Experiment-1

Cryptanalysis of Caesar Cipher using Frequency Analysis

Date:_____

AIM

Cryptanalysis of Caesar Cipher using Frequency Analysis

PROCEDURE

Step-1: Take sample encrypted message.

Step-2: Use Notepad and find the frequency of all letters appearing in the intercept.

Step-3: Know the frequency of characters in English.

Step-4: Use the Ctrl + R in the notepad, set the match case and start substituting one by one letters to get the final decrypted text.

SOURCECODE

Encrypted Message:

GFS WMY OG LGDVS MF SFNKYHOSU ESLLMRS, PC WS BFGW POL DMFRQMRS, PL OG CPFU M UPCCSKSFO HDMPFOSXO GC OIS LMES DMFRQMRS DGFR SFGQRI OG CPDD GFS LISSO GK LG, MFU OISF WS NGQFO OIS GNNQKKSFNSL GC SMNI DSOOSK. WS NMDD OIS EGLO CKSJQSFODY GNNQKKSFNSL GC SMNI DSOOSK. WS NMDD OIS EGLO CKSJQSFODY GNNQKKPFR DSOOSK OIS 'CPKLO', OIS FSXO EGLO GNNQKKPFR DSOOSK OIS 'LSNGFU' OIS CGDDGWPFR EGLO GNNQKKPFR DSOOSK OIS 'OIPKU', MFU LG GF.

QFOPD WS MNNGQFO CGK MDD OIS UPCCSKSFO DSOOSKL PF OIS HDMPFOSXO LMEHDS. OISF WS DGGB MO OIS NPHISK OSXO WS WMFO OG LGDVS MFU WS MDLG NDMLLPCY POL LYEAGDL. WS CPFU OIS EGLO GNNQKKPFR LYEAGD MFU NIMFRS PO OG OIS CGKE GC OIS 'CPKLO' DSOOSK GC OIS HDMPFOSXO LMEHDS, OIS FSXO EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'LSNGFU' DSOOSK, MFU OIS CGDDGWPFR EGLO NGEEGF LYEAGD PL NIMFRSU OG OIS CGKE GC OIS 'OIPKU' DSOOSK, MFU LG GF, QFOPD WS MNNGQFO CGK MDD LYEAGDL GC OIS NKYHOGRKME WS WMFO OG LGDVS.

Step-1

Open the encrypted message only in Notepad.

Step-2

Find the frequency of each letter in the encrypted message to find the frequency of all the letters appearing in the intercept. For this intercept we get the values given in the table below.

Ciphertext Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency	5	2	26	42	23	51	67	8	33	1	35	39	35	29	85	30	14	17	88	0	17	3	16	6	10	0

Ciphertext Letter	S	O	G	F	D	L	K	M	I	P	N	C	E	R	U	W	Q	Y	H	X	A	V	B	J	T	Z
Frequency	88	85	67	51	42	39	35	35	33	30	29	26	23	17	17	16	14	10	8	6	5	3	2	1	0	0

Step-3

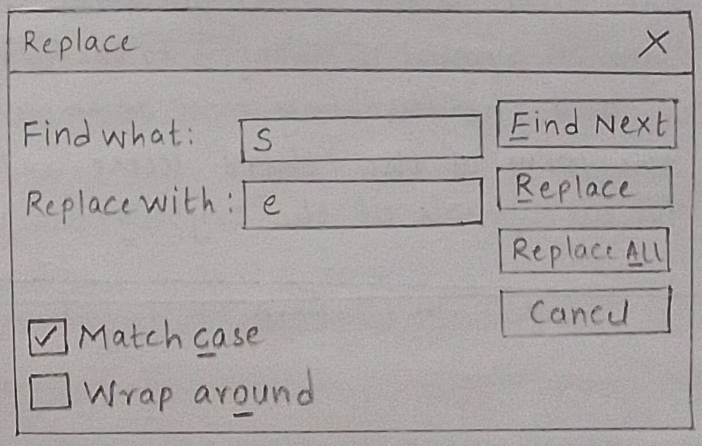
Follow the table below to find the characters to be substituted for the given encrypted menage.

Table 1 Frequency of character in English

Letter	Frequency	Letter	Frequency	Letter	Frequency	Letter	Frequency
E	12.7	H	6.1	W	2.3	K	0.08
T	9.1	R	6.0	F	2.2	J	0.02
A	8.2	D	4.3	G	2.0	Q	0.01
O	7.5	L	4.0	Y	2.0	X	0.01
I	7.0	C	2.8	P	1.9	Z	0.01
N	6.7	U	2.8	B	1.5		
S	6.3	M	2.4	V	1.0		

Step-4:

click ctrl+R in the notepad



click the check box: Match case

Step-5:

Start substituting one by one letters by following the sequence

S→e O→t I→h G→o F→n M→a X→x

W→w B→k U→d D→I K→r P→i L→s V→v

H→p A→b X→x Y→y E→m N→c C→f

OUTPUT

R → g Q → u J → q

Step-6:

Final decrypted text will be as shown below.

Week1 - Notepad

File Edit Format View Help

one way to solve an encrypted message, if we know its language, is to find a different plaintext of the same language long enough to fill one sheet or so, and then we count the occurrences of each letter. we call the most frequently occuring letter the 'first', the next most occuring letter the 'second' the following most occuring letter the 'third', and so on, until we account for all the different letters in the plaintext sample. then we look at the cipher text we want to solve and we also clasify its symbols. we find the most occuring symbol and change it to the form of the 'first' letter of the plaintext sample, the next most common symbol is changed to the form of the 'second' letter, and the following most common symbol is changed to the form of the 'third' letter, and so on, until we account for all symbols of the cryptogram we want to solve.

VIVA QUESTIONS

1. What is cryptography?

Ans. Cryptography is the practice and study of techniques for securing communication and data from unauthorized access by converting it into a coded format.

2. What is cryptanalysis?

Ans. Cryptanalysis is the science of analyzing and breaking cryptographic coder and ciphers to gain accer to the original information without knowing the key.

3. What is cipher text?

Ans. Cipher text is the encrypted version of the original plain text, which is unreadable without the correct decryption key.

4. What is the ceaser cipher?

Ans. The Caeser cipher is a simple substitution cipher where each letter in the plain text is shifted a fixed number of places down or up the alphabet.

5. What is a symmetric key cryptosystem?

Ans. A symmetric key cryptosystem is an encryption method where the same key is used for both encryption and decryption of the data.

Experiment-2

Cryptanalysis of RSA

Date:_____

AIM

Implementation of Cryptanalysis using RSA.

PROCEDURE

Step-1: Install VMWare and host Kali Linux.

Step-2: Login to Kali Linux and open Terminal and run commands.

Step-3: Use Hexadecimal to decimal convertor.

Step-4: Use factordb.com to find the factors for the decimal value.

Step-5: Write an exploit in python and get the plain text.

SOURCECODE

Steps

1. Create a folder name 'rsa' in kali linux desktop.
2. Open browser, in github download three files,
   enc.txt exploit.py pubkey.pem
   GitHub link - https://github.com/rampriyakilari/ICS-Needs
3. Copy those three files and paste in rsa folder.
4. Now open cmd in Kali and type commands.

→ $ cd Desktop

→ $ cd rsa

→ $ ls

It lists all the files as follows.

enc.txt exploit.py pubkey.pem

→ $ cat pubkey.pem

It is used to access the content of the file.

→ $ openssl rsa -pubin -inform PEM -text -noout < pubkey.pem

→ $ touch exploit.py

→ $ pip install pycryptodome

→ $ python exploit.py

→ $ openssl pkeyutl -decrypt -in enc.txt -out dec.txt
-inkey private.pem

→ $ cat dec.txt

It displays output as

RSAisEasy

VIVA QUESTIONS

1. What is RSA?

Ans. RSA is a widely used encryption algorithm that secures data using a pair of keys - public and private - for secure communication.

2. What is public key encryption?

Ans. Public key encryption uses two keys: one for encrypting (public key) and one for decrypting (private key). Only the intended recipient can decrypt the message.

3. What is an asymmetric key cryptosystem?

Ans. An asymmetric key cryptosystem uses two different keys - one for encryption and one for decryption, such as RSA, ensuring secure communication.

4. Why do we need to use kali linux?

Ans. Kali Linux is used for ethical hacking, penetration testing, and security research because it includes many pre-installed security tools.

5. What is an exploit?

Ans. An exploit is a method or tool used to take advantage of vulnerabilities in software or systems to gain unauthorized access.

6. What is the command to create an empty file in the kali linux?

Ans. The command to create an empty file is:

touch filename

Experiment-3

Examination of a Website to Test the Vulnerability of Attacks – DVWA Setup & SQLi

Date:_____

AIM

Examination of a website to test the vulnerability of attacks – DVWA setup & SQLi.

PROCEDURE

Step-1: Login the kali linux. Open browser and search for DVWA—a vulnerable website.

Step-2: Install DVWA in Kali using Terminal

Step-3: Copy config.inc.php.dist and in new file change the login credentials.

Step-4: start mysql service and login to it.

Step-5: Create a database, user and add permissions to that user and exit from the database.

Step-6: Start apache service and open browser and search for http://localhost/DVWAor http://127.0.0.1/DVWA/login.php

Step-7: login to DVWA. Goto DVWA Security click on impossible and change it to LOW.

Step-8: Attack the system using SQLinjection

SOURCECODE

1 Open cmd in Kali

→ $ cd ..

→ $ cd ..

→ $ ls

2. List all files. we need to go to var file

→$ cd var

→$ ls

3. List the files. we need to go to www directory

→$ cd www

→$ ls

4. List all the files and go to html file.

→$ cd html

→$ ls

5. Go to browser and search dvwa, and go to github link. Under the code section, copy the link from clone and paste it.

→$ sudo git clone https://github.com/digininja/DVWA.git

6. password for cloning is "kali"

→$ ls

7. create dvwa8

→$ sudo mv DVWA dvwa8

→$ ls

8. change directory to dvwa8

→$ cd dvwa8

→$ ls

9. It lists all the files, go to config file.

→$ cd config

→$ ls

config.inc.php.dist

10. We have to make this into a php file.

→$ sudo cp config.inc.php.dist config.inc.php

→$ ls

config.inc.php config.inc.php.dist

11. Open the config.inc.php file
→ $ sudo nano config.inc.php
12. To open the file, we have to change the following
db_database = 'dvwa8', db_user = 'admin',
db_password = 'password'
13. Now hold ctrl and press x, y and then Enter.
14. Check if the changes are done in the file displayed.
→ $ cat config.inc.php
15. Remember server number '127.0.0.1', username and password
→ $ sudo service mysql start
→ $ sudo mysql -u root -p
16. Enter password as "kali" and click Enter.
→ 17. MariaDB > show databases;
Now it will display all databases.
Now we have to create a new dvwa8 database.
→ 18. MariaDB > create database dvwa8;
→ 19. MariaDB > show databases;
→ 20. MariaDB > grant all on dvwa8.* to admin@127.0.0.1;
Here we are checking the created database and granting the permission.
21. To exit, type - exit;
→ MariaDB > exit;
→ $ cd /etc
→ $ ls
→ $ cd php
→ $ cd 8.2
→ $ cd apache2

OUTPUT

→$ ls
conf.d php.ini
→$ sudo nano php.ini
Enter password: Kali

22. Press ctrl+w, type fopen and press Enter.

In Fopen wrappers

23. check allow_url_fopen = On and allow_url_include = On.
These should be On. If its is in off change to On.

24. Now hold ctrl and press X, y and then Enter.

→ $ sudo service apache2 start

25. Open browser and type https://127.0.0.1/dvwa8/login.php, type username as 'admin' and password as 'password' and click on login. Click on reset database and login again.

26. Click on DVWA security and change to low and submit.

Now attacking the system,

27. For this, click on SQL injection, in user ID, enter 1 and submit, it displays the information in database.

28. You can also try to retreive the data with id's 2, 3 .. as well.

29. Enter %' or '1' = '1 and Submit.
You will get all the information.

30. Note: If any error occur while granting permission in database just type command -
Create user 'admin'@'127.0.0.1' identified by 'password'

VIVA QUESTIONS

1. What is an attack? List its types?

Ans. An attack is an attempt to access, damage, or disrupt a system without authorization. Types :- 1) Passive Attacks (e.g., eavesdropping) 2) Active Attacks (e.g., denial-of-service) 3) Insider Attacks 4) External Attacks.

2. What is VMWare and it's advantages?

Ans. VMWare is a virtualization platform that allow users to run multiple OS on a single computer by creating virtual machines. Adv :- Security, Resource management, cloud computing etc.

3. What is SQL Injection attack?

Ans. SQL Injection is a code injection technique that exploits vulnerabilities in an application's software by inserting malicious SQL queries into input fields. It is also a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed.

4. What is the command used to clear the privileges in kali linux?

Ans. reset or clear commands can be used to reset terminal privileges or clear the terminal screen.

5. What is a DVWA?

Ans. DVWA (Damn Vulnerable Web Application) is a PHP/MySQL web application designed to help security professionals test their skills and tools in a legal environment.
It is a software project that intentionally includes security vulnerabilities and is intended for educational purposes.

Experiment-4

Examination of a Website to test the Vulnerability of Attacks

Date:_____

AIM

Examination of a website to test the vulnerability of attacks– XSS & CSRF & Command Line injection attack.

PROCEDURE

Use previous experiment to setup DVWA

Step-1: If the DVWA website setup is done run apache and my sql service in the terminal and open a browser to access the website.

Step-2: Change the level of DVWA security.

Step-3: Click Command Injection and run IP address to test.

Step-4: Click and test XSS Reflection.

Step-5: Click and test CSRF Attack

SOURCECODE

→ $ sudo service apache2 start

→ Goto browser and give http://localhost/DVWA or http://127.0.0.1/DVWA/login.php

→ Now Goto DVWA security click on impossible and set it as low and click submit.

→ Now click on Command Injection and Enter IP address. You will get the output when you submit.

- XSS Attack

→ click on XSS Reflection
→ Enter any name in the text box and click submit.
→ It will display as

Hello + "your entered text"

- CSRF Attack

→ click on CSRF, enter username and password which are used for DVWA login. Click on login.

VIVA QUESTIONS

1. What is XSS attack?

Ans. Cross-site scripting (XSS) is an attack in which an attacker injects malicious executable scripts into the code of a trusted application or website

2. What is command injection attack?

Ans. It is an attack in which the goal is execution of arbitrary commands on the host os via a vulnerable application.

3. What is the full form of CSRF and what is it?

Ans. Cross - Site Request Forgery is a type of cyber attack that tricks a user in to performing unwanted actions on a website they are already authenticated to.

4. What is payload?

Ans. Payload in the context of malware refers to malicious code that causes harm to the targeted victim.

5. What are the benefits of using kali linux?

Ans. Open source, secure environment, Extensive toolset, Regular updates, Forensic tools, customization and flexibility.

Experiment-9

Implementation of IT Audit, Malware Analysis and Vulnerability Assessment and Generate the Report

Date:_____

AIM

Implementation of IT Audit, malware analysis and Vulnerability assessment and generate the report.

PROCEDURE

Step-1: Collect information about malware

Step-2: Get the basic information about malware

Step-3: Get the report from filescan.io and virustotal.com

Step-4: Perform IT Audit to get the port information

SOURCECODE

Steps for Filescan.io (a malware analysis platform)

1. Download the malware file from github/browser. (malware.rar)
   Github link - https://github.com/rampriyakilari/ICS-Needs
2. Go to the downloaded location of the malware file.
3. Give right click on the malware file and click on "extract here" now file.exe appears.
4. Now open browser and type "Filescan.io".
5. Now Drag and Drop the file.exe in it.

6. It shows a dialog box, it shows 4 options in that just select last option.
   "I consent to the Terms of Use and Privacy Policy"
7. click on upload
8. Now it checks uploaded file whether it is malicious or not.

Steps for VirusTotal

1. Download the malware file from github/browser.
2. Go to the downloaded location of the malware file.
3. Give right click on the malware file and click on "extract here" now file.exe appears.
4. Now open browser and type "Virustotal".
5. Now Drag and Drop the file.exe in it.
6. It shows a dialog box, it shows 4 options in that just select last option.
   "I consent to the Terms of Use and Privacy Policy"
7. click on upload
8. After the file is uploaded, VirusTotal will automatically start scanning it. You may see a progress indicator showing that the file is being analyzed.
9. Once the scan is complete, VirusTotal will display the results on a new page.

   This report typically includes:

   - Detection status (e.g., clean, infected, suspicious).
   - A summary of findings from various antivirus engines (e.g., how many engines flagged the file).

- Additional details such as file metadata, behaviour analysis and more.

VIVAQUESTIONS

1. What is malware?

Ans. Malware is malicious software designed to harm or exploit any device, network, or service, such as viruses, trojans, or ransomware.

2. What is port scanning?

Ans. Port scanning is a technique used to identify open ports and services available on a networked system, often used for network security analysis.

3. List out any two websites used to get the malware analysis report?

Ans.
- VirusTotal
- Hybrid Analysis

4. What is nmap/Zenmap tool? Why is it used?

Ans. Nmap (or Zenmap, its GUI version) is a network scanning tool used to discover hosts and services on a network, helping in security Auditing (Examining and Evaluating of Security)

5. How is malware collected?

Ans. Malware is collected by using honeypots, analyzing suspicious files, or through network monitoring tools like packet sniffers.