CORPORATE OFFICE
Delhi Office
706 Ground Floor Dr. Mukherjee Nagar Near Batra Cinema Delhi – 110009
Noida Office
Basement C-32 Noida Sector-2 Uttar Pradesh 201301

CURRENT AFFAIRS

Yojna IAS
yojnaias.com
योजना है तो सफलता है

website : www.yojnaias.com
Contact No. : +91 8595390705

Date: 29 January 2024

AISHE REPORT

THIS ARTICLE COVERS 'DAILY CURRENT AFFAIRS' AND THE TOPIC DETAILS OF "ALL INDIA SURVEY ON HIGHER EDUCATION (AISHE) REPORT". THIS TOPIC IS RELEVANT IN THE "GOVERNANCE" SECTION OF THE UPSC CSE EXAM.

WHY IN THE NEWS?

More women than males have enrolled in higher education over the previous eight years, according to the newly released 2021-22 All India Survey on Higher Education (AISHE).

ABOUT ALL INDIA SURVEY ON HIGHER EDUCATION (AISHE) REPORT:

- The **All India Survey on Higher Education (AISHE) Report** is a thorough and systematic project launched by the Ministry of Education, Government of India, to collect and analyse data on the country's higher education system. The **major goal of AISHE** is to give reliable and up-to-date information regarding many sectors of higher education, including enrollment trends, infrastructure, faculty, and other pertinent factors.
- The AISHE Report, which is published annually, **plays an important role in developing policies and strategies for the growth of higher education in India**. It examines both traditional and unconventional institutions, providing insights on the variegated landscape of educational institutions across the country.
- The report normally **includes information about student enrollment, faculty composition, infrastructure facilities, gender distribution, and exam outcomes.** It enables policymakers, researchers, and educational institutions to discover trends, evaluate policy impacts, and make educated decisions to improve the quality and accessibility of higher education.
- One prominent component of the AISHE Report is its **emphasis on inclusivity**, which includes data on student enrollment from many social groups and backgrounds. This helps to assess the success of affirmative action measures and ensures equal access to education.
- The AISHE Report is an important resource for a variety of stakeholders, including government authorities, academic institutions, and researchers, since it promotes evidence-based decision-making and the continuing improvement of India's higher education system. As an updated document, the AISHE Report reflects the dynamic character of higher education, providing a comprehensive overview of the sector's progress and difficulties.

THE MAJOR FINDINGS OF AISHE REPORT 2021-22 ARE:

- The AISHE report 2021-22 was done over the academic session 2021-22. AISHE 2021-22 registered 1,168 universities/university level institutions, 45,473 colleges, and 12,002 stand-alone institutions.
- The poll included responses from 1,162 universities, 42,825 colleges, and 10,576 stand-alone institutions.

NUMBER OF INSTITUTIONS AS PER AISHE REPORT:

- **Since 2014-15, 341 universities or university-level institutes have been formed.** Out of 1168 registered universities, 685 are government-managed (240 by the central government and 445 by the state government), 10 are private deemed (aided), and 473 are private (unaided).
- There are **17 universities** specifically for women. It was 11 in 2014-15. In 2021-22, there were **18 Open Universities** (1 Central University, 16 State Universities, and 1 State Private University).
- **Enrollment in higher education:** Higher education enrollment is projected to reach over 4.33 crore in 2021-22, up from 3.42 crore in 2014-15.
- **Female enrollment** in higher education has risen to 2.07 crore (32% increase since 2014-15). The total number of pass-outs has climbed to 1.07 crore in 2021-22 from 95.4 lakh in 2020-21.

CASTE-BASED ENROLLMENT:

- **Caste breakdown of all enrolled students in 2021-22:** The student body is made up of 15.3% Scheduled Caste, 6.3% Scheduled Tribe, 37.8% Other Backward Class, and 40.6% from other categories.
- **Scheduled Caste student** enrollment has risen to 66.23 lakh in 2021-22, up from 58.95 lakh the previous year. The enrollment of **Scheduled Tribe** students has increased to 27.1 lakh in 2021-22 from 24.12 lakh in 2020-21.
- The number of **Scheduled Tribe Female** students enrolled grew to 13.46 lakh in 2021-22 from 12.21 lakh in 2020-21. While **Minority enrollment** has risen to 30.1 lakh in 2021-22 from 21.8 lakh in 2014-15.

ENROLLMENT IN STATES:

- The **top six states** in terms of student enrollment are Uttar Pradesh, Maharashtra, Tamil Nadu, Madhya Pradesh, West Bengal, and Rajasthan. They account for **53.3%** of the overall student enrollment.
- In 2021-22, there were approximately 15.98 lakh faculty/teachers in higher education, with 56.6% being male and 43.4% female.
- The number of educators in 2021-22 has increased by 46,618 from 2020-21.

PRELIMS PRACTICE QUESTION

Q1) Consider the following statements:

1) University Grants Commission (UGC) is the primary regulatory body overseeing higher education in India

2) National Skill Development Corporation (NSDC) in India primarily focuses on Vocational education and skill development

3) University Grants Commission (UGC) is responsible for conducting the All India Survey on Higher Education (AISHE) in India

How many of the above statements are correct? · ·

(a) Only one

(b) Only two
(c) All three
(d) None
ANSWER: B

MAINS PRACTICE QUESTION

Q1) In your opinion, how has the implementation of the Right to Education Act impacted the quality of primary education in the country?

Himanshu Mishra

END – TO – END ENCRYPTION AND RIGHT TO PRIVACY

SOURCE – THE HINDU AND PIB.

GENERAL STUDIES – PAPER 3 – PROTECTION OF PRIVACY, FUNDAMENTAL RIGHTS, INFORMATION TECHNOLOGY AND COMPUTERS, DATA SECURITY, DATA PROTECTION LAWS, ADVANTAGES AND DISADVANTAGES OF END-TO-END ENCRYPTION.

WHY IN THE NEWS ?

- On the one hand, in the context of compliance with India's proposed Online Security Bill (OSB) for the entire country, the head of WhatsApp has said that – **"WhatsApp will not comply with India's Online Security Bill (OSB), which effectively Prohibits "end-to-end (E2E) encryption."** Apple has announced that – **"It will further increase the data points protected by end-to-end encryption (E2EE) on iCloud from 14 to 23 categories, as a result of which the protection of consumers' privacy can be ensured. "**

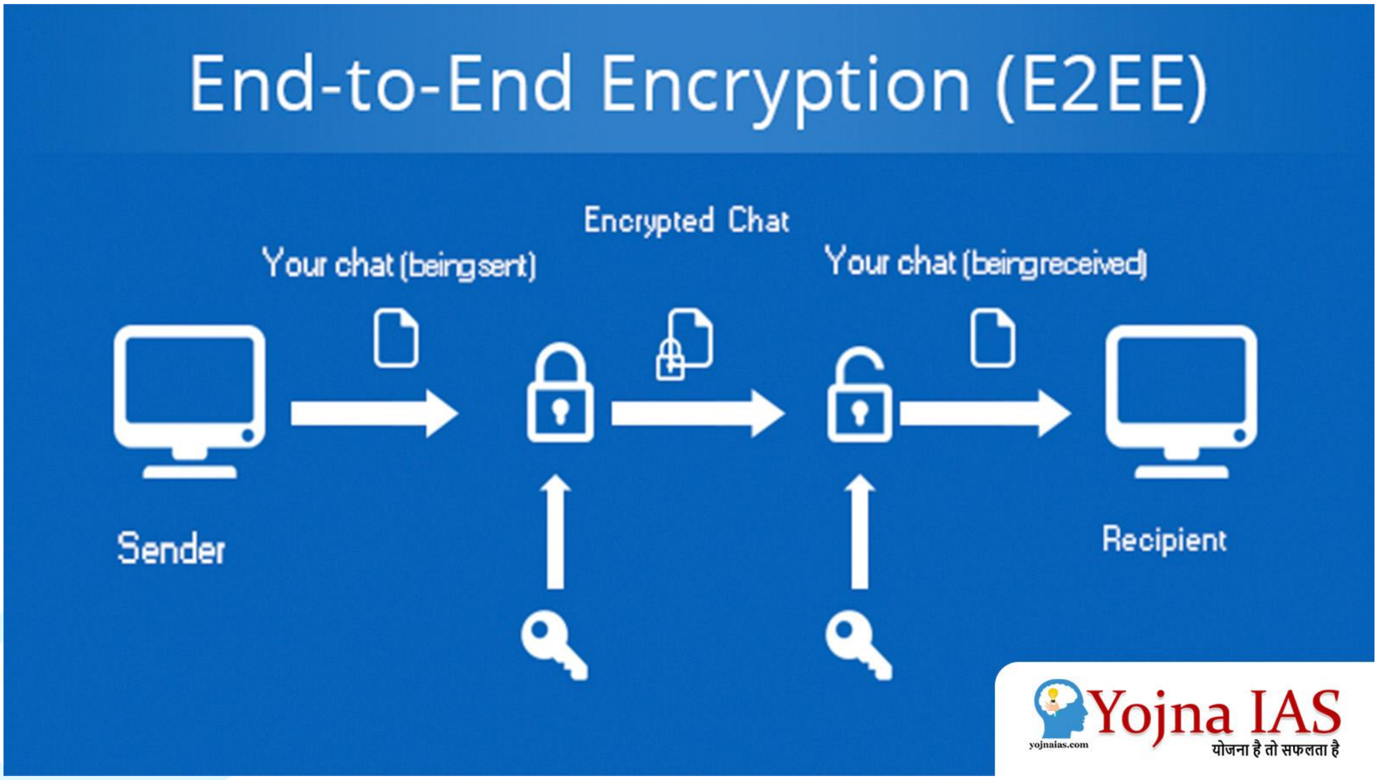
MAIN OBJECTIVES OF SHARING DATA – BREACH – RESEARCH :

- According to a recent survey-research conducted by Apple, which is also called data-breach-research, the total number of data breaches in India from the year 2013 to the year 2021 is three.

Has increased more than times. Only in the year 2021 . In this year alone, data of 1.1 billion personal records has been revealed.

- With this end-to-end encryption, even if someone's personal data is breached in the cloud, the user's data will remain completely safe. This additional layer/level of encryption will somehow prove to be extremely valuable from the right to privacy and security of personal data point of view to deal with the hacking attacks launched by some funded groups and also from data theft and other security point of view.

WHAT IS ENCRYPTION ?



- One way to protect data from unauthorized access or tampering is called encryption. This process involves converting data into a secret code that only the intended recipient can understand. It is useful for various cases. Such as securing mutual online communications, storing sensitive information among themselves and verifying their digital identities, etc.

There are mainly two types of encryption-

1. **SYMMETRICAL AND**
2. **ASYMMETRIC.**

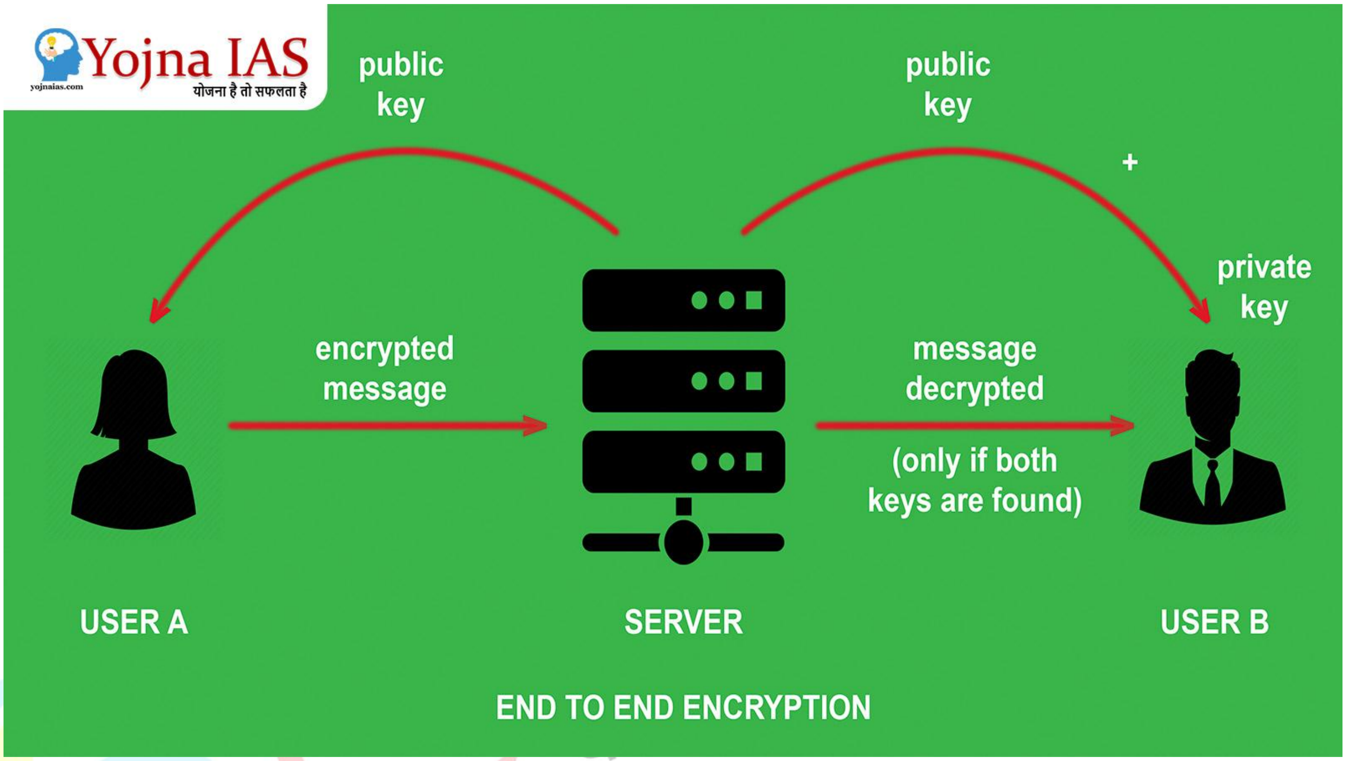
- Symmetric encryption uses a single key to encrypt and decrypt data, while asymmetric encryption uses a pair of keys – one public and one private. One thing to note is that any public key can be shared with anyone, but in asymmetric encryption the private key is always kept secret.

WORKING MECHANISM OF END-TO-END ENCRYPTION :

- Any end-to-end encryption relies on an elegant but complex cryptographic system to protect the data in transit or shared between two devices. The key element is asymmetric cryptography, which uses pairs of keys – public and private – to secure communications. The public key encrypts the data, while the private key decrypts it.

- It is a communication process that encrypts the data being shared between two devices.
- This prevents third parties such as Internet Service Providers (ISPs), cloud service providers and cyber criminals from accessing the data, especially when one's personal data is being transferred.

MECHANISMS USED IN END- TO- END ENCRYPTION :



- Cryptographic keys used to encrypt and decrypt messages are stored on endpoints.
- The process of end-to-end encryption uses an algorithm that converts standard text into an unreadable format.
- This format can only be opened or read by people with decryption keys, which are stored only on the endpoints and are not shared with any third parties, including service providing companies.

USEFULNESS OF END-TO-END ENCRYPTION IN MUTUAL COMMUNICATION :

- End-to-end encryption has long been commonly used in India when transferring business documents, financial statements, legal proceedings and personal conversations.
- It can also be used to control the authorization of users when accessing any stored data.
- End-to-end encryption is used to secure user-to-user communications.
- It is commonly used to secure any passwords, ensure the security of stored data, and also for provisional protection of data security on cloud storage.

BRITISH ONLINE SECURITY BILL :

- The Online Safety Bill (OSB) is a British proposed legislation to impose **'duty of care'** obligations on online platforms to improve online safety. Whose work is motivated by forcing Internet service providers to work to improve online security.
- Section 110 of the Terrorism and Child Sexual Exploitation and Abuse (CSEA) Content Identification and Online Safety Bill (OSB) empowers the regulator to issue notices to most internet service providers, including private messaging apps, to prevent terrorism and Child Sexual Exploitation and Abuse (CSEA) can be investigated and immediately removed from internet platforms.
- The Online Security Bill (OSB) does not mandate the removal of end-to-end encryption but would require any messaging app to scan all messages to flag such content, which would actually mean removing security mechanisms such as encryption. To break.
- The Online Security Bill (OSB) is seen as contradictory to the fundamental rights of an individual such as privacy and freedom of expression which allow states or governments to restrict and monitor the individual's fundamental rights such as privacy and freedom of expression.

ONLINE SECURITY BILL (OSB) IN INDIA :

INFORMATION TECHNOLOGY ACT 2000 :

- This Act brought by the Government of India regulates and guides the electronic and wireless modes of communication in the country. It exempts us from making any concrete provision related to encryption or making any strict policy at the concrete level, which makes this Act a matter of concern from the point of view of the question of privacy of consumers and it is a major step forward in the field of information and technology in India. Also demands making a concrete guideline.

DIGITAL MEDIA CODE OF CONDUCT – RULES 2021 :

- Through what is commonly called traceability, the Government of India has made it mandatory for messaging platforms with more than five million users in India to 'enable the identification of the first originator' of the message. The Government of India has mandated this through the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
- This information about the person who first sent the message, the number of times he has sent a message and the number of times he has forwarded it is also contained in this Code of Conduct rule.
- WhatsApp's penetration rate in India is over 97%, while in the United Kingdom it is around 75%. Because there are 487.5 million WhatsApp users in India where the messaging platform accounts for 22% i.e. 2.24 billion monthly active users.

BENEFITS OF END-TO-END ENCRYPTION (E2EE) :

END-TO-END ENCRYPTION HELPS IN PROVIDING SECURITY IN MUTUAL COMMUNICATION :

- End-to-end encryption helps provide security in communications because end-to-end encryption uses public key cryptography, which stores the private key on endpoint devices. Messages can only be decrypted using these keys, so only people with access to the endpoint device are able to read the message.

HELPFUL IN KEEPING SAFE FROM THIRD PARTIES :

- End-to-end encryption (E2EE) also serves to ensure that consumers or users are protected from malicious parties, including Internet data service providers, cloud storage providers, and companies that handle encrypted data.

IT IS FREE FROM ANY KIND OF INTERFERENCE :

- The decryption key does not need to be provided with E2EE as it is already available to the recipient.
- If a message encrypted with the public key is tampered with during transmission, the recipient will not be able to decrypt it and will not be able to access the tampered content.

UNREADABLE AND FORCED TO COMPLY WITH GOVERNMENT REGULATIONS :

- Many industries are bound by regulatory laws/requirements or compliance laws that require encryption-level data protection as a primary requirement. So end-to-end encryption (E2EE) can help organizations keep data secure by making it unreadable.

DISADVANTAGES OF END- TO- END ENCRYPTION (E2EE) :

IT IS EXTREMELY COMPLEX TO DEFINE ENDPOINTS :

- Some end-to-end encryption (E2EE) implementations in India allow encrypted data to be encrypted and re-encrypted at certain points during transmission.
- In this it clearly defines and differentiates the endpoints of the communication circuit. If the endpoints are compromised in any way, the encrypted data may be exposed. Therefore, it is extremely complex to define the endpoints of a communication circuit.

EXCESSIVE PROVISION OF CONFIDENTIALITY :

- Governments and government law enforcement agencies have always expressed concern that end-to-end encryption (E2EE) can protect people sharing illegal content because service providers are unable to provide access to the content to law enforcement.

LACK OF PROTECTION FOR METADATA AND FACILITATING DATA MISUSE :

- In any type of mutual communication, messages are encrypted, information related to the message such as date of message and sender's information etc. is visible even after sending the message, making it vulnerable to those who misuse the data in any way. It may prove helpful.

THE LEGAL FRAMEWORK CURRENTLY IN PLACE IN INDIA FOR END-TO-END ENCRYPTION (E2EE) :

CURRENTLY, INDIA LACKS ANY SPECIFIC LEGISLATION RELATED TO END- TO- END ENCRYPTION (E2EE) :

- At present, there is no specific law regarding end-to-end encryption (E2EE) in India. Although many industry standards governing the banking, finance, and telecommunications industries include minimum encryption standards that are used to protect mutual transactions, these are limited to certain specific sectors and are not easily accessible to common consumers. Unable to access.

RESTRICTIONS ON END- TO- END ENCRYPTION (E2EE) TECHNOLOGIES :

- Currently, as per the terms of the licensing agreement between ISPs and DoT in India, consumers or users are not allowed to use encryption standards larger than 40 bits using symmetric key algorithms or comparable methods without prior approval. , while in India itself there are several additional rules and recommendations that allow the use of encryption levels higher than 40 bits for specific regions of India.

CONCLUSION: / SOLUTION PATH :

- Through the Information Technology in India (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, the Government of India seeks to encourage self-regulation of these social messaging platforms while protecting the right of individuals to privacy and freedom of expression. It keeps and guides these messaging platforms keeping in mind the privacy of the consumers, but still there are some criticisms which draw our attention towards government regulation in this regard as it is related to the issue of individual privacy. Lives. Only by finding a solution to this, the concept of India as a democratic and public welfare state can be confirmed.

IT RULES DO NOT FOLLOW HUMAN RIGHTS CONVENTIONS :

- India’s new information technology (IT) rules violate the International Covenant on Civil and Political Rights (ICCPR) under the Human Rights Convention. Article 19(3) of the ICCPR provides for freedom of speech and expression. Which is for national security and public opinion or public health and morality. It is being said that all these things are being stopped due to the new IT rules.

THE GOVERNMENT WILL MANAGE THE DATA OF COMMON USERS :

- Despite there being a freedom of expression law in India, Special Messengers Company says that the government is monitoring the company and rapidly removing user generated content. This violates the right to freedom of expression in India. Common citizens of India have expressed concern that a system is being prepared to remove content from digital platforms. Due to which those working between consumers and the company can take advantage of it.

THE MAIN REASON FOR THE DISPUTE BETWEEN THE GOVERNMENT OF INDIA AND WHATSAPP :

- There is an ongoing dispute between the Government of India and WhatsApp regarding the end-to-end encryption (E2EE) technology of WhatsApp. Last month, WhatsApp had opposed the IT rule. It was alleged that consumers’ right to privacy is in danger. The UN has been supporting end-to-end encryption (E2EE) since its inception. They believe that this is an effective technical safeguard. This protects the right to privacy.

GOVERNMENT COLLECTS DATA TO PROTECT THE UNITY AND INTEGRITY OF INDIA AND TO PREVENT COMMUNAL RIOTS/VIOLENCE :

- When any violence or messages harming the unity and integrity of India go viral. It is used when a woman is being portrayed in a compromising position or in an inappropriate manner or when sexual issues related to children have to be explored. So who has spread the message and for what purpose can be found out.
- There is tension between WhatsApp and the Government of India regarding the rule of traceability. End-to-end encryption is designed to protect the privacy of users. The government’s argument is that if they get to read the messages of all the users, they will easily detect the person spreading

rumors on social media and prevent any kind of communal riots or violence while implementing measures to safeguard the unity and integrity of India. Can be stopped.

PRACTICE QUESTIONS FOR PRELIMINARY EXAM :

Q.1. Consider the following statements regarding the Online Security Bill (OSB) in India.

1. The Online Safety Bill (OSB) is a British proposed legislation to impose 'duty of care' obligations on online platforms to improve online safety.
2. Section 110 of the Terrorism and Child Sexual Exploitation and Abuse (CSEA) Content Identification and Online Security Bill (OSB) empowers the regulator to issue notices to most internet service providers.
3. Through traceability, the Government of India has made it mandatory for messaging platforms with more than five million users in India to 'enable the identification of the first originator' of a message.
4. There are four types of end-to-end encryption.

Which of the above statement /statements is correct?

(A) Only 1, 2 and 4
(B) Only 2, 3 and 4
(C) Only 2 and 4
(D) Only 1, 2 and 3

Answer – (D).

PRACTICE QUESTIONS FOR MAIN EXAM :

Q.1 How do the current online security bill in India and the individual's right to privacy and expression contradict each other ? Give a logical explanation.

Akhilesh kumar shrivastav