



## Department of Computer Science

# Flipped Classroom Strategy on “Cryptographic Technique

Class: B.Tech. (CS)/Sem-VI

Subject: Cyber Security

Topic: Cryptographic Technique

### Objective:

To help students understand the various cryptographic methods, including symmetric and asymmetric encryption, hashing, and digital signatures. Students will be able to apply basic cryptographic techniques to solve real-world security problems.

### Flipped Classroom Approach:

#### 1. Pre-Class Preparation:

##### o Video/Reading Material:

- Provide students with introductory videos or articles about basic cryptographic concepts (e.g., RSA, AES).
- Video Link: <https://archive.nptel.ac.in/courses/106/105/106105162/>
- Video Link: <https://www.youtube.com/watch?v=cOpYHlqis3o>

#### 2. In-Class Activities:

##### o Hands-on Cryptography Exercise:

- Break students into groups and assign them different encryption algorithms.
- Have them implement the encryption and decryption steps with sample data, either manually or using a programming language (eg. Java, Python).

##### o Collaborative Problem Solving:


- Present a scenario where students need to decide which cryptographic method to use.
- Students will be divided into groups and each group will be asked to analyse and select an appropriate cryptographic technique for the given problem.

##### o Group Discussion on Modern Cryptographic Challenges:

- Facilitate a class discussion on the current challenges in cryptography, such as the rise of quantum computing or encryption backdoors.
- Students can use the knowledge gained from pre-class activities to contribute to the discussion.

#### 3. Post-Class Assignment:

- **Case Study Analysis:** Provide a case study about a recent security breach or cryptographic failure.

  
Subject Teacher

## Department of Computer Science

- Ask students to analyze the breach in terms of cryptographic failure and propose solutions or alternative cryptographic techniques that could have prevented the issue.

### List of Real-World Problems and Challenges in Cryptographic Techniques:

#### Cryptographic Backdoors:

There are concerns about governments or organizations forcing companies to include backdoors in their encryption systems, compromising user privacy and data security.

#### Side-Channel Attacks:

These attacks exploit information leaks from physical systems (like CPU power consumption or electromagnetic emissions) to break encryption without needing to directly break the cryptographic algorithm.

#### Secure Communication in Mobile Networks:

Mobile devices face unique challenges in securing communications over insecure networks (e.g., public Wi-Fi), where attackers can intercept or modify encrypted data.

#### Digital Signature Forgery:

The challenge of ensuring digital signatures cannot be forged or tampered with remains critical, especially in applications like secure contracts and e-commerce.

#### Password Security and Storage:

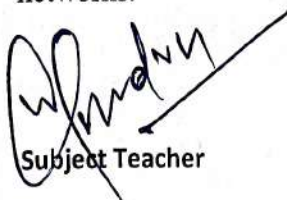
Ensuring passwords are securely hashed and stored is crucial to protecting user credentials. Weak or outdated hashing algorithms, like MD5 or SHA-1, are vulnerable to collision attacks.

#### Privacy-Preserving Cryptography:

Balancing cryptographic techniques with user privacy, especially when it comes to collecting and analyzing user data for marketing, social networks, or governmental purposes.

#### Blockchain Security:

While blockchain uses cryptographic techniques to secure transactions, challenges remain in ensuring the security and scalability of blockchain-based systems, especially in public networks.



Subject Teacher



## Department of Computer Science

### Attendance Sheet Academic Session: 2022-23 B. Tech. CS Sem. VI Subject: Cyber Security

Sr. No.	Name of Student	Roll No.	Signature
1	PATEL, JAYKUMAR	B203	Jay
2	TALAVIYA, KHUSHI	B204	Khushi
3	DALAL, PARAM	B205	Param
4	SAXENA, SHAURYA	B206	Shaurya
5	SHARMA, HRIDAYANK	B207	Hridayank
6	MODI, JAINIL	B208	Jainil
7	SAHNI, JASLEEN	B209	Jasleen
8	BAWASKER, ARYAN	B210	Aryan
9	KAMBLE, RUSHI	B211	Rushi
10	PAREKH, ADITYA	B213	Aditya
11	TOLIA, VEDANT	B214	Vedant
12	THOMAS, JOEL	B215	Joel
13	MAHESHWARI, AMAN	B216	Aman
14	BAKSHI, JASJOT	B217	Jasjot
15	PALIWAL, SHOBBIT	B218	Shobhit
16	NANDI, ANKON	B219	Ankon
17	SARAIYA, CHARVEE	B220	Charvee
18	DHUMALE, SAHIL	B222	Sahil
19	SHAH, HIRAK	B223	Hirak
20	RAUT, TANMAY	B224	Tanmay
21	KAUSHAL, PRIYANSHU	B226	Priyanshu
22	NAYAK, SATVIK	B227	Satvik
23	BANCHHOD, TANUSH	B228	Tanush
24	TRIPATHI, SWASTI	B229	Swasti
25	PATEL, BHAVYA	B230	Bhavya
26	THAKUR, SUMIT	B232	Sumit
27	RAWKA, TANISHK	B233	Tanishk
28	KUMAR, PRAVEEN	B234	Praveen
29	MANANI, HIREN	B235	Hiren

  
Subject Teacher

## Department of Computer Science

30	DARAK, SIDDHESH	B236	<i>Darak</i>
31	INAMDAR, ARYAN	B237	<i>Aryan</i>
32	TUTEJA, DEEPANSH	B238	<i>Deepansh</i>
33	JAIN, DEVANSH	B239	<i>Devansh</i>
34	PATIL, JAY	B240	<i>Jay Patil</i>
35	BHATIA, SADGI	B241	<i>Sadgi Bhatia</i>
36	KHANDELWAL, SPARSH	B242	<i>Sparskhanelwal</i>
37	JAIN, HARDIK	B243	<i>Hardik Jain</i>
38	AGRAWAL, TAPAN	B244	<i>Tapan</i>
39	SHUKLA, LAXITA	B245	<i>Laxita</i>
40	JAIN, NAITIK	B246	<del><i>Naitik</i></del>
41	DESAI, RAJAT	B247	<i>Rajat D.</i>
42	KHANDELWAL, ARIN	B248	<i>Arin</i>
43	DEVARU, ADITHYA	B249	<i>Aditya</i>
44	ARORA, ADVAIT	B250	<i>Advait</i>
45	DUBEY, SANIDDHYA	B251	<i>Sandhya</i>
46	GOLANI, SHIVAM	B252	<i>Shivam</i>
47	WADHWANI, MITANSH	B253	<i>Mitansh</i>
48	SINDHI, UMESH	B254	<i>Umesh</i>
49	SINGH, RAHUL	B256	<i>Rahul Singh</i>
50	KANJARIYA, TEJ	B257	<i>Tej</i>
51	SAXENA, AYUSH	B258	<i>Ayush</i>
52	PATIDAR, ADITYA	B259	<i>Aditya Patidar</i>
53	KUMARI, SAROJ	B260	<i>Saroj</i>
54	SINGH, SAURAV KUMAR	B261	<i>Saurav Singh</i>
55	JOSHI, ATHARVA	B265	<i>Atharva Joshi</i>
56	TAKKAR, MANAN	B266	<i>Manan Takkur</i>
57	MANTRI, ADITYA	B267	<i>Aditya Mantri</i>
58	CHOPRA, MUSKAN	B269	<i>Muskan Chopra</i>
59	SINGH, SAHIL	B270	<i>Sahil Singh</i>

*[Signature]*  
Subject Teacher