STRICTLY AS PER THE NEW REVISED SYLLABUS (REV-2019 'C' SCHEME)
OF MUMBAI UNIVERSITY W.E.F ACADEMIC YEAR 2021-22
(AS PER CHOICE BASED CREDIT AND GRADING SYSTEM)

MU

CRYPTOGRAPHY AND SYSTEM SECURITY

Bachelor of Engineering
Third Year (B.E.) Degree Course in **Computer Engineering**
Semester 6



Dr. YOGESH M. GAJMAL
PRANAV MORE
OMKAR D. DIKE

www.pragationline.com
facebook.com/niralibooks
@nirali.prakashan

NIRALI PRAKASHAN
ABUNDANCE OF KNOWLEDGE

A Text Book Of

CRYPTOGRAPHY AND SYSTEM SECURITY

CSC602

Semester - VI

BACHELOR OF ENGINEERING
THIRD YEAR DEGREE COURSE
COMPUTER SCIENCE ENGINEERING BRANCH

NEW SYLLABUS AS PER REV - 2019 'C' SCHEME OF MUMBAI UNIVERSITY
WITH EFFECT FROM 2021 - 2022

Dr. YOGESH MANOHAR GAJMAL
Ph.D. in CSE, M-Tech in Computer Engineering
Associate Profesor
Finolex Academy of Management & Technology,
Ratnagiri, Maharashtra.

Mr. PRANAV MORE
M.E. Computer Network,Ph.D. in CSE (Pursuing)
Assistant Professor
School of Technology Management & Engineering
SVKM's NMIMS University, Navi Mumbai

Mr. OMKAR DATTARAM DIKE
M-Tech in CSE
Assistant Professor,
Finolex Academy of Management & Technology,
Ratnagiri, Maharashtra.

NIRALI PRAKASHAN
ADVANCEMENT OF KNOWLEDGE

N6675

CRYPTOGRAPHY AND SYSTEM SECURITY **ISBN 978-81-19116-50-8**

First Edition : September 2023

© : Authors

The text of this publication, or any part thereof, should not be reproduced or transmitted in any form or stored in any computer storage system or device for distribution including photocopy, recording, taping or information retrieval system or reproduced on any disc, tape, perforated media or other information storage device etc., without the written permission of Authors with whom the rights are reserved. Breach of this condition is liable for legal action.

Every effort has been made to avoid errors or omissions in this publication. In spite of this, errors may have crept in. Any mistake, error or discrepancy so noted and shall be brought to our notice shall be taken care of in the next edition. It is notified that neither the publisher nor the authors or seller shall be responsible for any damage or loss of action to any one, of any kind, in any manner, therefrom. The reader must cross check all the facts and contents with original Government notification or publications.

Published By :
NIRALI PRAKASHAN
Abhyudaya Pragati, 1312, Shivaji Nagar,
Off J.M. Road, Pune – 411005
Tel - (020) 25512336/37/39
Email : niralipune@pragationline.com

Polyplate

Printed By :
PRINT CORNER
1025 Sadashiv Peth
Vishal Apartment, Shop No. 4/5
Opposite Shivaji Mandir Next to Indian Bank, Pune 411030
Mobile : 9145009800, Email : pod@printcorners.in

DISTRIBUTION CENTRES

PUNE

Nirali Prakashan
(For orders outside Pune)
S. No. 28/27, Dhayari Narhe Road, Near Asian College
Pune 411041, Maharashtra
Tel : (020) 24690204; Mobile : 9657703143
Email : bookorder@pragationline.com

Nirali Prakashan
(For orders within Pune)
119, Budhwar Peth, Jogeshwari Mandir Lane
Pune 411002, Maharashtra
Mobile : 9657703145, 9890997937
Email : niralilocal@pragationline.com

MUMBAI

Nirali Prakashan
Rasdhara Co-op. Hsg. Society Ltd., 'D' Wing Ground Floor, 385 S.V.P. Road
Girgaum, Mumbai 400004, Maharashtra
Mobile : 7045821020, Tel : (022) 2385 6339 / 2386 9976
Email : niralimumbai@pragationline.com

DISTRIBUTION BRANCHES

DELHI
Nirali Prakashan
Room No. 2 Ground Floor
4575/15 Omkar Tower, Agarwal Road Darya Ganj, New Delhi 110002
Mobile : 9555778814/9818561840
Email : delhi@niralibooks.com

BENGALURU
Nirali Prakashan
Maitri Ground Floor, Jaya Apartments, No. 99, 6th Cross, 6th Main, Malleswaram, Bengaluru 560003 Karnataka; Mob : 9686821074
Email : bengaluru@niralibooks.com

NAGPUR
Nirali Prakashan
Above Maratha Mandir, Shop No. 3, First Floor, Rani Jhanshi Square, Sitabuldi Nagpur 440012 (MAH)
Tel : (0712) 254 7129
Email : nagpur@niralibooks.com

KOLHAPUR
Nirali Prakashan
New Mahadvar Road, Kedar Plaza,
1st Floor Opp. IDBI Bank
Kolhapur 416 012 Maharashtra
Mob : 9850046155
Email : kolhapur@niralibooks.com

JALGAON
Nirali Prakashan
34, V. V. Golani Market, Navi Peth, Jalgaon 425001, Maharashtra
Tel : (0257) 222 0395
Mob : 94234 91860
Email : jalgaon@niralibooks.com

SOLAPUR
Nirali Prakashan
R-158/2, Avanti Nagar, Near Golden Gate,
Pune Naka Chowk
Solapur 413001, Maharashtra
Mobile 9890918687
Email : solapur@niralibooks.com

marketing@pragationline.com | www.niralibooks.com

Also find us on www.facebook.com/niralibooks

Preface ...

We have great pleasure in presenting this text book on **CRYPTOGRAPHY AND SYSTEM SECURITY** to the students of Third year Computer Science and Engineering department. This book is written strictly according to the revised syllabus of Mumbai University Revised 2019 'C' Scheme of Mumbai University with effective from 2021-2022

We have taken utmost care to present the matter systematically and with proper flow of concepts. Here, we have posed questions of simple, difficult and intuitive type in nature. It is expected that the students should think over it and try to find the answers. This will assess the understanding of the knowledge of the Chapter.

We are thankful to Shri Dineshbhai Furia, Shri Jignesh Furia, Shri Dhairya Furia, Mrs Anagha Medhekar (Co-ordinator), Mr. Ilyas Shaikh, Ms. Shraddha (Figure Drawing), Mr. Jayant Dedhia (Marketing Executive, Mumbai) and the staff of Nirali Prakashan for the great efforts that they have taken to publish the book in time.

We are also thankful to our family members, friends, colleagues and students for their encouragement.

We welcome the valuable suggestions from our colleagues and readers for the improvement of the book.

Authors ...

Syllabus ...

1. Introduction - Number Theory and Basic Cryptography (08)

1.1 Security Goals, Attacks, Services and Mechanisms, Techniques. Modular Arithmetic: Euclidean Algorithm, Fermat's and Euler's theorem.

1.2 Classical Encryption techniques, Symmetric cipher model, mono-alphabetic and polyalphabetic substitution techniques: Vigenere cipher, playfair cipher, Hill cipher, transposition techniques: keyed and keyless transposition ciphers.

2. Symmetric and Asymmetric Key Cryptography and Key Management (11)

2.1 Block cipher principles, block cipher modes of operation, DES, Double DES, Triple DES, Advanced Encryption Standard (AES), Stream Ciphers: RC4 algorithm.

2.2 Public key cryptography: Principles of public key crysptosystems - The RSA Cryptosystem, The knapsack cryptosystem.

2.3 Symmetric Key Distribution: KDC, Needham-Shroedker protocol. Kerberos: Kerberos Authentication protocol. Kerberos: Kerberos Authentication protocol, Symmetric key agreement: Diffie Hellman, Public key Distribution: Digital Certificate: X.509, PKI.

3. Cryptographic Hash Functions (03)

3.1 Cryptographic hash functions, Properties of secure hash function, MD5, SHA-1, MAC, HMAC, CMAC.

4. Authentication Protocols and Digital Signature Schemes (05)

4.1 User Authentication, Entity Authentication: Password Base, Challenge Response Based.

4.2 Digital Signature, Attacks on Digital Signature, Digital Signature Scheme: RSA.

5. Network Security and Applications (09)

5.1 Network security basics: TCP/IP vulnerabilities (layer wise), Network Attacks: Packet Sniffing, ARP spoofing, Port scanning, IP spoofing.

5.2 Denial-of-Service: DOS attacks, ICMP flood, SYN flood, UDP flood, Distributed Denial-of-Service.

5.3 Internet Security Protocols: PGP, SSL, IPSEC. Network security: IDS, Firewalls.

6. System Security (03)

6.1 Buffer Overflow, Malicious Programs: Worms and Viruses, SQL injection.

Contents ...

1. Introduction - Number Theory and Basic Cryptography 1.1 - 1.29

1.1 Introduction to Cryptography 1.1
1.2 Security Goals 1.2
1.3 Attacks 1.3
1.4 Security Services 1.6
1.5 Security Mechanism 1.7
1.6 Techniques 1.8
1.7 Modular Arithmetic 1.10
1.8 Classical Encryption Techniques 1.13
1.9 Monoalphabetic and Polyalphabetic Substitution Techniques 1.15
1.10 Keyed and Keyless Transposition Ciphers 1.23
• Questions 1.29

2. Symmetric and Asymmetric Key Cryptography and Key Management 2.1 - 2.49

2.1 Block Cipher Principles 2.1
2.1.1 Block Cipher Modes of Operation 2.3
2.1.2 DES 2.8
2.1.3 Double DES 2.13
2.1.4 Triple DES 2.14
2.1.5 Advanced Encryption Standard 2.15
2.1.6 Stream Ciphers 2.19
2.2 Public Key Cryptography 2.22
2.2.1 Principles of Public Key Cryptosystems 2.23
2.3 Symmetric Key Distribution 2.28
2.3.1 Key Distribution Centre 2.29
2.3.2 Needham-Schroeder Protocol 2.33
2.3.3 Kerberos 2.35
2.3.4 Symmetric Key Agreement 2.37
2.3.5 Public Key Distribution 2.38
2.3.6 Digital Certificate 2.41
• Questions 2.49

3. Cryptographic Hash Functions 3.1 - 3.16

3.1 Introduction 3.1
3.2 Properties of Secure Hash Function 3.6
3.3 MD5 3.7

3.4 SHA-1 3.10
3.5 MAC 3.12
3.6 HMAC 3.13
3.7 CMAC 3.15
• Questions 3.16

4. Authentication Protocols and Digital Signature Schemes 4.1 - 4.12

4.1 User Authentication 4.1
4.2 Entity Authentication 4.2
4.2.1 Password-Based Authentication 4.2
4.2.2 Challenge Response Authentication 4.4
4.3 Digital Signatures 4.6
4.3.1 Attacks on Digital Signature 4.7
4.3.2 Digital Signature Scheme 4.7
• Questions 4.12

5. Network Security and Applications 5.1 - 5.22

5.1 Introduction 5.1
5.1.1 TCP/IP Protocol 5.2
5.1.2 The Five-Layer TCP/IP Model Vulnerabilities 5.2
5.2 Network Attacks 5.4
5.2.1 Packet Sniffing 5.4
5.2.2 ARP Spoofing 5.4
5.2.3 Port Scanning 5.5
5.2.4 IP Spoofing 5.6
5.3 Denial of Service 5.7
5.3.1 Denial of Service Attack 5.7
5.3.2 ICMP Flood 5.7
5.3.3 SYN Flood Attack 5.8
5.3.4 UDP Flood Attack 5.9
5.3.5 Distributed Denial-of-Service 5.10
5.4 Internet Security Protocols 5.11
5.4.1 PGP 5.11
5.4.2 Secure Sockets Layer 5.12
5.4.3 Internet Protocol Security (IPSec) 5.16
5.5 Network Security 5.17
5.5.1 Intrusion Detection System (IDS) 5.18
5.5.2 Firewall 5.19
• Questions 5.22

6. System Security **6.1 - 6.14**

6.1 Buffer Overflow 6.1

6.2 Malicious Programs 6.4

6.2.1 Worms 6.4

6.2.2 Viruses 6.8

6.2.3 SQL Injection 6.12

- Questions 6.14



MODULE - I

CHAPTER - 1

INTRODUCTION - NUMBER THEORY AND BASIC CRYPTOGRAPHY

SYNOPSIS

Security Goals, Attacks, Services and Mechanisms, Techniques. Modular Arithmetic: Euclidean Algorithm, Fermat's and Euler's theorem.

Classical Encryption techniques, Symmetric cipher model, mono-alphabetic and polyalphabetic substitution techniques: Vigenere cipher, playfair cipher, Hill cipher, transposition techniques: keyed and keyless transposition ciphers.

1.1 INTRODUCTION TO CRYPTOGRAPHY

Cryptography is the study of using math to hide and reveal information. Cryptography lets you store or send sensitive information over unsecure networks, like the Internet, so that only the person you want to see it can read it. Cryptography is the study of how to keep information safe, while cryptanalysis is the study of how to analyse and break secure communication. Classical cryptanalysis is a fun mix of analytical thinking, using mathematical tools, finding patterns, patience, determination, and a little bit of luck. An attacker is another word for a cryptanalyst. Both cryptography and cryptanalysis are part of cryptology.

Strong Cryptography:

"There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files."

—Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C

The strength of a cryptosystem is measured by how much time and resources it would take to get back to the plaintext. Strong cryptography makes ciphertext that is hard to figure out without the right tool. How hard is it? Even if a billion computers each did a billion checks per second, it would not be possible to figure out the answer to a strong cryptography problem before the end of the universe.

So, you might think that strong encryption would work well even against a very determined cryptanalyst. Who can say for sure? No one has shown that the strongest encryption we have now will still work with the computers of tomorrow. But the strong cryptography used by PGP is the best that can be found right now. You will be safer if you are careful and watchful than if you say you can't be broken into.

How does cryptography work?

Cryptography takes a plaintext, which is also called a cleartext, and turns it into something that only the people who are supposed to understand it can understand. If this information gets into the wrong hands, no one else should be able to understand it.

Practices of encryption are used to change a plaintext into a ciphertext. Practices for decryption are used to turn a ciphertext into a plaintext.

There are many ways to encrypt a plaintext. Some of the most common are symmetric encryption, asymmetric encryption, hashing functions, blockchain, and digital signatures. They are often used with other ways to keep computers safe.

Why is cryptography important?

As our business processes become more and more digitalized and as web-based activities like online shopping become more common, a lot more sensitive information is being passed around. Because of this, keeping personal information private has become very important, and cyber security experts now put a lot of emphasis on encryption and cryptography.

A few decades ago, hackers only went after big companies. But as private information has become easier to share and information itself has become one of the most valuable things you can own, hackers have been going after companies of all sizes and even individuals. In fact, new research shows that hackers have been going after smaller companies even more because most of them don't put much money or people into their cyber security operations. This means that they are easier to take down.

If you want to keep your business safe, you need to use cryptography and encryption in the right way. This will keep your employee information, customer data, business communications, and other things safe from people who want to hurt your business.

1.2 SECURITY GOALS

The security goals include different measures to secure the data, like confidentiality, integrity, and availability.

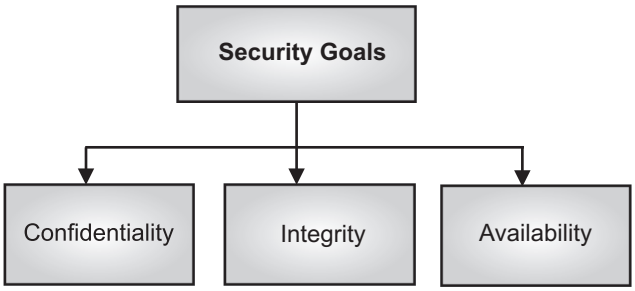


Fig. 1.1

1. Confidentiality: Keeping legal limits on who can access and share information, including ways to protect personal privacy and confidential information. When information is shared without permission, this is called a loss of confidentiality. It consists of the following two concepts:

- **Data confidentiality:** Data confidentiality makes sure that private or secret information isn't given to or shared with people who shouldn't have it.
- **Privacy:** This makes sure that each person has control over what information about them can be collected, stored, and shared, and by whom and to whom.

2. Integrity: Keeping information from being changed or deleted in the wrong way, as well as making sure information can't be disputed and is real. When information is changed or deleted without permission, this is called a loss of integrity. It consists of the following two concepts:

- **Data:** Makes sure that information and programmes can only be changed in certain ways that have been approved.
- **System:** Makes sure that a system does what it's supposed to do without being messed with by people who shouldn't be able to.

Integrity models have three goals:

- Prevent unauthorized users from making modifications to data or programs
- Prevent authorized users from making improper or unauthorized modifications
- Maintain internal and external consistency of data and programs.

Integrity checks include balancing a batch of transactions to make sure that all the information is there and correct.

3. Availability: Making sure that people can get to and use information in a timely and reliable way. When access to or use of information or an information system is cut off, this is called a loss of availability. Makes sure the system works quickly and that authorised users don't get turned away from services. Most of the time, people who work in information security deal with three common problems:

- Denial of Service (DoS) caused by attacks on purpose or by flaws in the way it was set up that haven't been found yet (for example, a programme written by a programmer who is unaware of a flaw that could crash the programme if a certain unexpected input is encountered).
- Loss of information system capabilities due to natural disasters (fires, floods, storms, or earthquakes) or human actions (bombs or strikes).
- Equipment failures during normal use.

1.3 ATTACKS

An attack is a way to get around a cryptographic system's security by finding a flaw in a code, cipher, cryptographic protocol, or key management scheme. Attacks are usually put into groups based on what the attacker does.

Attacks on security can be put into two groups: passive attacks and active attacks. A passive attack tries to get information from the system or use it, but it doesn't hurt the system's resources. Active attacks try to change system resources or interfere with how they work.

Passive Attacks:

Eavesdropping or keeping an eye on transmissions is a type of passive attack. The opponent's goal is to get the information that is being sent. The release of message contents and the traffic analysis are two types of passive attacks.

The release of message contents is easily understood (Fig. 1.2).

There may be sensitive or private information in a phone call, an email message, or a file that is transferred. We don't want an opponent to be able to figure out what these transmissions are about.

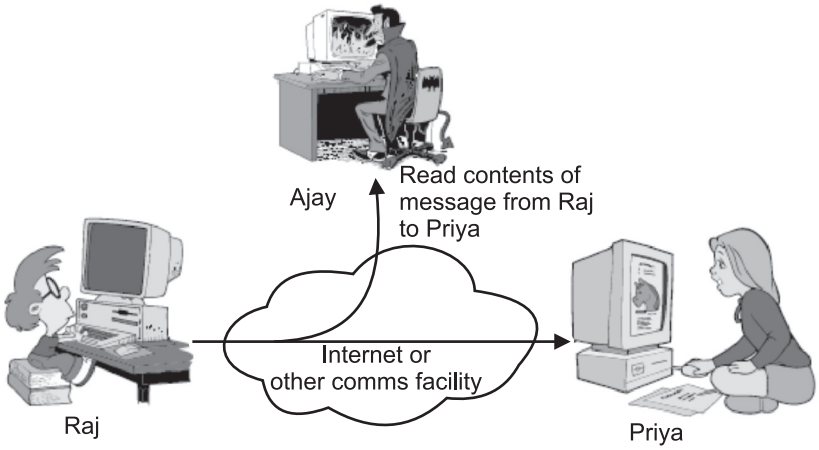


Fig. 1.2: Release of Message Contents

Traffic analysis is a second type of passive attack that is more sneaky (Fig. 1.3). Imagine that we had a way to hide the information in messages or other information traffic so that even if an opponent got a hold of the message, they couldn't figure out what it said even if they read it. Encryption is the most common way to hide information. If we had encryption protection in place, an opponent might still be able to see the pattern of these messages. The opponent could find out where and who the communicating hosts were, as well as how often and for how long they were sending messages. With this information, you might be able to figure out what kind of conversation was going on.

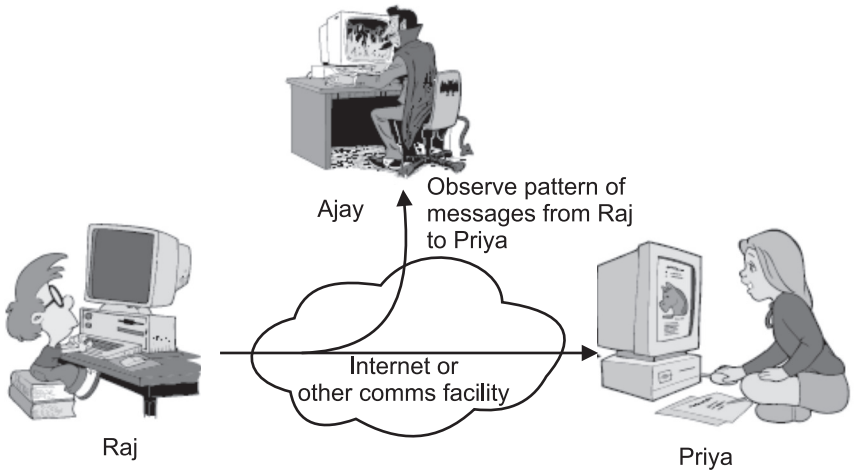


Fig. 1.3: Traffic Analysis

Passive attacks are hard to spot because they don't change the data. Most of the time, messages are sent and received in what looks like a normal way, and neither the sender nor the receiver knows that a third party has read the messages or seen the traffic pattern. But it is possible to stop these attacks from being successful, usually through encryption. So, the best way to deal with passive attacks is to stop them from happening instead of looking for them.

Active Attacks:

Active attacks involve changing the data stream or making a fake stream. There are four types of active attacks: masquerade, replay, message modification, and denial of service.

1. Masquerade: A masquerade is when one person or thing pretends to be something else (Fig. 1.4). Most of the time, one of the other types of active attack is also used in a masquerade attack. For example, authentication sequences can be recorded and played back after a valid authentication sequence has happened. This lets an authorised entity with few privileges impersonate an entity with those privileges to get more privileges.

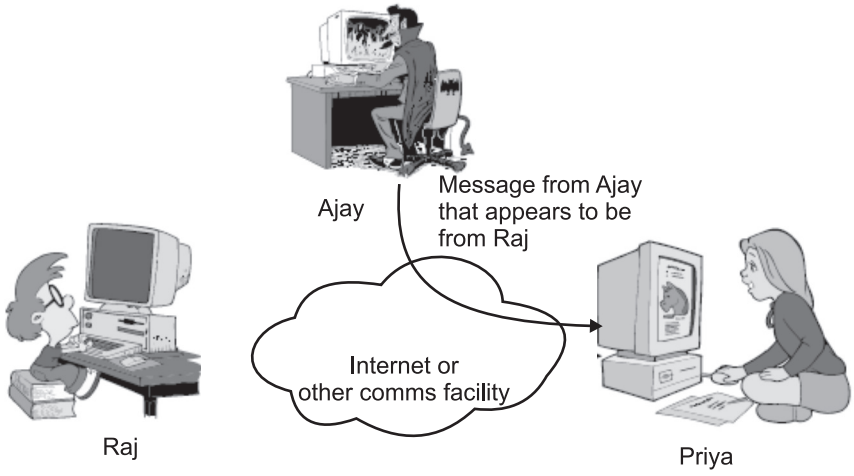


Fig. 1.4: Masquerade

2. Replay: Replay involves the passive capture of a data unit and its unauthorized retransmission. (Fig. 1.5).

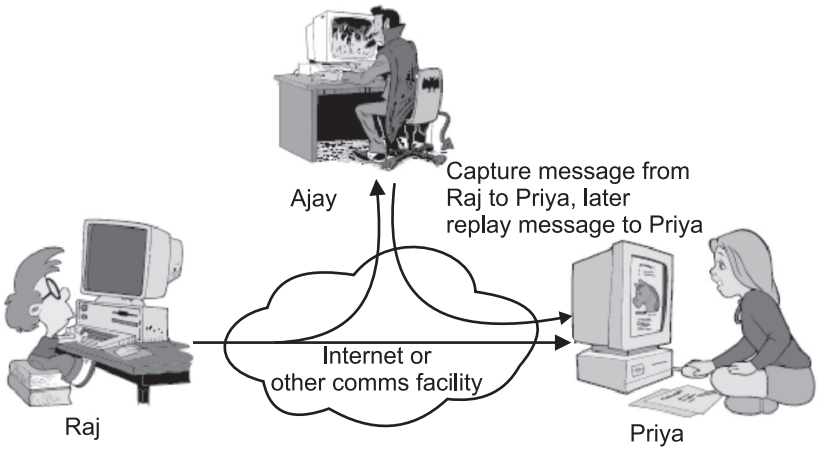


Fig. 1.5: Replay

3. Message Modification: Modification of messages just means that part of a legitimate message is changed or those messages are delayed or switched around to get an unintended result (Fig. 1.6). For example, a message that says "Allow John Smith to read confidential file accounts" is changed to say "Allow Fred Brown to read confidential file accounts.

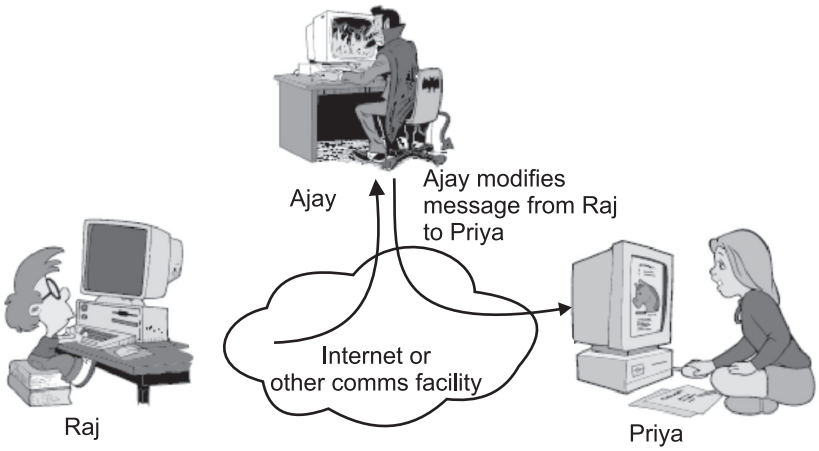


Fig. 1.6: Modification of Messages

4. Denial of Service: The denial of service makes it hard or impossible for communication facilities to be used or managed normally (Fig. 1.7). This attack could be aimed at a specific person or place. For example, an entity could stop all messages going to a certain place (e.g., the security audit service). Another way to deny service is to stop a whole network from working, either by turning it off or by sending too many messages to it so that it can't do its job as well.

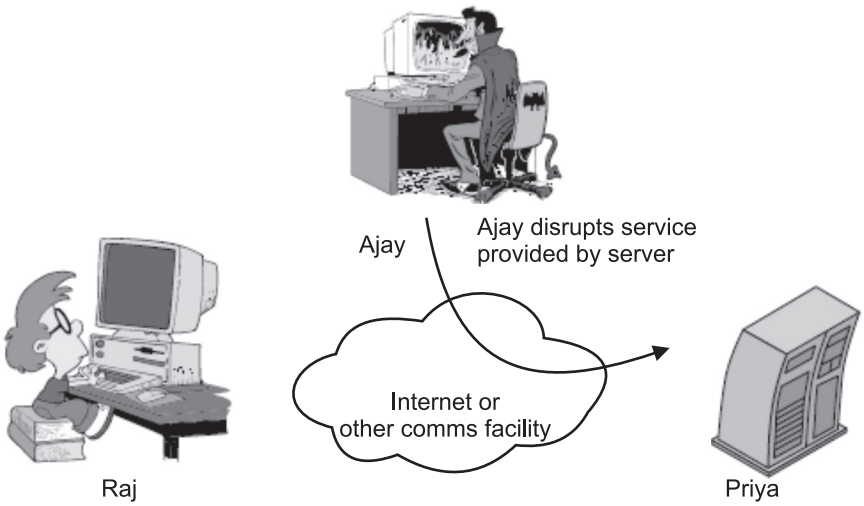


Fig. 1.7: Denial of Service

Active attacks are the opposite of passive attacks in every way. Even though passive attacks are hard to spot, there are ways to stop them from working. On the other hand, it is hard to completely stop active attacks because there are so many possible physical, software, and network weaknesses. Instead, the goal is to find attacks that are already happening and fix any problems or delays they cause. If the detection works as a deterrent, it could also help stop the crime.

1.4 SECURITY SERVICES

Security Service is a processing or communication service that improves the safety of an organization's data processing systems and information transfers. The services are meant to protect against security attacks. To do this, they use one or more security mechanisms.

1. Confidentiality:

Confidentiality is protecting data from passive attacks while it is being sent. It is used to stop information from getting out to people or systems that shouldn't have it. It has been defined as "making sure that only people who are allowed to see information can see it." The other part of privacy is making sure that traffic flow can't be analysed.

Example: A credit card number has to be secured during online transaction.

2. Authentication:

This service makes sure that a message is real. For a single message, its job is to let the recipient know that the message came from the right place. There are two parts to a relationship that keeps going. First, when the connection is first made, the service makes sure that both parties are real. Second, the connection between the two hosts is not interrupted, so a third party can pretend to be one of the two parties. X.800 specifies two different kinds of authentication services.

- **Peer entity authentication**: Checks the identities of the entities that are talking to each other. It can be used when setting up a connection and while data is being sent. Gives assurance against a disguise or a replay attack
- **Data origin authentication**: This assumes that the source of a data unit is real, but it doesn't protect against data units being copied or changed. Supports applications like e-mail where the people talking to each other have never talked to each other before.

3. Integrity:

When data has integrity, it means that it can't be changed without permission. It can be used on a stream of messages, a single message, or certain fields within a message, just like confidentiality. There are two kinds of integrity services.