

**Experiment No. 7**

**Title: Password Cracking using Burp Suite**

(Autonomous College Affiliated to University of Mumbai)

**Batch: B1 Roll No.:1914078 Experiment No.:7**

**Title: Explore the burp suite**

**Resources needed:** Burp suite Professional.

**Procedure / Approach /Algorithm / Activity Diagram:**

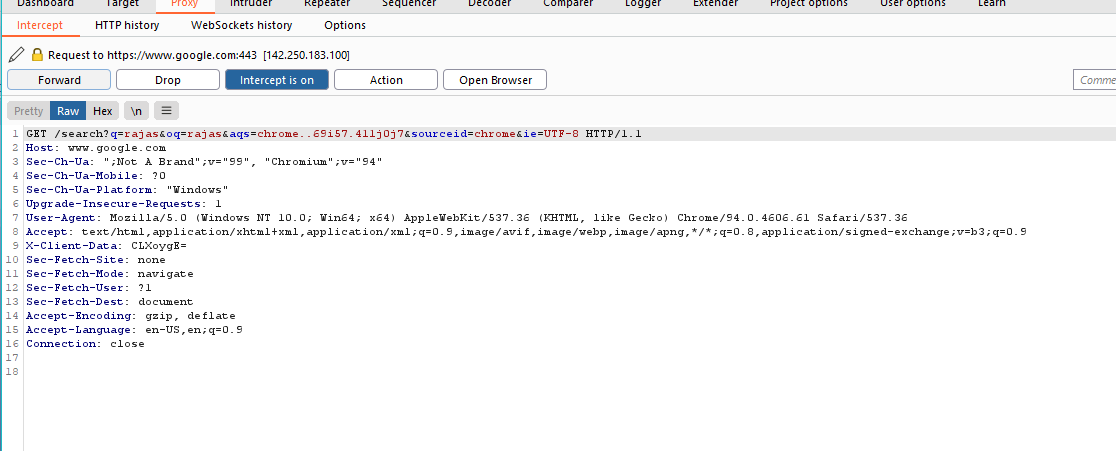
* Burp Suite has been installed
* DVWA ( Damn vulnerable Web Application) has been installed carry out the the further procedure.
* **Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.**

**Implementation:**

**Task1: Explain dictionary attack step by step using Burp Suite (Including screenshots)**

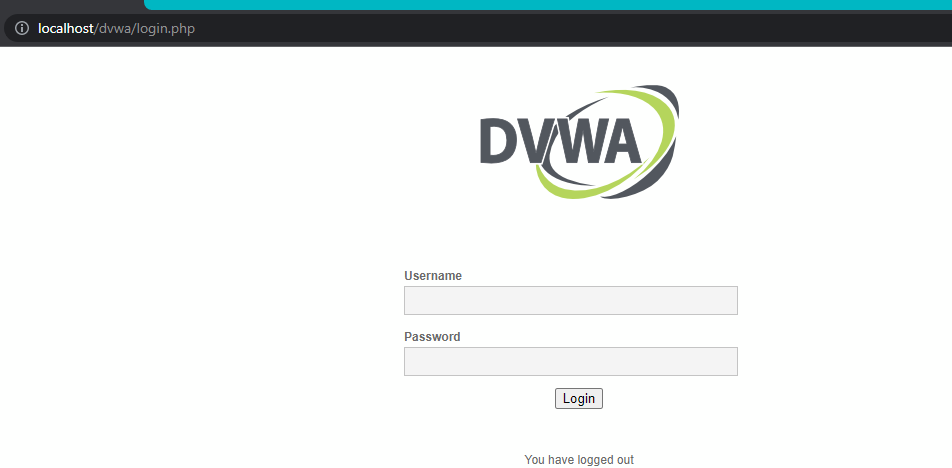
1: **Interception on Burp suite**

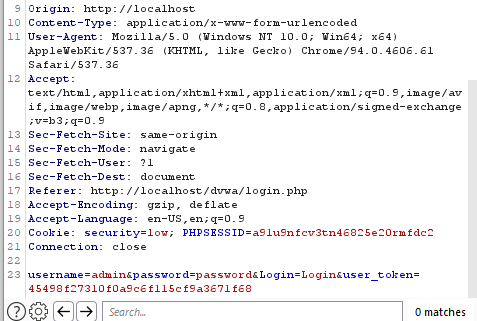
(Random search on google)



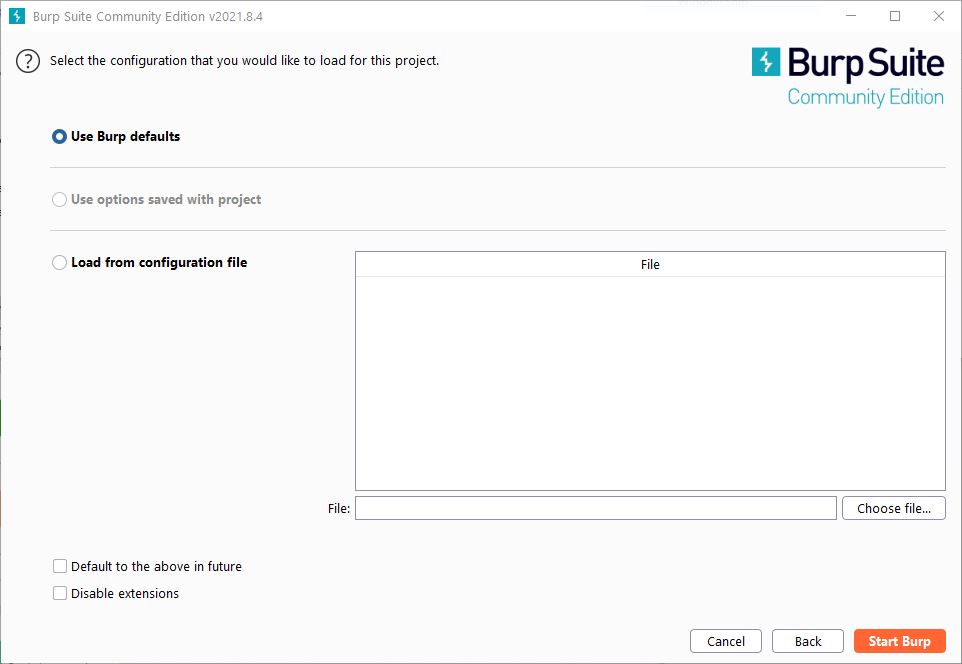
2. **Logging in dvwa (set security to low)**

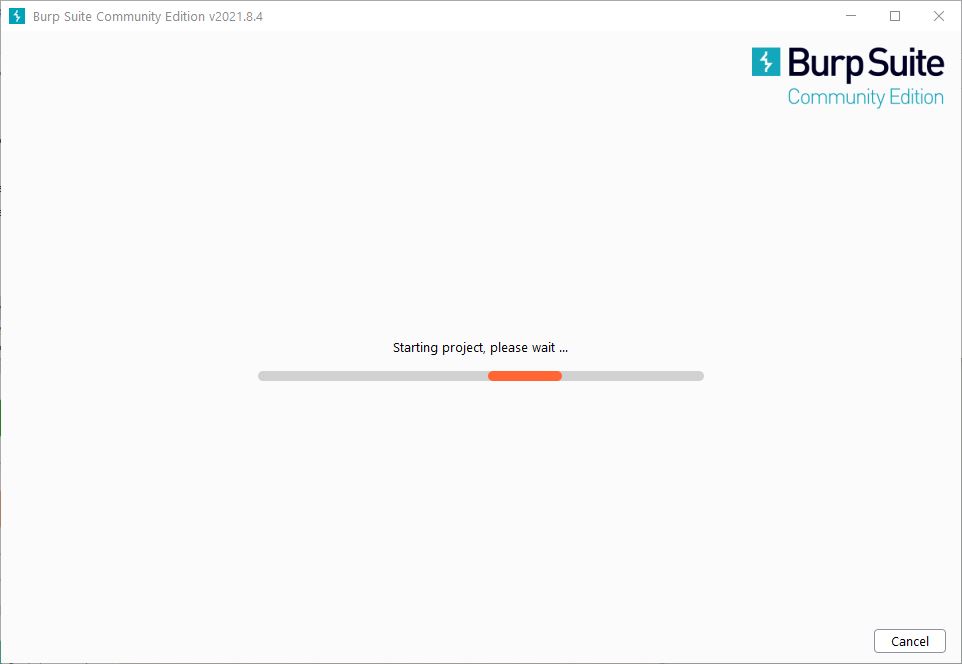
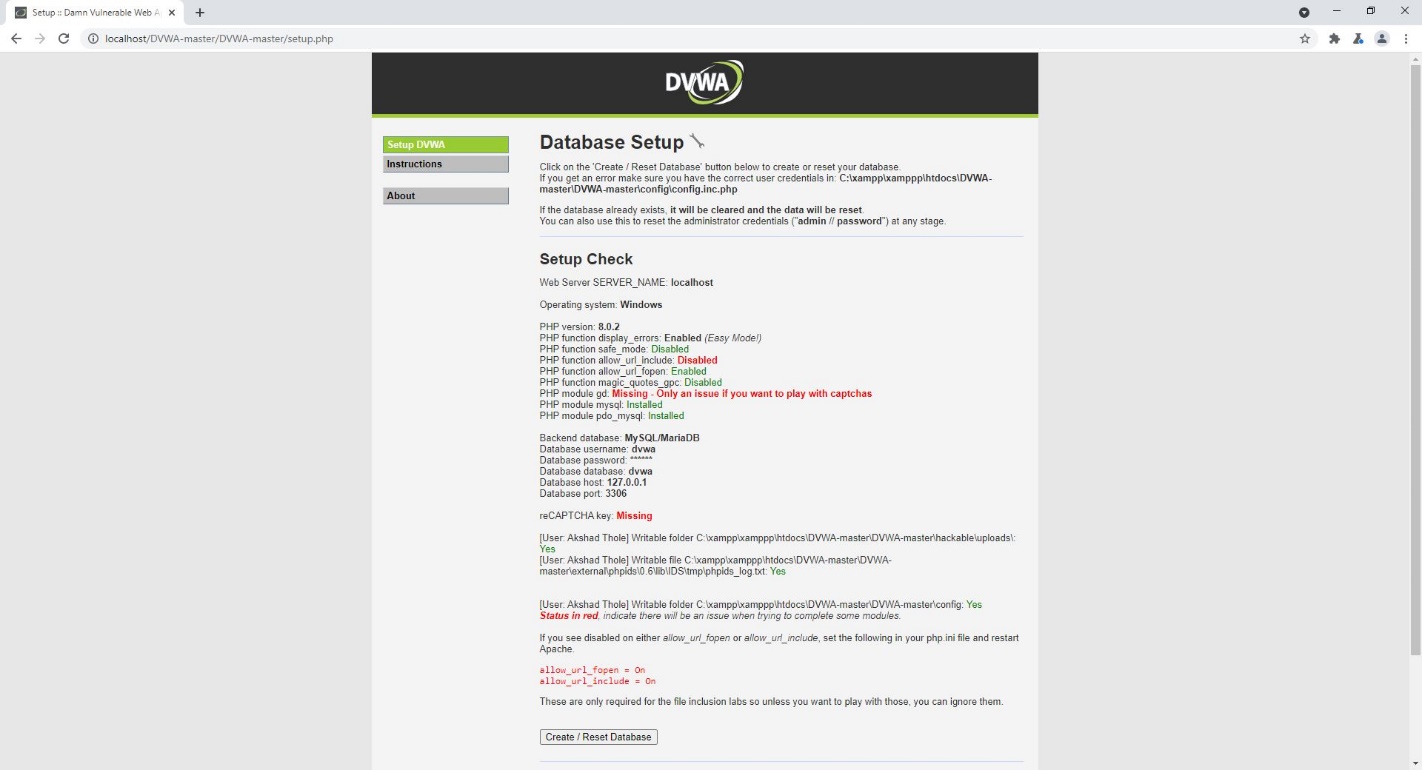
* Login: admin-password
* Picking up the packet and then selecting Action- send to intrude
* Setting payload and marking fields of username and password

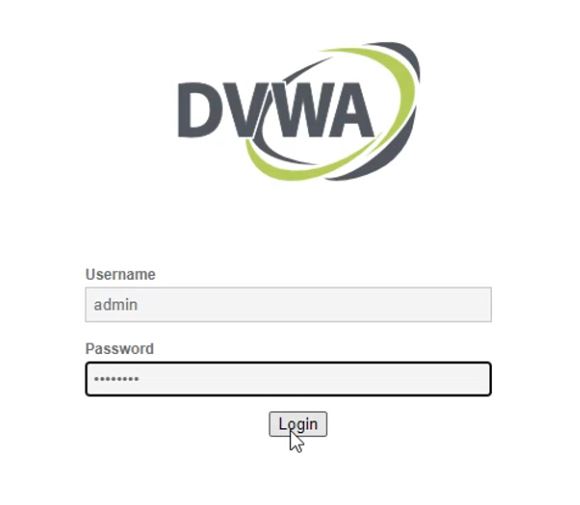




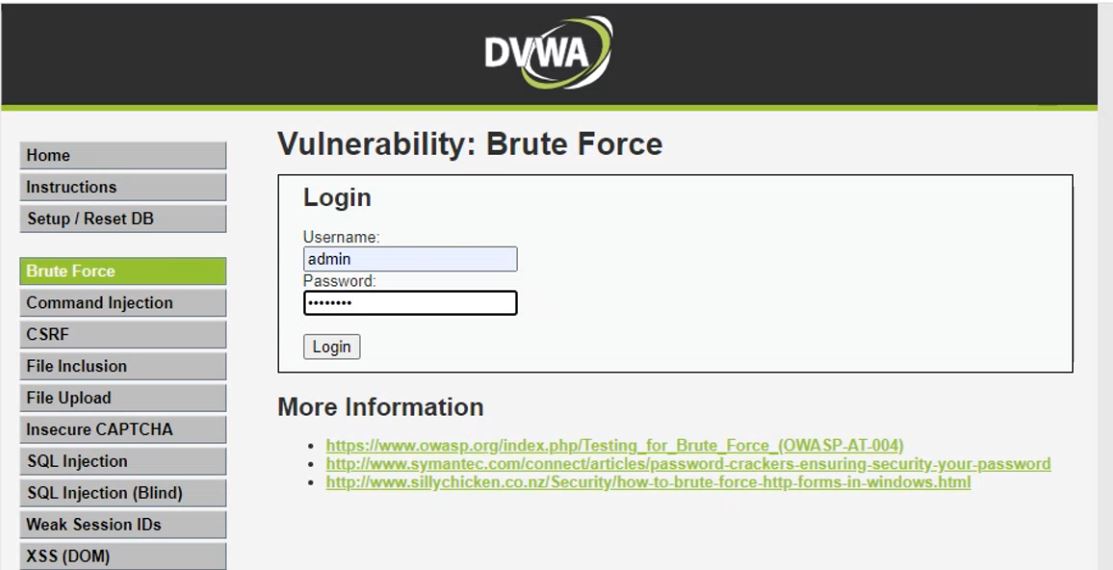
3. **The request packet is displayed on burp suite**

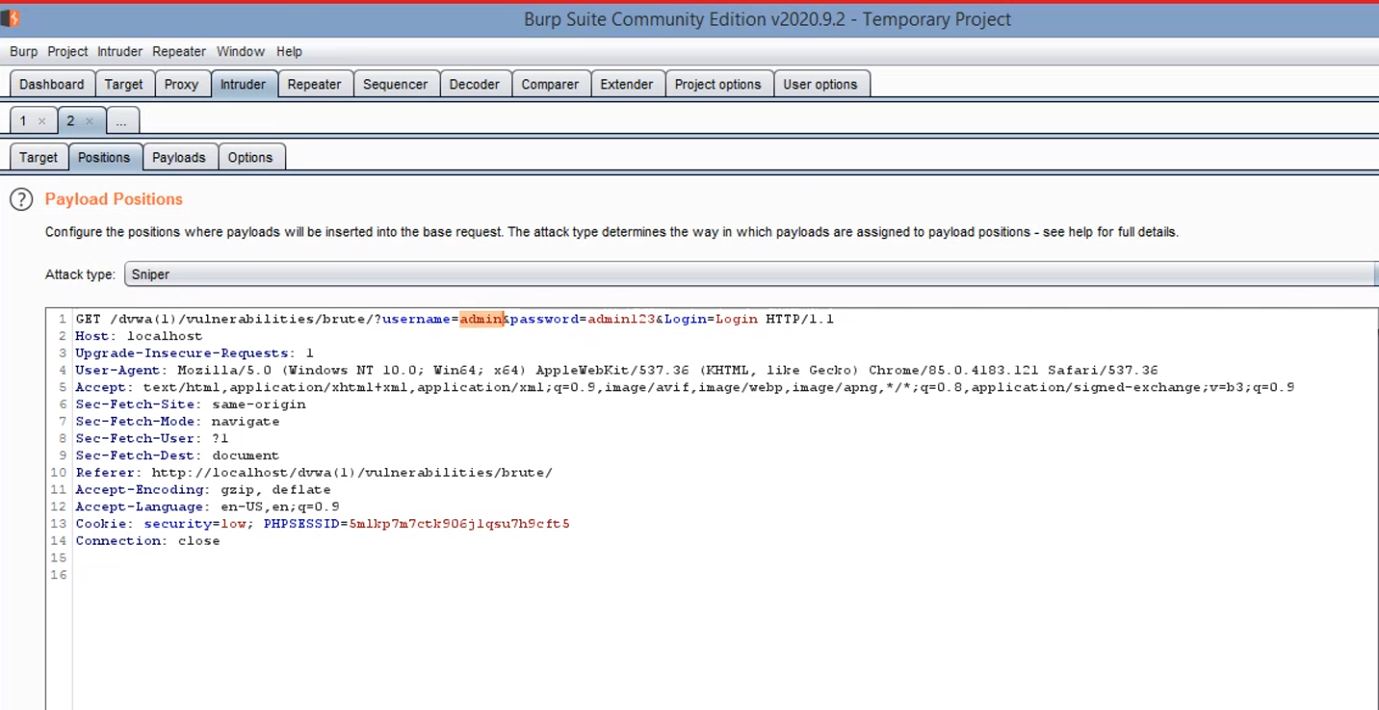


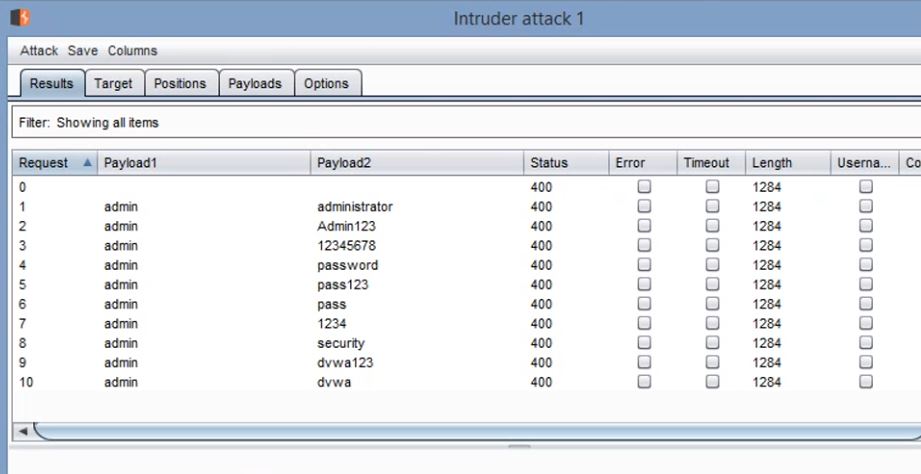


4. **Starting the brute force attack.**

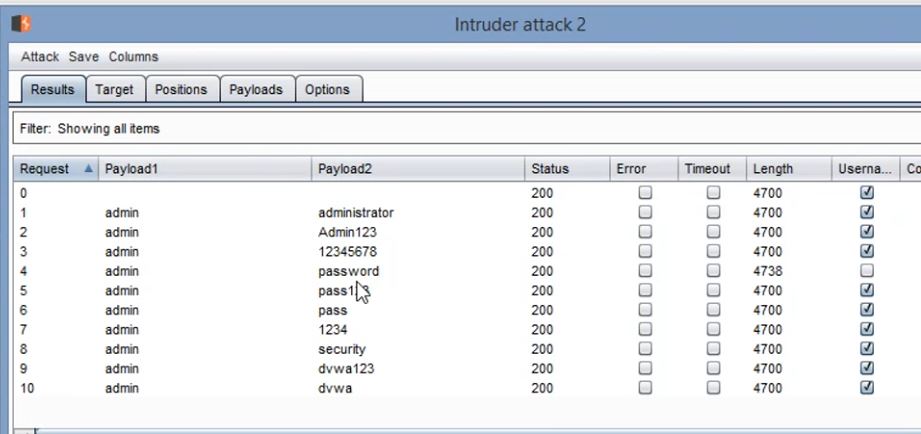




**5. Adding number of possible usernames in payload 1 and adding number of possible passwords in payload 2 and Setting grep match allowing us to detect which password and username combination didn’t work.**



**6. This shows us that every combination didn’t worked apart from admin and password combination**



**Task2: Explore any web exploit.**

* **Cross Site Request Forgery (CSRF):** This is an example of a confused deputy attack whereby the browser is fooled by some other party into misusing its authority. A 3rd party site, for example, can make the user’s browser misuse it’s authority to do something for the attacker.

In the case of CSRF, a 3rd party site issues requests to the target site (e.g., your bank) using your browser with your cookies / session. If you are logged in on one tab on your bank’s homepage, for example, and they are vulnerable to this attack, another tab can make your browser misuse its credentials on the attacker’s behalf, resulting in the confused deputy problem. The deputy is the browser that misuses its authority (session cookies) to do something the attacker instructs it to do.

An example for this could be –

Attacker Anna wants to lighten target Tom’s wallet by transfering some of his money to her. Tom’s bank is vulnerable to CSRF. To send money, Tom has to access the following URL:

http://example.com/app/transferFunds?amount=1500&destinationAccount=4673243243

After this URL is opened, a success page is presented to Tom, and the transfer is done. Anna also knows, that Tom frequently visits a site under her control at blog.aliceisawesome.com, where she places the following snippet:

<img src=http://example.com/app/transferFunds?amount=1500&destinationAccount=4673243243 width=0 height=0 />

Upon visiting Anna’s website, Tom’s browser thinks that Anna links to an image, and automatically issues an HTTP GET request to fetch the picture, but this actually instructs Tom’s bank to transfer $1500 to Anna.

# Questions:

1. **What is the difference between professional Burp suite and open-source Burp suite? (Justify your answer with features).**

**Ans)**

**Burp Suite Free Edition** (i.e. Community Edition) contains everything you need to carry out manual security testing of web applications.

You can:

* Inspect and modify traffic between the browser and the target application, using the intercepting Proxy.
* Crawl application content and functionality, with the application-aware Spider.
* Manipulate and resend individual requests, using the Repeater tool.
* Benefit from various other handy utilities for analysing and decoding application data.

**Burp Suite Professional** contains numerous powerful features to make your work faster and more effective, letting you find more vulnerabilities in a shorter time.

You can:

* Automatically probe for security flaws, with the state-of-the-art web application Scanner.
* Discover and exploit complex and unusual vulnerabilities, using the Intruder tool to deliver powerful customized attacks.
* Save your Burp session and resume working later.
* Benefit from numerous high-value features, including search, target analysis, content discovery, and task scheduling.
* Receive frequent product updates and earlier access to new releases.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Outcomes: CO4: Understand Security issues related to Software, Web and Networks.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Conclusion:** We understood and implemented the password cracking using burp suite.

# Grade: AA / AB / BB / BC / CC / CD /DD

**Signature of faculty in-charge with date**

**References:**

**Books/ Journals/ Websites:**

* + Mark Stamp, “Information security Principles and Practice” Wiley
  + Behrouz A. Forouzan, “Cryptography and Network Security”, Tata McGraw Hill.
  + William Stalling, “Cryptography and Network Security”, Prentice Hall.