers for providing valuable suggestions for the improvement of this book..

Dr. V.S. Janakiraman, SG College of Arts and Sciences, Coimbatore, **Ms. V. Valli Kumari,** Andhra University, Vishakhapatnam, **Prof Jaydip Sen,** Future Institute of Engineering and Management, Kolkata, and **Prof. Bhushan H Trivedi,** GLS Institute of Computer Technology, Bangalore. Prof. **L.K. Suresh Kumar,** Osmania University, **Mr. Dilip Kumar,** National Institute of Technology, Jamshedpur.

I would be very happy to hear from you at akahate@gmail.com.

ATUL KAHATE

Preface to the First Edition

Background

"Three people can keep a secret only if two of them are dead!"

— *Benjamin Franklin*

Quotes such as these are quite common. Keeping secrets is not easy. In fact, human tendency is such that when told that something is a secret and asked to keep it secret, people are actually quite eager to share that secret with everyone else! It is often said that to make something public, it should be called a secret, and told it in a very hush-hush manner to as many people as possible. The word of mouth will automatically spread it!

In the early days of serious computing (1950s-60s), there was not a great deal of emphasis on security, because the systems in those days were proprietary or closed. In simple terms, although computers exchanged data and information with each other, they formed a part of a network that was completely under the control of an organization. The protocols used for computer-to-computer communication in those days were also not known to the general public. Therefore, the chances of someone getting an access to the information being exchanged were not very high. That was also the reason why information security was not a major issue in those days.

As the minicomputers and microcomputers evolved in the 1970s and 1980s, the issue of information security started to gain more prominence. However, it was still not an item of the highest priority on the agenda of the managers and technologists. People used to treat information security as one of the objectives of a hardware/software system. This continued well into the early 1990s. However, it was the Internet, which changed the whole computing paradigm, and brought a tremendous change in the way computers communicated with each other. The world of computers had suddenly become very open. Proprietary protocols (such as IBM's SNA) were no longer popular. It was the open standard of TCP/IP, which was the glue between the computers scattered around the world.

The stupendous growth of the Internet opened up unlimited opportunities for computing. However, at the same time, it also brought about a plethora of new issues and concerns, chief among them being the security of information being exchanged. For example, some of the possibilities were:

- It was no longer safe to send your credit cards details over the network (Internet) to another computer.
- A person accessing the connection between the sender and the recipient could read the e-mails being exchanged.
- People would try to login with someone else's credentials, and use the privileges of that person.

Now, there were so many new threats and possible attacks on information. As the technologists found new ways to thwart these attacks, the attackers found new ways to beat the technologists. This continues even now, and in all probability, it will continue to happen in the future. Therefore, it is very important to know how we can make information exchange secure.

Motivation

Having worked in the area of Information Technology for about 8 years, I had read a lot about information security, and how to achieve it. However, my concepts were vague, and I knew the technology of security in bits and pieces. This was quite annoying, as it never gave a feeling of satisfaction. It was as if I did not know the complete picture. For example, I did know that number systems played an important role in cryptography, but did not know how much I should know about them to understand the concepts thoroughly. Similarly, I knew that digital certificates and Public Key Infrastructure (PKI) were quite wonderful technologies, but knew only to some extent as to how they worked. Numerous other examples can be given.

Then I got an opportunity to lead a PKI project. I knew that I could learn a lot simply by working on that project. However, I also felt very strongly that until I was thorough with all the aspects of computer security/cryptography myself, I would not be able to do true justice to this project. It was for this reason that I took up the task of studying each and every aspect of these technologies. Unfortunately, there were a lot of hurdles. The main hurdle was that there was not a single book, which explained all that I wanted, and more importantly, in the manner that I wanted. My colleagues in the project also expressed this feeling on many occasions. The information available was scattered, was quite complex to understand, and was not explained to the level that makes one completely understand what is going on. I had to struggle a lot to understand how it all works.

The struggle for learning was quite wonderful! However, it also convinced me that I should make an attempt to explain what I know, in a very simple manner, so that others who venture into this area do not have to struggle the way I did. This is perhaps the main intention behind this book. In simple terms, it is something, which makes me feel, 'if only such a book were available when I started exploring and learning about security/cryptography'. The biggest satisfaction will be if and when readers in similar situations, who have the same feeling, feel contented after reading this book.

Intended Audience

This book is targeted at two sets of readers: IT professionals and undergraduate/graduate/post-graduate students. To satisfy the diverse needs of both of these categories, the book is designed very carefully. On one hand, it touches upon the aspects that the IT professionals like to know (conceptual level), and it also goes into the depth of every aspect, to satisfy the needs of the students.

Organization

Teachers teaching information security/cryptography courses would find the book very helpful. It discusses the technology in great detail, and there are over 400 diagrams, which the teachers can use in classroom discussions. Each chapter contains the summary of salient points and a list of terms and concepts. To help the reader to check the understanding of the concepts, each chapter concludes with self-assessment questions. There are Multiple Choice Questions (MCQ), Review Questions, and a unique section on Design/Programming Exercises. This provides the reader with sufficient hands-on opportunities.

An attempt has been made to keep the presentation style lucid and the language simple.

An online learning centre is set up for the teachers, where they can find answers to the chapter-end Review Questions and solutions to the Design/Programming Exercises. This site also contains important diagrams from the book as PowerPoint slides (with appropriate notes), which can be directly used for classroom discussions or presentations.

The chapter-wise organization of the book is explained at the end of the first chapter.

Feedback/Comments

You are welcome to write to me at **akahate@indiatimes.com** with your suggestions or comments about this book. Your feedback would help in making this book better when we revise it for the next edition.

ATUL KAHATE

Important Terms and Abbreviations

1-factor authentication Authentication mechanism, which involves the party to be authenticated concerned with only one factor (e.g., *know* something).

2-factor authentication Authentication mechanism, which involves the party to be authenticated concerned with two factors (e.g., *know* something and *have* something).

3-D Secure Payment mechanism developed by Visa for Web-based transactions.

Acquirer Bank/financial institution that facilitates a merchant to accept and process credit card payments.

Active attack Form of attack on security where the attacker makes attempts to change the contents of the message.

ActiveX control Small client-side program that gets downloaded along with a Web page, and executes inside the browser. This is a Microsoft technology. ActiveX controls are somewhat similar to Java applets.

Algorithm mode Defines the details of a cryptographic algorithm.

Algorithm type Defines how much plain text should be encrypted/decrypted at a time.

Application gateway Type of firewall that filters packets at the application layer of TCP/IP stack. Same as *Bastion host* or *Proxy server*.

Asymmetric Key Cryptography Cryptographic technique where a key pair is used for encryption and decryption operations.

Authentication Principle of security, which identifies a user or a computer system, so that it can be trusted.

Authentication token Small piece of hardware used in 2-factor authentication mechanisms.

Authority Revocation List (ARL) List of revoked Certification Authorities (CA).

Availability Principle of security, which ensures that a resource/computer system is available to the authorized users.

Bastion host Type of firewall that filters packets at the application layer of TCP/IP stack. Same as *Application gateway* or *Proxy server*.

Behaviour-blocking software Software that integrates with the operating system of the computer and keeps a watch on virus-like behavior in real time.

Bell-LaPadula model a highly trustworthy computer system is designed as a collection of objects and subjects. Objects are passive repositories or destinations for data, such as files, disks, printers, etc. Subjects are active entities, such as users, processes, or threads operating on behalf of those users.

Biometric authentication Authentication mechanism that depends on the biological characteristics of a user.

Block cipher Encrypts/decrypts a group of characters at a time.

Bucket brigade attack A form of attack in which the attacker intercepts the communication between two parties, and fools them to believe that they are communicating with each other, whereas they actually communicate with the attacker. Same as *man-in-the-middle attack*.

Book Cipher Cryptographic technique involving the key selected randomly from a page in a book.

Brute-force attack Form of attack wherein the attacker tries all possible combinations of the key one after the other in quick succession.

Caesar Cipher Cryptographic technique wherein each plain text character is replaced with an alphabet three places down the line.

Cardholder Customer, who shops online on the Web, and makes payments for the same using a credit/debit card.

Certificate directory Pre-specified area containing the list of digital certificates.

Certificate Management Protocol (CMP) Protocol used in the requesting of a digital certificate.

Certificate Revocation List (CRL) List of revoked digital certificates. It is an offline certificate checking mechanism.

Certificate Signing Request (CSR) Format used by a user to request for a digital certificate from a CA/RA.

Certificate-based authentication Authentication mechanism wherein the user needs to produce her digital certificate, and also has to provide a proof of possessing that certificate.

Certification Authority (CA) Authority that can issue digital certificates to users after proper authentication checks.

Certification Authority hierarchy Hierarchy that allows multiple CAs to operate, thereby taking load off a single CA.

Chain of trust Mechanism whereby a trust is established from the current CA up to the root CA.

Chaining mode Technique of adding complexity to the cipher text, making it harder to crack.

Challenge/response token Type of authentication token.

Chosen cipher text attack Type of attack where the attacker knows the cipher text to be decrypted, the encryption algorithm that was used to produce this cipher text, and the corresponding plain text block. The attacker's job is to discover the key used for encryption.

Chosen plain text attack Here, the attacker selects a plain text block, and tries to look for the encryption of the same in the cipher text. Here, the attacker is able to choose the messages to encrypt. Based on this, the attacker intentionally picks patterns of cipher text that result in obtaining more information about the key.

Chosen text attack This is essentially a combination of *chosen plain text attack* and *chosen cipher text attack*.

Cipher Block Chaining (CBC) Mechanism of chaining.

Cipher Feedback (CFB) Mechanism of chaining.

Cipher text Result of encryption on a plain text message.

Cipher text only attack In this type of attack, the attacker does not have any clue about the plain text. She has some or all of the cipher text.

Circuit gateway Form of application gateway, which creates a connection between itself and the remote host/server.

Clear text Message in an understandable/readable form, same as *Plain text*.

Collision If two messages yield the same message digest, there is a collision.

Confidentiality Principle of security, which ensurres that only the sender and the recipient of a message come to know about the contents of that message.

Confusion Performing substitution during encryption.

Counter (mode) In this algorithm mode, a counter and plain text block are encrypted together, after which the counter is incremented.

Cross-certification Technology wherein CAs from different domains/locations sign each other's certificates, for ease of operation.

Cryptanalysis Process of analyzing cipher text.

Cryptanalyst Person who performs cryptanalysis.

Cryptographic toolkit Software that provides cryptographic algorithms/operations for use in applications.

Cryptography Art of codifying messages, so that they become unreadable.

Cryptology Combination of cryptography and cryptanalysis.

Data Encryption Standard (DES) IBM's popular algorithm for symmetric key encryption, uses 56-bit keys, not used widely of late.

Decryption Process of transforming cipher text back into plain text - opposite of *Encryption.*

Demilitarized Zone (DMZ) Firewall configuration that allows an organization to securely host its public servers and also protect its internal network at the same time.

Denial Of Service (DOS) attack An attempt by an attacker to disallow authorized users from accessing a resource/computer system.

Dictionary attack Attack wherein the attacker tries all the possible words from the dictionary (e.g. as a password).

Differential cryptanalysis Method of cryptanalysis that looks at pairs of cipher text whose plain texts have particular differences.

Diffusion Performing transposition during encryption.

Digital cash Computer file representing the equivalent of real cash. Bank debits the user's real bank account and issues digital cash, instead. Same as *electronic cash.*

Digital certificate Computer file similar to a paper-based passport, links a user to a particular public key, and also provides other information about the user.

Digital envelope Technique wherein the original message is encrypted with a one-time session key, which itself is encrypted with the intended recipient's public key.

Digital Signature Algorithm (DSA) Asymmetric key algorithm for performing digital signatures.

Digital Signature Standard (DSS) Standard specifing how digital signature should be done.

DNS spoofing See *Pharming.*

Double DES Modified version of DES, involves 128-bit keys.

Dual signature Mechanism used in the Secure Electronic Transaction (SET) protocol whereby the payment details are hidden from the merchant, and the purchase details are hidden from the payment gateway.

Dynamic packet filter Type of packet filter, which keeps learning from the current status of the network.

Electronic cash Computer file representing the equivalent of real cash. Bank debits the user's real bank account and issues digital cash, instead. Same as *digital cash.*

Electronic Code Book (ECB) Mechanism of chaining.

Electronic money See *Electronic cash.*

Encryption Process of transforming plain text into cipher text - opposite of *Decryption.*

Fabrication False message created by an attacker to distort the attention of the authorized users.

Firewall Special type of router, which can perform security checks and allows rule-based filtering.

Hash *Finger print* of a message, same as *Message digest.* Identifies a message uniquely.

Hill Cipher Hill cipher works on multiple letters at the same time. Hence, it is a type of polygraphic substitution cipher.

HMAC Similar to a message digest, HMAC also involves encryption.

Homophonic Substitution Cipher Technique of encryption in which one plain text character is replaced with one cipher text character, at a time. The cipher text character is not fixed.

Integrity Principle of security, which specifies that the contents of a message must not be altered during its transmission from the sender to the receiver.

Interception Process of an attacker getting hold of a message in transit, before it reaches the intended recipient.

International Data Encryption Algorithm (IDEA) International Data Encryption Algorithm (IDEA) - a symmetric key encryption algorithm, developed in 1990's.

Internet Security Association and Key Management Protocol (ISAKMP) Protocol used in IPSec for key management. Also called as Oakley.

Interruption Attacker creating a situation where the availability of a system is in danger. Same as *Masquerade*.

IP Security (IPSec) Protocol to encrypt messages at the network layer.

Issuer Bank/financial institution that facilitates a cardholder to make credit card payments on the Internet.

Java applet Small client-side program that gets downloaded along with a Web page, and executes inside the browser. This is a Sun technology. Java applets are somewhat similar to ActiveX controls.

Java Cryptography Architecture (JCA) Java's cryptography mechanism, in the form of APIs.

Java Cryptography Extensions (JCE) Java's cryptography mechanism, in the form of APIs.

Kerberos Single Sign On (SSO) mechanism, that allows a user to have a single user id and password to access multiple resources/systems.

Key The secret information in a cryptographic operation.

Key Distribution Center (KDC) A central *authority* dealing with keys for individual computers (nodes) in a computer network.

Key wrapping See *Digital envelope*.

Known plaintext attack In this case, the attacker knows about some pairs of plain text and corresponding cipher text for those pairs. Using this information, the attacker tries to find other pairs, and therefore, know more and more of the plain text.

Lightweight Directory Access Protocol (LDAP) Protocol that allows easy storage and retrieval of information at/from a central place.

Linear cryptanalysis An attack based on linear approximations.

Lucifer One symmetric key encryption algorithm.

Man-in-the-middle attack A form of attack in which the attacker intercepts the communication between two parties, and fools them to believe that they are communicating with each other, whereas they actually communicate with the attacker. Same as *bucket brigade attack*.

Masquerade Attacker creating a situation where the availability of a system is in danger. Same as *Interruption*.

MD5 Message digest algorithm, now seems vulnerable to attacks.

Merchant Person/organization, who sets up an online shopping site, and accepts electronic payments.

Message Authentication Code (MAC) See *HMAC*.

Message digest *Finger print* of a message, same as *Hash*. Identifies a message uniquely.

Microsoft Cryptography Application Programming Interface (MS-CAPI) Microsoft's cryptography mechanism, in the form of APIs.

Modification Attack on a message where its contents are changed.

Mono-alphabetic Cipher Technique of encryption in which one plain text character is replaced with one cipher text character, at a time.

Multi-factor authentication Authentication mechanism, which involves the party to be authenticated concerned with multiple factors (e.g. *know* something, *be* something and *have* something).

Mutual authentication In mutual authentication, A and B both authenticate each other.

Network level attack Security attacks attempted at the network/hardware level.

Non-repudiation Provision whereby the sender of a message cannot refuse having sent it, later on, in the case of a dispute.

One-Time Pad Considered very secure, this method involves the usage of a key, which is used only once and then discarded forever.

One-time password Technology that authenticates user based on passwords that are generated dynamically, used once, and then destroyed.

One-way authentication In this scheme, if there are two users A and B, B authenticates A, but A does not authenticate B.

Online Certificate Status Protocol (OCSP) Online protocol to check the status of a digital certificate.

Output Feedback (OFB) Mode of chaining.

Packet filter Firewall that filters individual packets based on rules. Works at the network layer.

Passive attack Form of attack on security where the attacker does not make an attempt to change the contents of the message.

Password Authentication mechanism that requires a user to enter a secret piece of information (i.e. the password) when challenged.

Password policy Statement outlining the structure, rules and mechanisms of passwords, in an organization.

Pharming Modifying the Domain Name System (DNS) so as to direct genuine URLs to false IP addresses of attackers.

Phishing Technique used by attackers to fool innocent users into providing confidential/personal information.

Plain text Message in an understandable/readable form, same as *Clear text*.

Playfair Cipher A cryptographic technique that is used for manual encryption of data. This scheme was invented by Charles Wheatstone in 1854.

Polygram Substitution Cipher Technique of encryption where one block of plain text is replaced with another, at a time.

Pretty Good Privacy (PGP) Protocol for secure email communications, developed by Phil Zimmerman.

Privacy Enhanced Mail (PEM) Protocol for secure email communications, developed by Internet Architecture Board (IAB).

Proof Of Possession (POP) Establishing the proof that a user possesses the private key corresponding to the public key, as specified in the user's digital certificate.

Proxy server Type of firewall that filters packets at the application layer of TCP/IP stack. Same as *Application gateway* or *Bastion host*.

Pseudocollision Specific case of collision in the MD5 algorithm.

Psuedo-random number Random number generated using computers.

Public Key Cryptography Standards (PKCS) Standards developed by RSA Security Inc for the Public Key Infrastructure (PKI) technology.

Public Key Infrastructure (PKI) Technology for implementing ansymmetric key cryptography, with the help of message digests, digital signatures, encryption and digital certificates.

Public Key Infrastructure X.509 (PKIX) Model to implement PKI.

Rail Fence Technique Example of transposition technique.

RC5 Symmetric key block encryption algorithm, involving variable length keys.

Reference monitor Central entity, which is responsible for all the decisions related to access control of computer systems.

Registration Authority (RA) Agency that takes some of the jobs of a Certification Authority (CA) on itself, and helps the CA in many ways.

Replay attack Form of attack wherein an attacker gets hold of a legal message, and attempts a re-transmission of the same at a later point of time.

Replay attack Attack on a system wherein the attacker gets hold of a message, and attempts to re-send it, hoping that the receiver does not detect this as a message sent twice.

Roaming certificate Digital certificate, which can be carried along as users move from one computer/location to another.

RSA algorithm Asymmetric key algorithm, widely used for encryption and digital signatures.

Running Key Cipher Techique where some portion of text from a book is used as the key.

Secure Electronic Transaction (SET) Protocol developed jointly by MasterCard, Visa and many other companies for secure credit card payments on the Internet.