THIS PIECE OF STUDY MATERIAL HAS BEEN BROUGHT TO YOU BY

MUSTUDENTS UNITED

contributed by - Iram Mohd Ahmed Shaikh

of college - M.H Saboo Siddik College

Anjuman – I - Islam's

M.H SABOO SIDDIK COLLEGE OF ENGINEERING

8, Saboo Siddik Polytechnic Rd., Byculla, Mumbai – 400 008.

Department of C. S. E. (AI & ML)

(2022-2025)

Subject Name: CSS
Subject Code:

Assignment No:	1
Title:	Module 1,2,3
Date of Performance:	13/3/24
Date of Submission:	22/3/24
Roll No:	211714
Name of the Student:	Sram Mohd Ahmed Shaikh.

Evaluation:

Sr. No	Rubric	Marks
1	On time Submission & Completion (2)	2
2	Technical Content (2)	2
3	Presentation & Organization (1)	1

13/24

Q1 Explain playfair cipher. Solve the following
plain text : attack
Key : monarchy

Playfair Cipher is a multiple letter encryption technique, which uses 5x5 matrix table to store the letters of the phrase given for encryption which letter on becomes key for encryption and decryption.

In the first step all letters are to be filled in that matrix from left to right, the letters which are already been placed is not be placed again in that matrix.

After filling up of the given letter, fill rest of the space in the matrix with the remaining letters alphabetically with no repetitions.

The letter I and J will be considered as one letter. So if I is already placed then no need to place J in rest of the matrix

The letters which are already written/mentioned need not to be placing that letter in given matrix.

Example:
plain text : attack
key : monarchy

m	o	n	a	r
c	h	y	b	d
e	f	g	i/j	k
l	p	q	s	t
u	v	w	x	z

The message is attack divided the letter's into the set of two characters.

plain text : attack

at
ta
ck

cipher text :

at → rs
ta → sr
ck → de

ciphertext : rs sr de
Decrypt : at ta ck
text : attack

Explain (AES) Advanced Encryption Standard

Advanced Encryption Standard (AES) is a Symmetric key block cipher that can encrypt and decrypt data using keys of 128, 192, or 256 bits. AES was ~~developed~~ adopted by the U.S government as a standard in 2001, and is widely used for securing sensitive data. AES is based on a mathematical structure called a substitution-permutation network, which consist of a series of transformation that mix the input data and the key. AES operates on blocks of the 16 bytes (128 bits), which are arranged in a 4x4 matrix. The number of rounds of transformation depends on the key size, as follows:

128-bit key : 10 rounds
192-bit key : 12 rounds
256-bit key : 14 rounds

Each round, except the last one, consist of 4 steps:

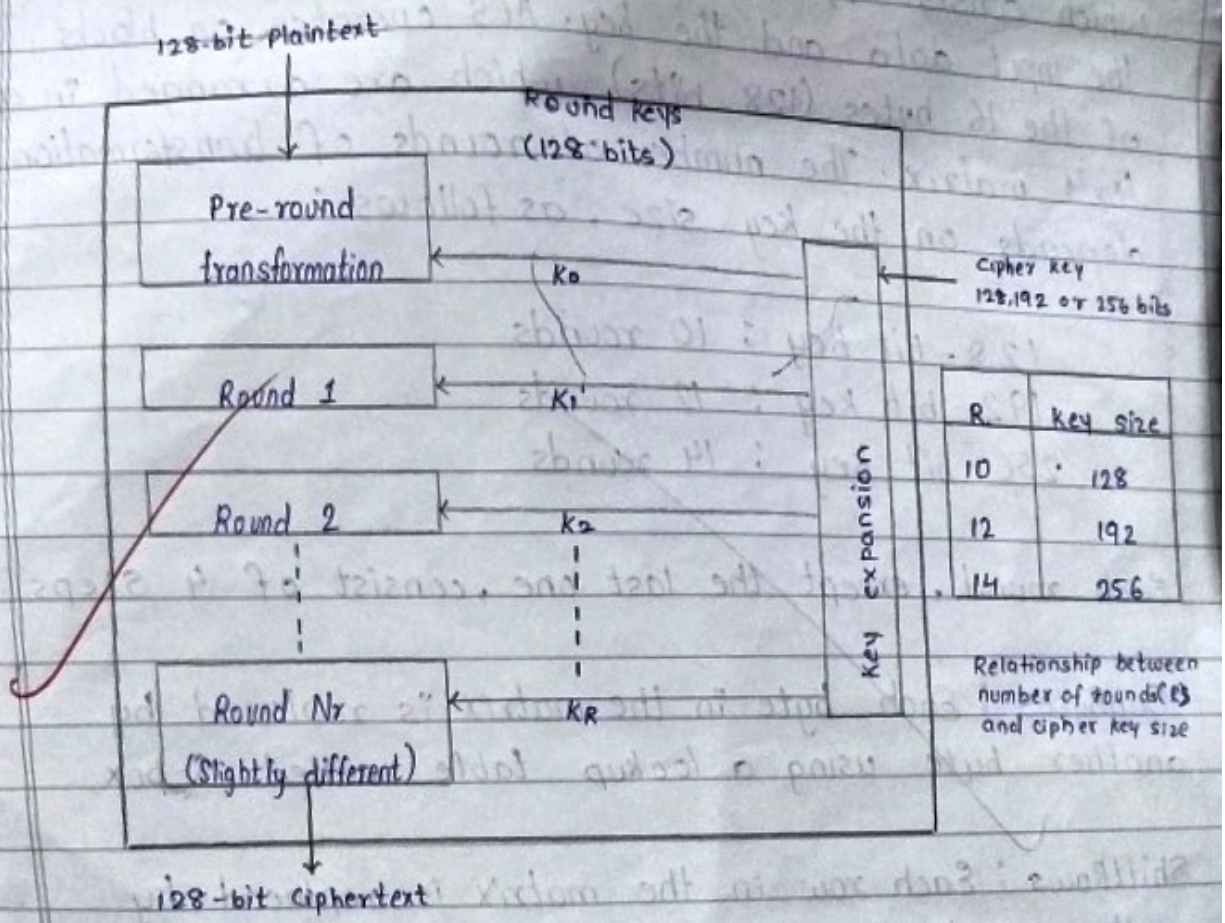
SubBytes : Each byte in the matrix is replaced by another byte using a lookup table called S-box.

ShiftRows : Each row in the matrix is ~~replaced by another~~ cyclically shifted to the left by a certain number of positions.

MixColumns : Each columns in the matrix is multiplied by a fixed polynomial and the result is reduced modulo another polynomial.

AddRoundkey : The matrix is XORed with a round key derived from the original key using a key schedule algorithm.

The last round omits the MixColumns step. Before the first round and after the last round, an initial and a final permutation are applied to the matrix, respectively.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

The above diagram shows the schematic structure of AES.

23 Explain MD5 and Draw digital certificate X.509

MD5 is a cryptographic hash function algorithm that takes the message as input of any length and changes it into a fixed-length message of 16 bytes. MD5 algorithm stands for the message-digest algorithm. MD5 was developed in 1991 by Ronald Rivest. The output of MD5 is always 128 bits.

Use of MD5 Algorithm :

It is used for file authentication.

In a web application, it is used for security purposes. eg: Secure password of users, etc.

Using this algorithm, we can store our password in 128 bits format.

How does MD5 work?

The MD5 message-digest hashing algorithm processes data in 512 bit string, broken down into 16 words composed of 32 bits each. The output from MD5 is a 128-bit message-digest value.

Computation of the MD5 digest value is performed in separate stages that process each 512-bit block of data along with the value computed in the preceding stage. The first stage begins with the message-digest values initialized using consecutive hexadecimal numerical values. Each stage includes four message-digest passes, which manipulate values in the current data block and values processed from the previous block. The final value computed from the last block becomes the MD5 digest for that block.

Is MD5 secure

The goal of any message-digest is to produce digest that appear to be random. To be considered cryptographically secure, the hash function should meet two requirements :

1.] It is impossible for an attacker to generate a message matching a specific hash value.

2] It is impossible for an attacker to create two messages that produce the same hash value.

Process

$F(B,C,D) = (B \wedge C) \vee (\neg B \wedge D)$

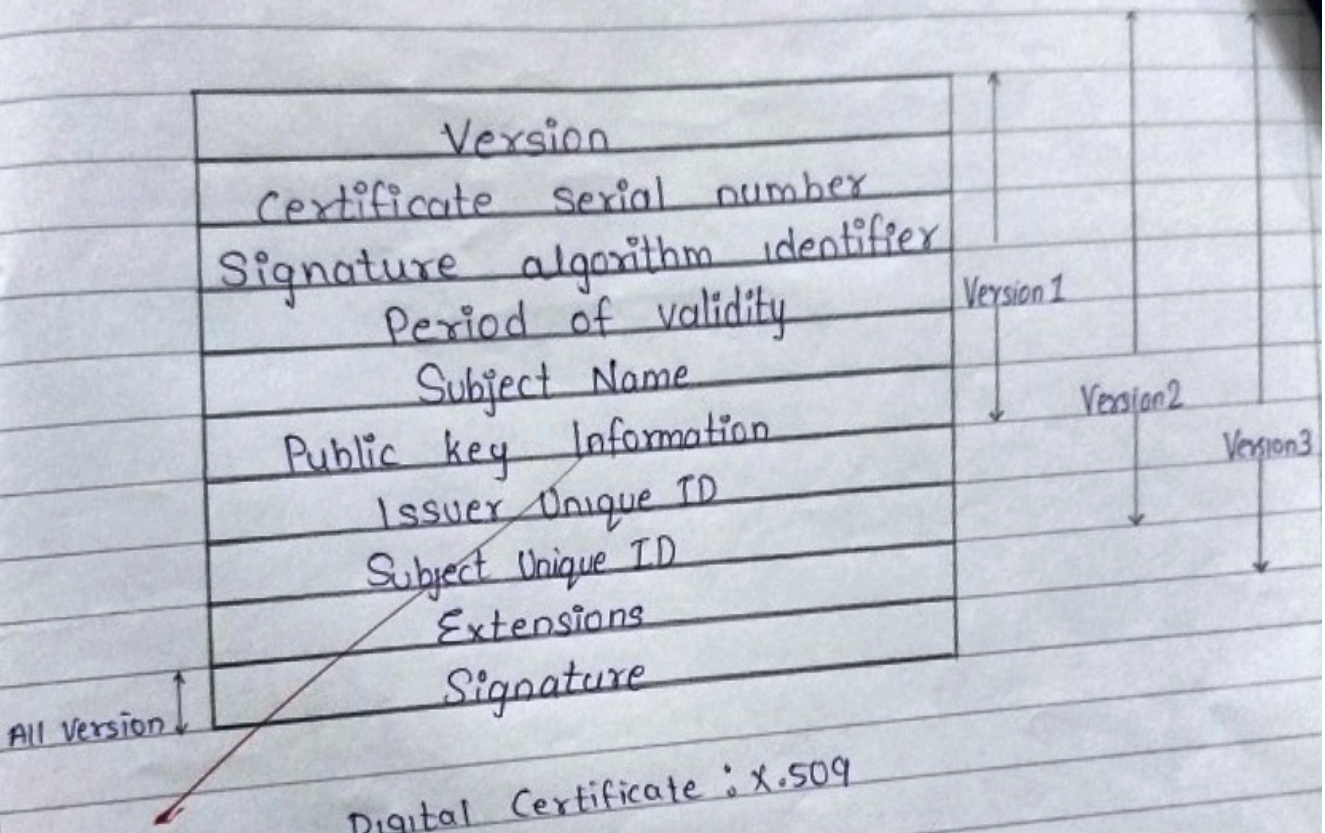
$G(B,C,D) = (B \wedge D) \vee (C \wedge \neg D)$

$H(B,C,D) = B \oplus C \oplus D$

$I(B,C,D) = C \oplus (B \vee \neg D)$

$\vee$ - OR
$\wedge$ - AND
$\oplus$ - XOR
$\neg$ - NOT

Digital Certificate : X.509



Digital Certificate : X.509

Anjuman - I -Islam's

M.H SABOO SIDDIK COLLEGE OF ENGINEERING

8, Saboo Siddik Polytechnic Rd., Byculla, Mumbai – 400 008.

Department of Computer Science & Engineering (AI & ML)

(2023-2024)

For Assignment [5 Marks]

Class: CSE(AIML)-TE

Subject Name: CSS

Subject Code:

Assignment No:	2
Title:	4,5,6
Date of Performance:	3/4/24
Date of Submission:	
Roll No:	211714
Name of the Student:	Jram Mohd Ahmed Shaikh

Evaluation:

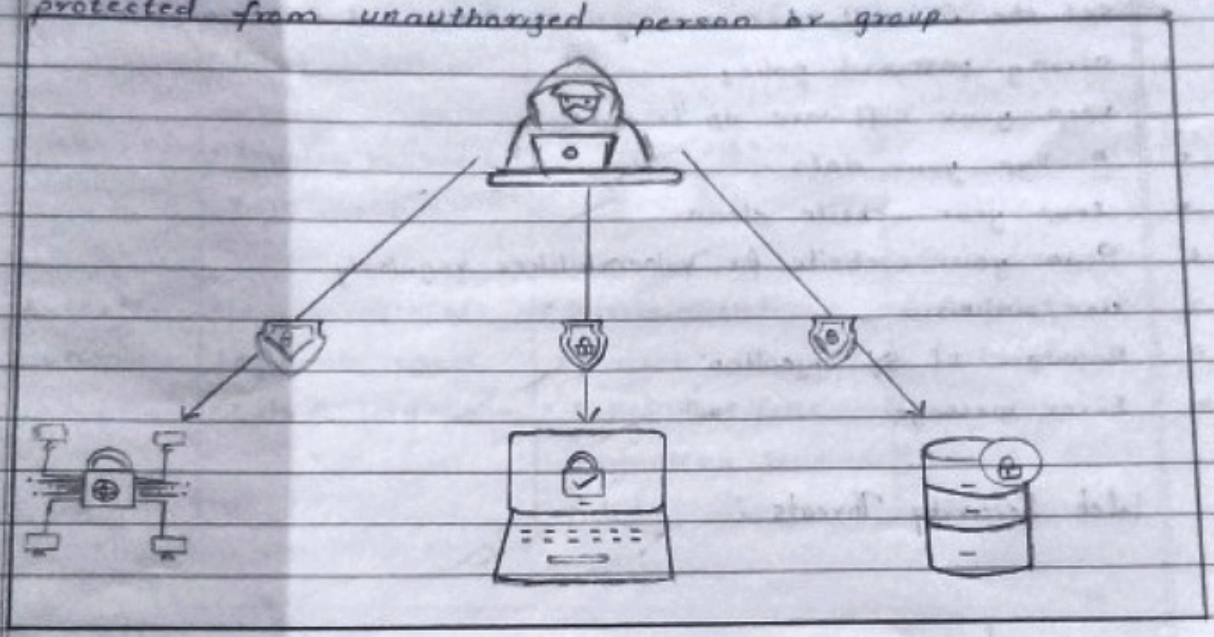
Sr. No	Rubric	Marks
1	On time Submission & Completion (2)	
2	Technical Content (2)	
3	Presentation & Organization (1)	
4	Total (5)	

Signature of the Teacher:

Date:

Q1 Explain web security considerations.

Web Security refers to network, computer system and data are protected from unauthorized person or group.



purpose of web security is to prevent attacks such as active and passive attack.

Active attack:
active attack in which the hacker attempt to change or transform the content of message or information. These attack are a threat to the integrity and availability of the system.

Passive attack:
Passive attack are the ones in which the attacker observes all the message and copy the content of message or information. They focus on monitoring all the transmission & gaining the data.

There are various tools and technologies available to achieve web security. Such as :

1. Set the firewall between your website and data connection.
2. Strong password policy
3. Keep your software up to date
4. Backup your data
5. Keep your website clean
6. Scan your website for vulnerabilities regularly
7. Use antivirus
8. Beaware of Sql injection
9. Error message.

Web Security Threats :

	Threats	Effects	prevention measures
Integrity	• Modification of user data • Modification of memory • Modification of message traffic in transit	• Loss of information • Compromise of machine • Vulnerability of all other threats.	• Cryptographic checksums.
Confidentiality	• Eavesdropping on the net • Theft of information from server • Theft of data from client • Info about network configuration.	• Loss of information • Loss of privacy	• Encryption • Web proxies.

Denial of Service	• killing of user threads • Flooding machine with bogus request • Filling up disk or memory • Isolating machine by DNS attack	• Disruptive • Annoying • Prevent user from getting work done	• Difficult to prevent
Authetication	• Impersonation of legitimate users • Data forgery	• Misrepresentation of user • Belief that false information is valid	• Cryptographic techniques.

Q2 Explain Cookies.

a Cookies is a small piece of text sent to your browser by website you visit.

b Cookies are created by website and Stored in user's browser.

c Cookies stored limited amout of data in the form of files.

d It is use to monitor you and remember certain information about you which can make easier to visit the site again and make the site useful to you.

e Cookies data is available - based on types.

Types of Cookies :

Session cookies : (temporary cookies)

Permanent cookies

First party cookies

Third party cookies

Zombie Cookies.

Session cookies are used only when a person is actively navigating a website ; once you leave the site, the session cookie disappears

Permanent cookies are stored on your computer or device even after you close the site/browser.

Zombie cookies are difficult to handle since they recreate themselves after being erased. Because they make it easier for parties you cannot identify to track your online activities.

Third party cookies are also raise Security and privacy issues.

Cookies are mainly used for three purposes :

Session management - Logins, Shopping carts, game scores, or anything else the server should remember.

Personalization - User preferences, themes, & other Settings.

Track & Analyze - Tracking Recording & analyzing user behaviours.

Q3 # Explain Https.

a The basic protocol used to transmit data between a web browser and a website is HTTP; while HTTPs is the secure version of HTTP.

b HTTPs is a combination of HTTP and TLS/SSL.

c HTTPs encrypts messages using an encryption protocol. previously known as Secure Socket Layer (SSL), the technology is now known as Transport Layer Security (TLS).

d This kind of mechanism encrypts communication between two parties using two unique keys The public key and private key.

e The private key is a controllable key that, as the reader would have guessed, is kept private by the owner of a website Information encrypted by the public key is decrypted using this key, which is stored on a web server.

f The public key, which is accessible to anyone who want to communicat securely with the server. Only the private key is capable of decrypting data that has been encrypted using the public key.

g What makes HTTPs crucial? Https stops website from broadcasting their information in a way that anyone spying on the network may easily view.

h As a result, data transmission over an insecure channel, like public Wi-fi, is extremely susceptible to eavesdropping. All Communication through Http is done so in plain text, making it extremely easy for anyone with the right tools to view it & making susceptible to on-path assaults.

j So why use HTTPs for website:

1 The first reason is that users are most likely to trust websites the employ HTTPS.

2 The Second justification is that HTTPS is safer for user and website owner alike.

3 Third reason: Websites are authenticated by HTTPS.

~~HTTPs provides Data Integrity: Data integrity ensures~~

k HTTPS ensures data integrity by preventing unauthorized modification during transmission. This protect against tampering or injection of malicious code into web pages.

k HTTPS is essential for protecting sensitive information such as login credentials, payment details and personal info submitted through web forms.

l HTTPS involves obtaining an SSL/TLS certificate, configuring the web server to use HTTPS and ensuring that all internal in' links and resources also use HTTPS to avoid mixed content warning.

Q4 What is click jacking ? Explain in short.

a Click jacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause user to unwittingly download malware, visit malicious web pages, provide credential or sensitive information.

b There are several variations of clickjacking attack such as,

1 Lifejacking - a technique in which the facebook "Like" button is manipulated, causing users to "like" a page they actually did not intend to like.

2 Cursorjacking - a UI redressing technique that changes the cursor for the position the user perceives to another position.

c A web user accesses a decoy website and click on a button to win a prize.
Unknowingly, they have been deceived by attacker into pressing an alternative hidden button and this result in the payment of an account on another site.

d Example : • Button on it that says "click here for a free ipod"
• Facebook's "Like" button
• Down load latest version of adobe media player.

e prevention : • One way to defend clickjacking is to include a "frame-breaker" script in each page that should not be framed.

f Clickjacking Mitigation

1 There are two general ways to defend against clickjacking:

1 Client-side methods - the most common is called Frame Busting. client-side method can be effective in some cases, but are considered not to be best practice, because they can be easily bypassed.

2 Server-side methods - the most common is X-Frame-Options. Server-side method are recommended by security expert as an effective way to defend against clickjacking.

Q5 Web security threads

a Web security threats refers to vulnerabilities, risks and potential danger that can compromise the security of websites and web applications. These threats can come into various forms and can target different layer of a web applications or website.

b Web security threats are constantly emerging and evolving, but many threats consistently appear at the top of the list of web security threats. These includes:

1 Cross-site scripting (XSS) - Attackers inject malicious script into webpages viewed by other users, allowing them to steal session cookies, redirect users to malicious sites, or deface websites.

2 SQL injection (SQLi) - Attackers exploit vulnerabilities in web application to inject malicious SQL code into database queries, potentially gaining unauthorized access to sensitive data.

3 Phishing - Attackers attempt to deceive user into disclosing sensitive information, such as login credentials or financial details by impersonating legitimate websites or organization via email, messaging or fake website.

4 Denial of Service - Attackers overwhelm a web server with a massive volume of traffic or request, causing it to become unavailable to legitimate users.

Brute Force Attacks - Attackers attempts to guess usernames and passwords by systematically trying different combinations until then gain unauthorized access to an account or system.

Clickjacking - It involves tricking users into clicking on something different from what they perceive, such as disguised button or link.

and many more....