CYBERSECURITY ASSIGNMENT -2

R. AISHWARYA REDDY

REG.NO.282023-039

PREPARE A CASE STUDY ON THE SHORTAGE OF CYBERSECURITY PROFESSIONALS IN INDIA, ITS IMPACT ON ORGANIZATIONS, AND THE MEASURES NEEDED TO ADDRESS THIS CHALLENGE(DISCUSS THE SPECIFIC IMPLICATIONS FOR THE INDIAN CONTEXT)

First question

CASE STUDY ON THE SHORTAGE OF CYBERSECURITY PROFESSIONALS IN INDIA

- Its rapidly expanding digital landscape and rising internet usage present a serious obstacle: a lack of skilled cybersecurity experts. This case study looks at the severity of the scarcity, its underlying causes, and the major effects it has on businesses in different industries.
- The magnitude of the Deficit:
- Numbers: It is estimated that India lacks more than a million cybersecurity specialists, and that demand will quadruple by 2025.
- Talent Market: It is challenging for businesses, particularly smaller ones, to recruit and retain qualified employees due to the tiny pool of available talent, severe competition, and expensive compensation.
- Skill Gap: Upskilling and reskilling activities are necessary since there is frequently a mismatch between industry demands and skill sets, even among experts who are readily available.

ROOT CAUSES: THE EXTENT OF THE SHORTAGE

Education System: There is a gap between academics and the workforce as a result of the current education system's lack of emphasis on industry-aligned curriculum and practical cybersecurity skills.

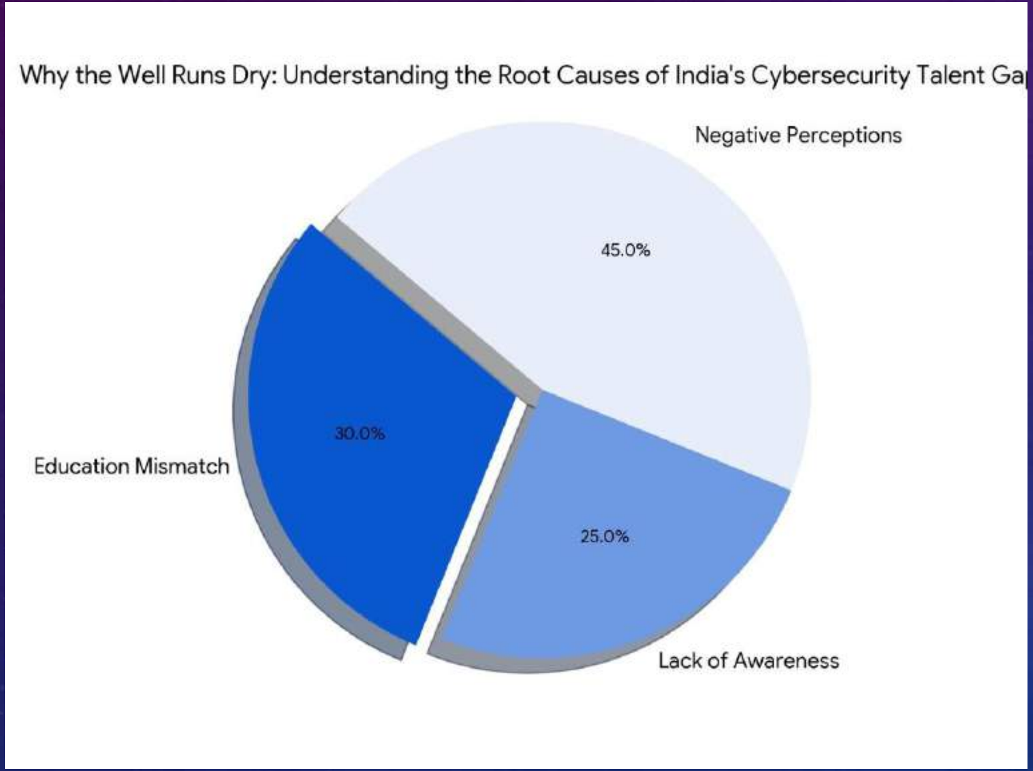
Knowledge: The development of the talent pipeline is hampered by the lack of knowledge, particularly among younger generations, concerning employment in cybersecurity.

Perception: Prospective applicants are deterred by stereotypes and misconceptions about the area, which frequently present it as intricate and intimidating.

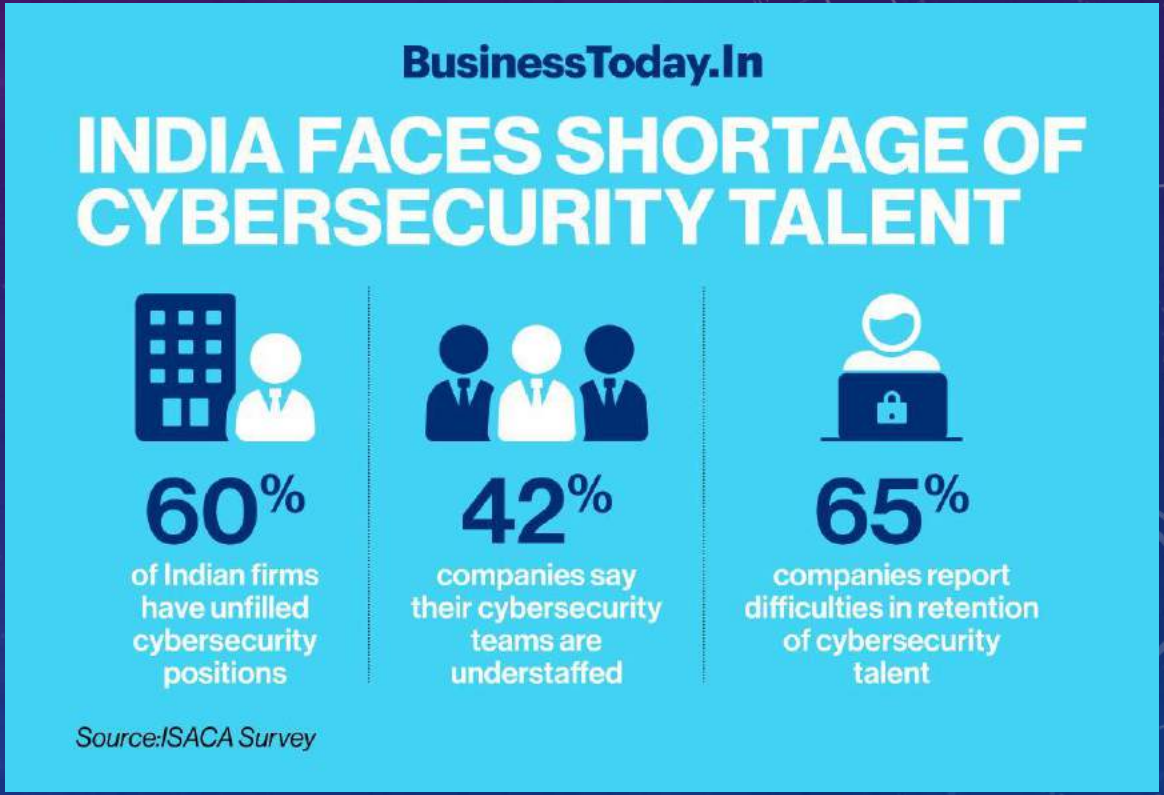
Awareness: Limited awareness about cybersecurity careers, especially among younger generations, hinders talent pipeline development.

Perception: Stereotypes and misconceptions about the field, often portraying it as complex and intimidating, discourage potential candidates.

ROOT CAUSE OF INDIA'S CYBERSECURITY TALENT GAP



Why the Well Runs Dry: Understanding the Root Causes of India's Cybersecurity Talent Ga



BusinessToday.In

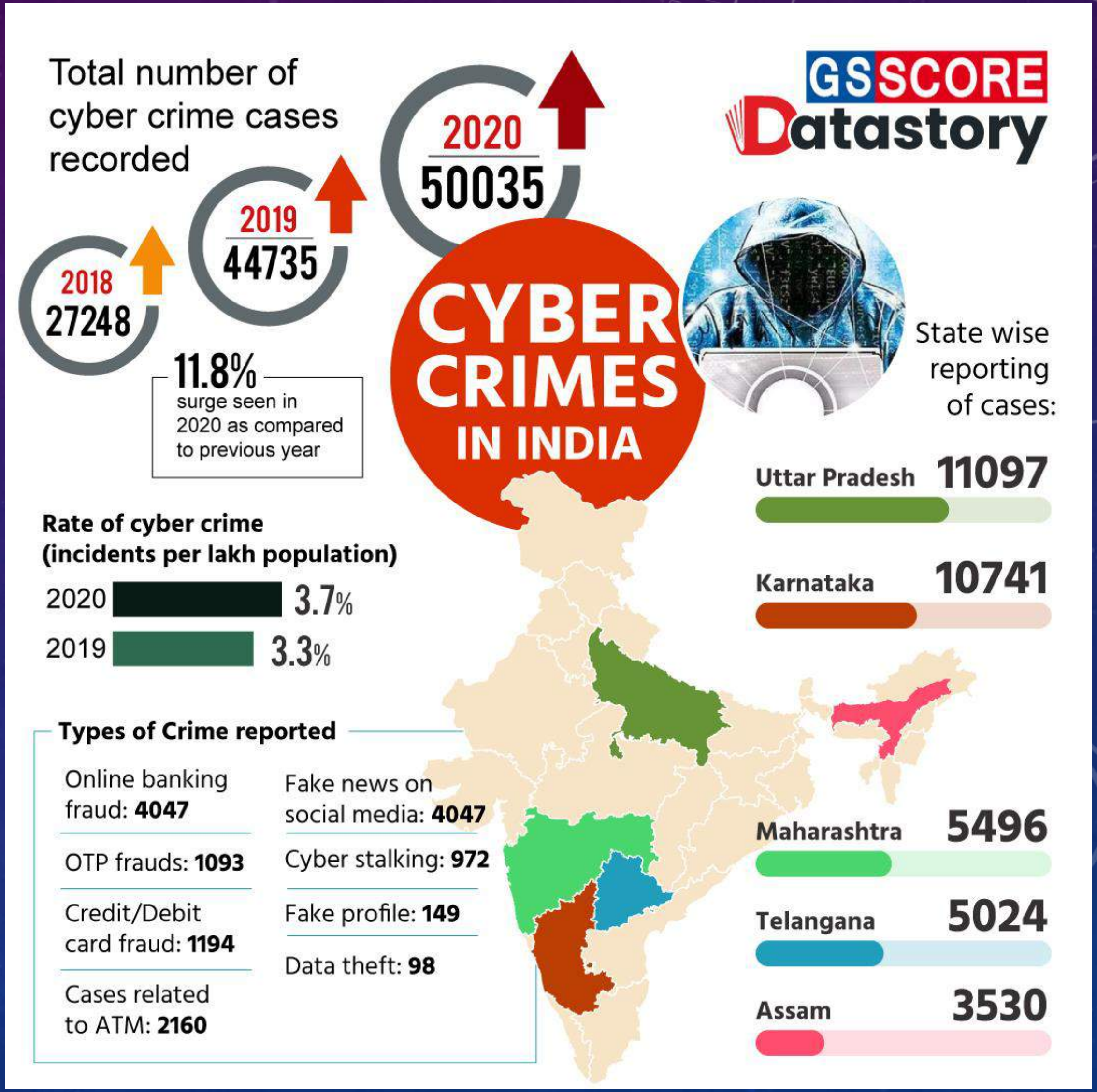
INDIA FACES SHORTAGE OF CYBERSECURITY TALENT

60% of Indian firms have unfilled cybersecurity positions

42% companies say their cybersecurity teams are understaffed

65% companies report difficulties in retention of cybersecurity talent

Source:ISACA Survey



GS SCORE Datastory

CYBER CRIMES IN INDIA

Total number of cyber crime cases recorded

Year	Cases
2018	27248
2019	44735
2020	50035

11.8% surge seen in 2020 as compared to previous year

Rate of cyber crime (incidents per lakh population)

Year	Rate
2020	3.7%
2019	3.3%

Types of Crime reported

Type	Cases
Online banking fraud	4047
OTP frauds	1093
Credit/Debit card fraud	1194
Cases related to ATM	2160
Fake news on social media	4047
Cyber stalking	972
Fake profile	149
Data theft	98

State wise reporting of cases:

State	Cases
Uttar Pradesh	11097
Karnataka	10741
Maharashtra	5496
Telangana	5024
Assam	3530

GOVERNMENT ROLE

India is a country where providing skills at a reasonable cost lies on the shoulder of the Government. In a country with a majority of middle-class families with meagre incomes, it naturally becomes tough to invest anywhere around Rs. 3-11 lakh for cybersecurity trainingThe governments' role in bridging the demand-supply gaps is equivocally undeniable. There is a silver lining amidst royal chaos in the form of the 8000 crores set aside for developing the scope of Quantum technologies and application. If put into practice the non-Indian way, this initiative can be a game-changer in the field of cybersecurity.

Corporate Insecurity and hesitancy to investIf there is a problem of execution on the government's part, corporates have their issues too. The ethic of which is up for discussion, but some other day. Right now, let us see what the problem is.Consider a scenario where a company X has provided the cybersecurity training program, and you have signed a two-year contract. Naturally, you will stay on for two years, but what after that. Say, if your foreign company is paying dollars to a rupee. Naturally, you will prefer the Dollar or Pound.

IMPACT ON ORGANIZATIONS:

Increased Vulnerabilities: The lack of skilled professionals leaves organizations exposed to cyberattacks, data breaches, and financial losses.

Compliance Challenges: Meeting stringent data privacy regulations and industry standards becomes difficult without adequate cybersecurity expertise.

Reputational Damage: Cyberattacks can severely damage an organization's reputation and erode customer trust.

Operational Disruption: Data breaches and cyberattacks can lead to business disruptions, impacting productivity and service delivery.

Innovation Hindrance: Fear of cyberattacks can hinder organizations from adopting new technologies and exploring digital transformation opportunities.

Education Reform: Develop industry-aligned cybersecurity programs, promote STEM education, and encourage hands-on training.

Awareness Campaigns: Organize workshops, career fairs, and mentorship programs to attract talent and address misconceptions.

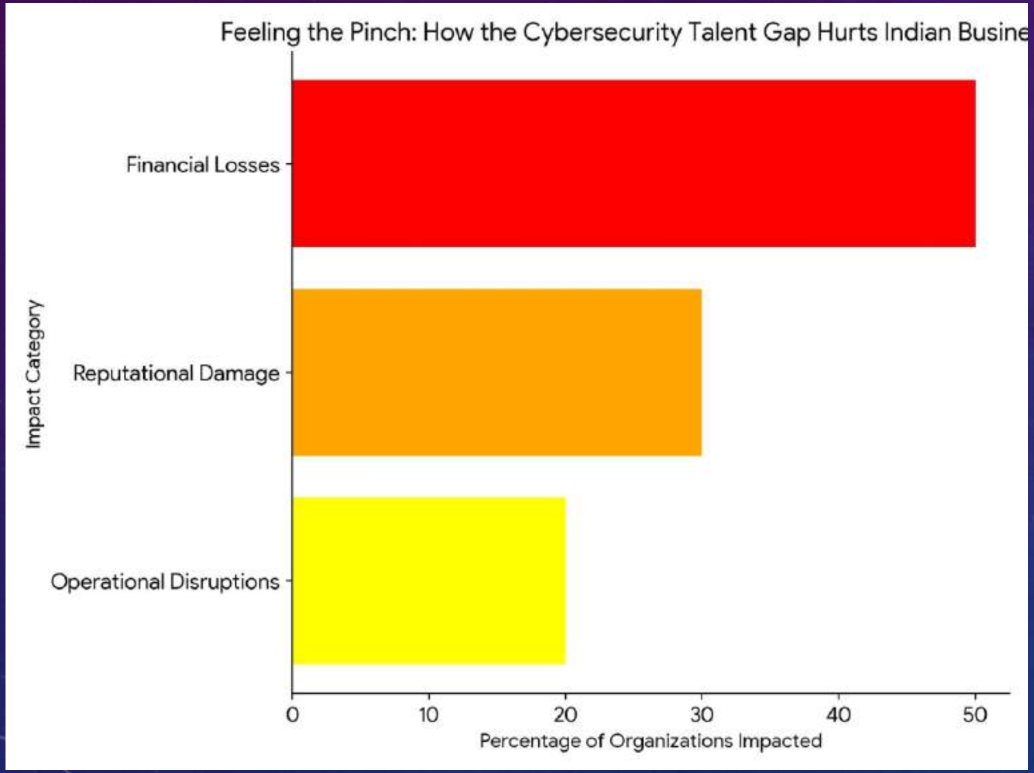
Upskilling Initiatives: Provide existing employees with cybersecurity training and certification programs to bridge the skill gap.

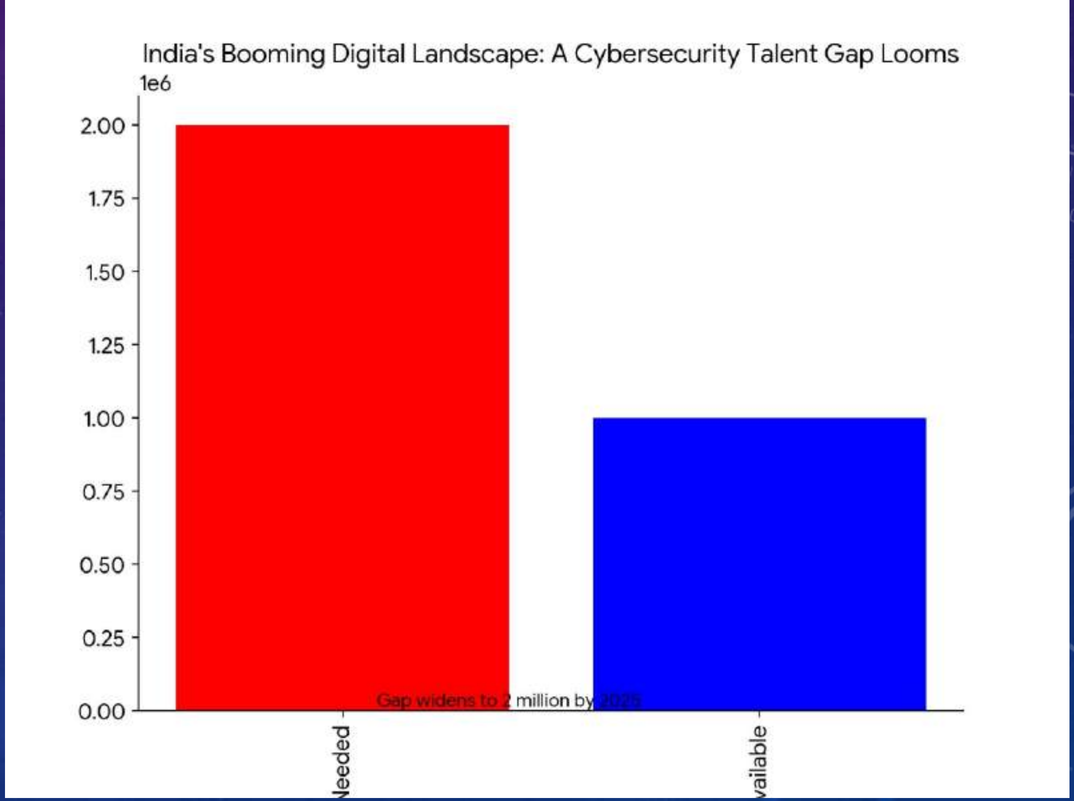
Government Support: Offer financial incentives, tax breaks, and research grants to encourage cybersecurity education and industry collaboration.

Public-Private Partnerships: Develop collaborative initiatives between academia, industry, and government to address the talent shortage effectively.

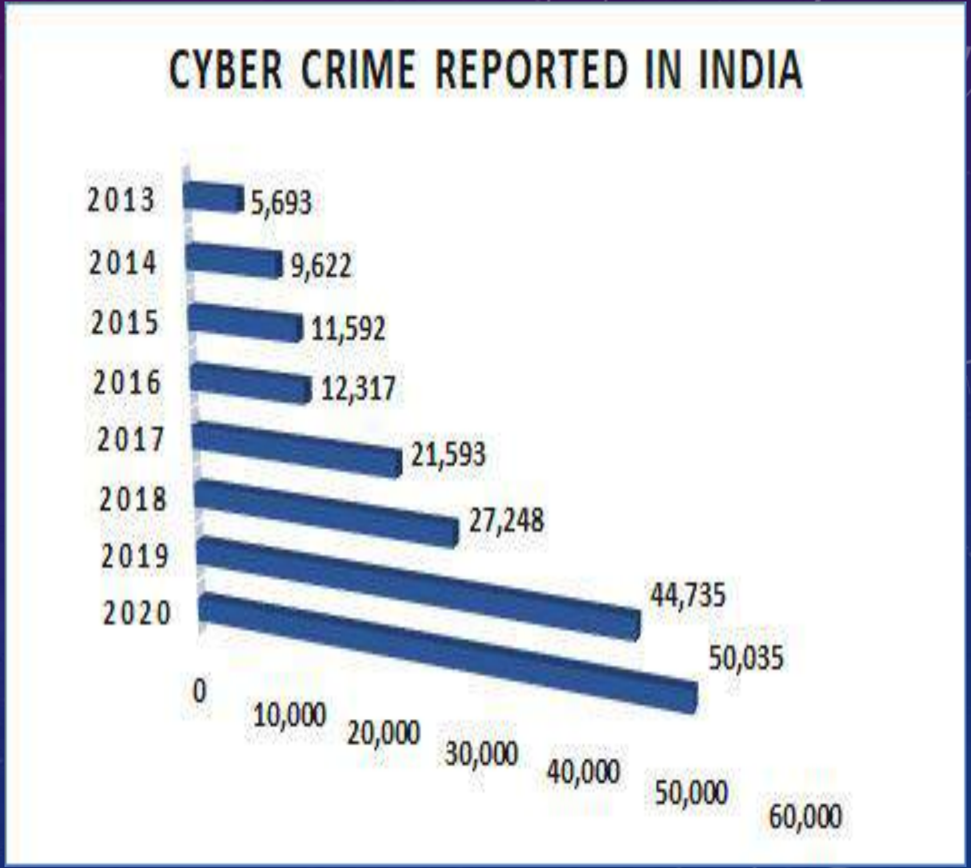
Conclusion: The shortage of cybersecurity professionals in India poses a significant threat to organizational security, compliance, and innovation. Addressing this challenge requires a multi-pronged approach involving education reform, awareness campaigns, upskilling initiatives, and government support. By working together, stakeholders can build a robust cybersecurity workforce and ensure a secure digital future for India.

CYBERSECURITY TALENT GAP





This cycle irks corporate employers, so many do not provide the advanced training required for cyber forensics. On some levels, their argument can be deemed as valid as they are putting in time and resources to train a candidate, hoping they would stay on and not abandon them mid-way.



LACK OF AWARENESS OF CYBER-SECURITY AS A POTENTIAL CAREER OPTION

Suppose you are a student in India who wishes to be a cybersecurity professional. Either of the two factors might have influenced you to consider this profession.

First, you might have seen your friends or relatives earning Pounds or Dollars, so the idea might draw you to this course too. Secondly, you must have been inspired by a movie.

There is no real awareness of the cybersecurity training program from authentic sources. The students are unaware of the salary that cybersecurity professionals get in India. This is also a part of the reason why aspiring students move abroad for cyber training for a better ROI, even in a situation where the Indian companies are willing to pay 2-to-10X of the standard salary.

If India needs to meet the demand for cyber professionals, the changes need to come from the grassroots level.

LACK OF EDUCATIONAL SPACE FOR CYBERSECURITY

The educational ecosystem is yet to create a considerable space for the cybersecurity section. The problem here is two-fold, at one level, there aren't enough training facilities to accommodate the number of students who are slowly showing interest in such a course.Secondly, cybersecurity is a dynamic field of study. It needs learning and relearning. So, the curriculum needs to be regularly updated, which is not just happening. As a result, students who are passing out and getting into the real world fail to deliver.Some of the private universities like AMITY have started providing cybersecurity courses. But the real change can come from the edtech startups and universities in combination with the likes of industry bodies like CII and NASSCOM.

OVERALL COST OF CYBERATTACKS IN INDIA:

The Rising Cost of Cybercrime in India

Average cost of a data breach in India (2023): ₹17.9 crore (Source: IBM Security Cost of a Data Breach Report 2023)

Estimated yearly losses due to cybercrime in India: ₹2 trillion (Source: NASSCOM)

Increase in average data breach cost in

India since 2020: 28%

Beyond the Breach: The Invisible Costs of Cyberattacks

- **Percentage of "hidden" costs in a data breach:** 60% (Source: Deloitte)
- **Hidden cost categories:** Reputation damage, operational disruption, loss of intellectual property, legal and regulatory fines
- **Example of hidden cost:** Data breach at Marriott International led to a $123 million fine from the UK Information Commissioner's Office (ICO)

Analyze a significant cyber attack(s) that has affected an Indian organization or institution. Evaluate the specific challenges faced, the response to the incident, and the lessons learned

Second Question

CYBERSECURITY CHALLENGES

- Cyberattacks are malicious attempts to gain unauthorized access to computer systems or networks. Attackers can then steal data, disrupt operations, install malware, or extort money. Common cyberattacks include:
- **Phishing:** Deceptive emails or messages designed to trick victims into revealing sensitive information.
- **Malware:** Malicious software that can damage or steal data.
- **Ransomware:** Encrypts data and demands ransom for its decryption.
- **Denial-of-Service (DoS) attacks:** Overload systems with traffic, making them unavailable to legitimate users.

ANALYZING THE COSMOS BANK CYBERATTACK: A CASE STUDY IN INDIA’S

- In 2018, Cosmos Bank, a cooperative bank in Pune, India, fell victim to a sophisticated cyberattack, exposing the vulnerabilityes of Indian institutions and highlighting the need for robust cybersecurity measures. This case study analyzes the Cosmos Bank attack, exploring the challenges faced, the response, and the key lessons learned.
- The Attack: Hackers gained access to Cosmos Bank’s ATM server, compromising debit card details of thousands of customers across 28 countries. Over ₹94.42 crore (roughly $1.3 million) was siphoned off within hours, highlighting the attack’s efficiency and devastating financial impact.
-

CHALLENGES FACED:

.

- **Outdated Technology:** Cosmos Bank relied on older, less secure systems, making them susceptible to vulnerabilities exploited by attackers.
- **Limited Cybersecurity Awareness:** Lack of employee training and awareness campaigns left staff vulnerable to phishing attacks and social engineering tactics.
- **Inadequate Security Measures:** Weak passwords, lack of multi-factor authentication, and insufficient data encryption contributed to the breach.
- **Delayed Response:** Initial delays in identifying and responding to the attack allowed hackers to move funds before mitigation efforts could be implemented.

IN REACTION TO THE EVENT:

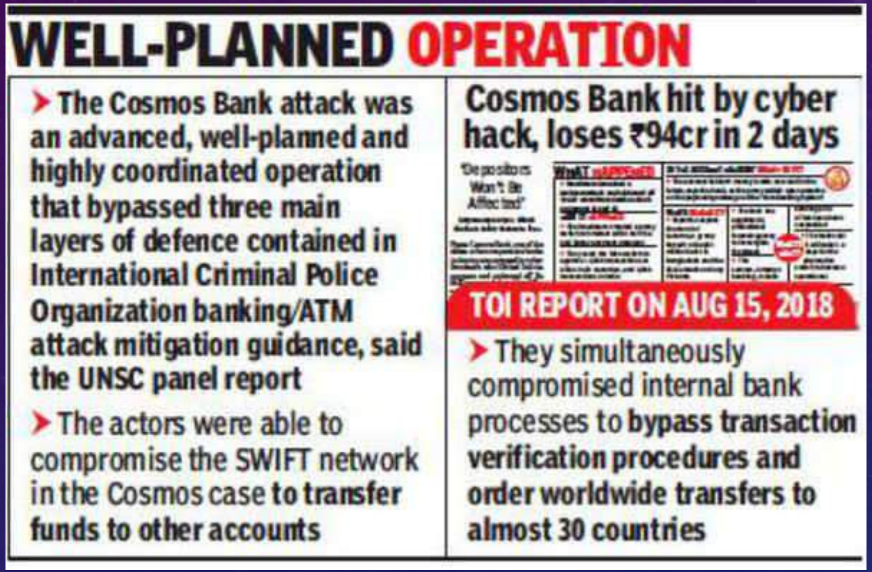
Investigation and Forensics: In order to look into the incident, locate its source, and stop additional harm, Cosmos Bank collaborated with specialists in cybersecurity.

Law Enforcement Involvement: In order to locate the attackers and retrieve the pilfered money, authorities were alerted and requested international cooperation.

Measures of Compensation: The bank showed responsibility and customer concern by paying out compensation to impacted clients for their losses.

Cosmos Bank strengthened their security protocols by introducing more stringent measures such as personnel training, system updates, and improved data encryption.

DATA AND IMPACT:



WELL-PLANNED OPERATION

➤ The Cosmos Bank attack was an advanced, well-planned and highly coordinated operation that bypassed three main layers of defence contained in International Criminal Police Organization banking/ATM attack mitigation guidance, said the UNSC panel report

➤ The actors were able to compromise the SWIFT network in the Cosmos case to transfer funds to other accounts

Cosmos Bank hit by cyber hack, loses ₹94cr in 2 days

'Depositors Won't Be Affected'

TOI REPORT ON AUG 15, 2018

➤ They simultaneously compromised internal bank processes to bypass transaction verification procedures and order worldwide transfers to almost 30 countries

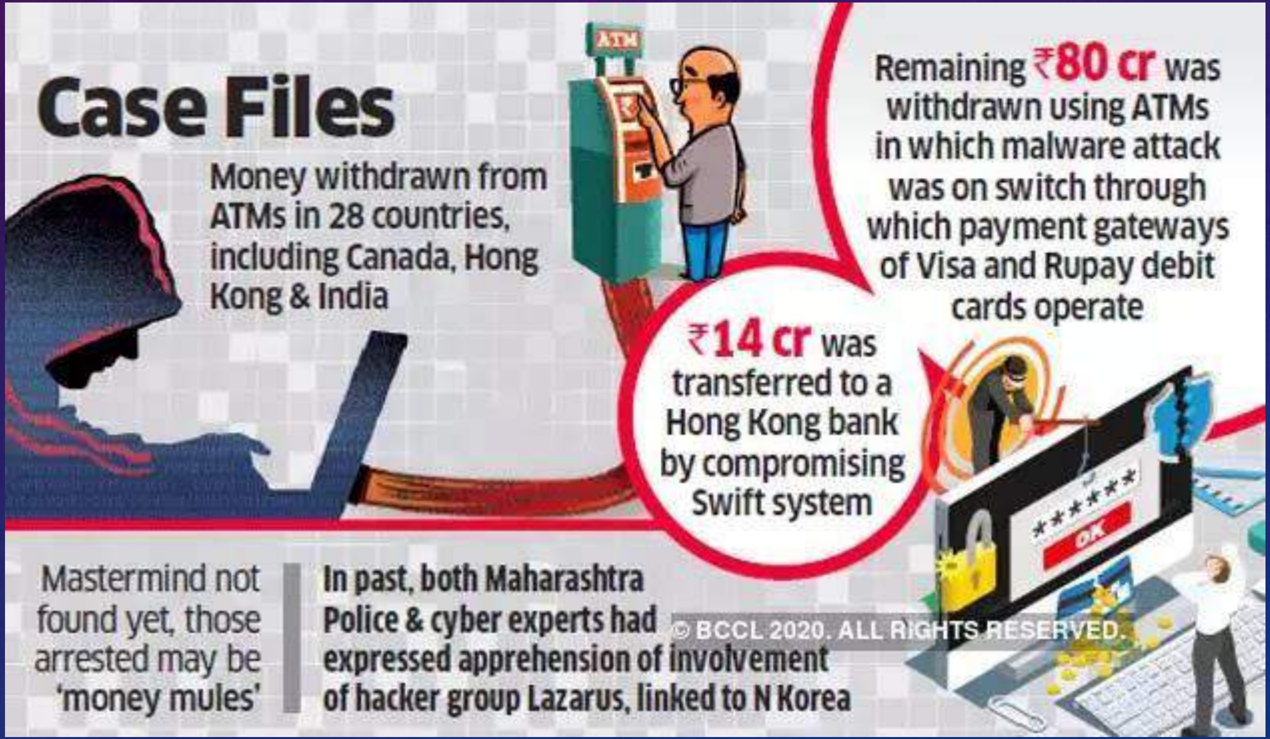
Stolen Amount: ₹94.42 crore (≈ $1.3 million)

Affected Customers: Thousands across 28 countries

Reputational Damage: Significant loss of trust and brand image

Regulatory Fines: Potential penalties for non-compliance with data privacy regulations

NEWS ARTICLES



Case Files

Money withdrawn from ATMs in 28 countries, including Canada, Hong Kong & India

Remaining ₹80 cr was withdrawn using ATMs in which malware attack was on switch through which payment gateways of Visa and Rupay debit cards operate

₹14 cr was transferred to a Hong Kong bank by compromising Swift system

Mastermind not found yet, those arrested may be 'money mules'

In past, both Maharashtra Police & cyber experts had expressed apprehension of involvement of hacker group Lazarus, linked to N Korea

The cyberattack on Cosmos Bank is a sobering reminder of how urgently India needs strong cybersecurity protections. Organisations may create strong defences against changing cyberthreats and protect their operational integrity, customer confidence, and financial stability by investing in technology, training, and awareness.

INVESTIGATE THE TOP CYBERSECURITY PROBLEMS FACED BY UNIVERSITIES AND COLLEGES, WITH A FOCUS ON THE SPECIFIC TYPES OF CYBERATTACKS TARGETING HIGHER EDUCATION INSTITUTIONS

THIRD QUESTIONS

CYBERSECURITY CHALLENGES FOR UNIVERSITIES AND COLLEGES

- Targeted Attacks on Higher Education
- Universities and colleges hold a wealth of sensitive data, making them prime targets for cybercriminals. This analysis investigates the top cybersecurity problems faced by these institutions, focusing on the specific types of cyberattacks they encounter.
- Critical Cybersecurity Issues:
- 1. Phishing: Social engineering attempts remain a top threat, tricking unsuspecting students, faculty, and staff into clicking on malicious links or attachments. These attacks can expose credentials, steal sensitive data, or infiltrate malware.

- Ransomware: Universities are increasingly targeted by ransomware attacks, encrypting crucial data and demanding hefty ransoms for decryption. Disrupting research, admissions, and financial operations, these attacks carry significant financial and reputational costs
- 3. Data Breaches: From student records to research data, universities store various sensitive information prone to breaches through vulnerabilities in systems, human error, or targeted attacks. Data breaches can compromise intellectual property, expose personal information, and violate privacy regulations.
- 4. Insider Threats: Malicious insiders with authorized access can pose a significant risk, intentionally or unintentionally causing damage through data theft, misuse of privileges, or sabotage.
- **Unpatched Systems & Outdated Software:** Outdated software and unpatched systems often have known vulnerabilities that attackers can exploit to gain access or install malware. Universities struggle to manage diverse systems and prioritize patching due to budget constraints and resource limitations.
- **6. Lack of Cybersecurity Awareness:** Insufficient cybersecurity awareness among staff and students can leave them susceptible to phishing attacks, social engineering tactics, and risky online behavior.

SPECIFIC TYPES OF CYBERATTACKS TARGETING HIGHER EDUCATION:

1. Credential Stuffing: Hackers leverage stolen login credentials from other sources to gain unauthorized access to university systems.

2. Spear Phishing: Targeted phishing attacks aimed at specific individuals or departments, exploiting personal information or research interests to increase trust and success rates.

3. Malware Attacks: Malware like keyloggers, data exfiltration tools, and ransomware are often deployed through phishing emails or by exploiting system vulnerabilities.

4. Denial-of-Service (DoS) Attacks: Overwhelming university websites or networks with traffic to disrupt operations, access to online resources, or critical services.

Supply Chain Attacks: Targeting vulnerabilities in third-party software or services used by the university to gain access to their systems and data.

6. Zero-Day Attacks: Exploiting previously unknown vulnerabilities in software or systems before patches are available, making them particularly challenging to defend against.

IMPORTANCE AND CHALLENGES

- Impact of Cyberattacks:
-
- Financial losses from ransom payments, data recovery, and system repairs.
- Reputational damage and loss of trust among students, faculty, and donors.
- Operational disruptions impacting research, admissions, and student services.
- Compliance violations and potential regulatory fines.

- Addressing the Challenges
- Implement comprehensive cybersecurity awareness training for staff and students.
- Utilize multi-factor authentication and strong password policies.
- Patch systems regularly and address software vulnerabilities promptly.
- Conduct regular security assessments and penetration testing.
- Have a robust incident response plan and disaster recovery procedures.
- Invest in security technologies and monitoring tools.
- Collaborate with cybersecurity experts and other institutions to share information and best practices.

REAL-TIME EXAMPLE OF A CYBERSECURITY ATTACK ON AN INDIAN UNIVERSITY (OCTOBER 27, 2023)

Institution: National Institute of Technology, Warangal (NITW)

Attack Type: Ransomware

Impact: Over 20 servers encrypted, including those belonging to crucial departments like the library, administration, and placement cell.

Access to online academic resources, student portals, and administrative workflows disrupted.

Exams and admissions processes are potentially affected.

- The attack reportedly occurred on October 27, 2023, and initially targeted the library server before spreading to other systems.
- The ransomware strain is yet to be identified, but the attackers demanded a ransom for decryption.
- NITW authorities shut down affected systems and launched an investigation with the help of cybersecurity experts.
- No data exfiltration has been confirmed as of yet.

- Significance
- This attack highlights the ongoing vulnerability of Indian educational institutions to cyber threats. It serves as a timely reminder for universities to:
- Further Developments:
- The investigation into the attack is ongoing, and NITW has not yet confirmed whether they paid the ransom or successfully decrypted the systems.
- The Ministry of Education has issued an advisory to all universities and colleges, urging them to strengthen their cybersecurity posture.

CONCLUSION

- Universities and colleges face a growing array of cybersecurity threats. By understanding the specific challenges they encounter and implementing robust security measures, institutions can protect their valuable data, ensure operational stability, and build trust with their communities.

Select and analyze three real-world malware attacks, covering different malware types
such as viruses, worms, and ransomware. For each case, describe the attack vector, the
target, the impact.

Fourth question

VIRUS

Consider it as: A malicious application that joins itself to a trustworthy application or file.

How does it proliferate? The virus multiplies and becomes active when you access the infected file or programme, infecting further files or computers on the network.

Impact: Viruses can steal data, corrupt or damage files, and disrupt with system functionality.

Examples are Code Red, Melissa, and Stuxnet.

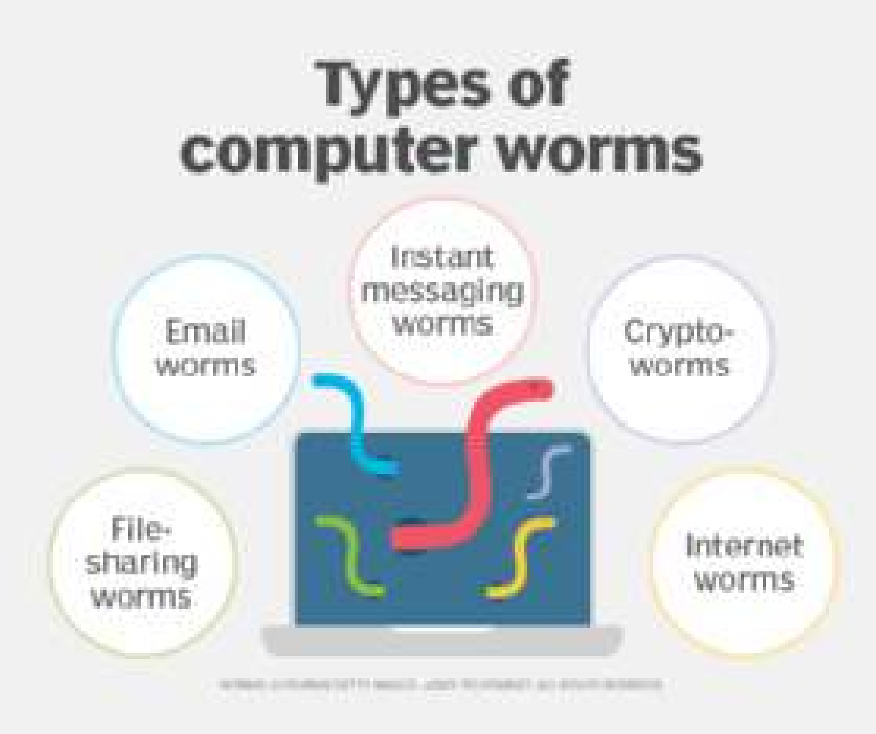
WORM

Think of it as: A self-replicating program that doesn't necessarily need to attach itself to other files.

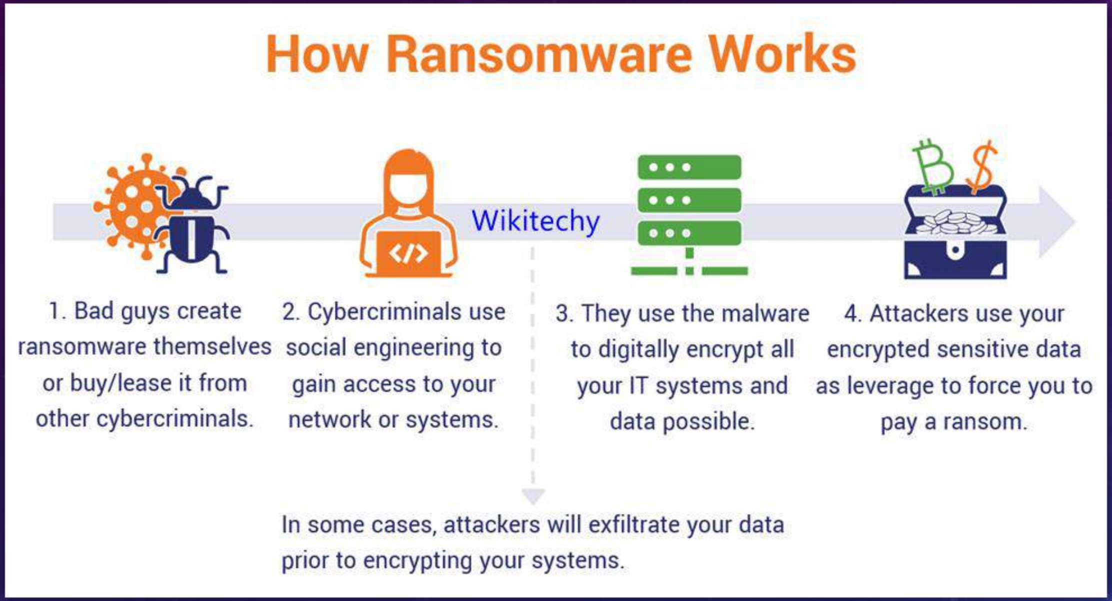
How it spreads: Worms exploit vulnerabilities in systems or networks to spread rapidly, often through network connections or removable media.

Impact: Worms can consume system resources, clog networks, and potentially deliver other malware like viruses or ransomware.

Examples: Morris Worm, Conficker, Blaster



RANSOMWARE



How Ransomware Works

1. Bad guys create ransomware themselves or buy/lease it from other cybercriminals.
2. Cybercriminals use social engineering to gain access to your network or systems.
3. They use the malware to digitally encrypt all your IT systems and data possible.
4. Attackers use your encrypted sensitive data as leverage to force you to pay a ransom.

In some cases, attackers will exfiltrate your data prior to encrypting your systems.

Think of it as: A type of malware that encrypts your files, making them inaccessible.

How it works: Ransomware can infect your computer through various means like phishing emails, malicious websites, or infected attachments. Once activated, it encrypts your files and demands a ransom payment for decryption.

Impact: Ransomware can lock you out of your important data, causing significant disruption and financial loss. Paying the ransom doesn't guarantee data recovery and might encourage further attacks.

Examples: WannaCry, Locky, REvil

NOTPETYA: A DEVASTATING WORM (JUNE 2017)

Attack Vector: Phishing emails containing malicious attachments.

Target: Primarily Ukrainian organizations, but spread globally due to vulnerable systems.

Malware Type: Worm - self-replicating and spreading automatically.

Impact:

Over 200,000 systems infected worldwide, including hospitals, banks, and government agencies.

Wiped data from infected systems, rendering them unusable.

Estimated global economic losses exceeding $10 billion.

NotPetya disguised itself as legitimate software updates, exploiting vulnerabilities in popular accounting software. Its rapid spread highlighted the interconnectedness of global systems and the potential for catastrophic damage from worms

WANNACRY RANSOMWARE: A GLOBAL CRY FOR HELP (MAY 2017)

- EternalBlue exploit targeting unpatched Windows systems.
- Target: Organizations worldwide, regardless of size or industry.
- Malware Type: Ransomware – encrypts files and demands ransom for decryption.
- Impact:
- Infected over 300,000 computers in 150 countries.
- Caused significant disruptions in hospitals, businesses, and critical infrastructure.
- Ransom demands ranged from $300 to $300,000 per infected device.
- Analysis: WannaCry exploited a known vulnerability in older Windows versions, highlighting the importance of timely patching. The attack sparked global discussions on cybersecurity preparedness and ransomware threats.

ATTACK: EMOTET (2023)

- Type: Polymorphic virus (able to change its code to evade detection)
- Target: Individuals and organizations worldwide
- Attack Vector: Phishing emails with malicious attachments or links
- Impact:
- Spreads to other devices on the network: Emotet infects a single device first and then uses it to spread to other connected devices within the network, compromising multiple systems.
- Downloads additional malware: Once installed, Emotet acts as a backdoor, allowing attackers to download other malware like ransomware or steal sensitive data.

- **Disrupts operations:** By infecting multiple devices and potentially downloading additional malware, Emotet can disrupt business operations, leading to lost productivity and financial losses.
- **Data theft:** Stolen data can be used for identity theft, financial fraud, or sold on the black market.
- May 2023, Emotet targeted several healthcare organizations in the United States with phishing emails containing malicious attachments. The attack compromised numerous devices and allowed attackers to steal sensitive patient data. The healthcare providers had to invest significant resources in recovering their systems, mitigating the damage, and restoring patient trust.
- Key Takeaways:
- Viruses like Emotet can have a cascading effect, compromising multiple devices and leading to additional malware infections.
- They can cause significant disruptions to operations and data breaches, resulting in financial losses and reputational damage.
- Staying vigilant and practicing safe online habits like avoiding suspicious emails and attachments is crucial in protecting yourself from virus attacks.

CONCLUSION

- Always use caution when using the internet, such as by avoiding dubious links and attachments.
- Make use of reliable malware and antivirus programmes.
- Utilise the most recent security fixes to keep your operating systems and applications updated.
- Make frequent backups of your data to lessen the effect of potential intrusions.
- You can safeguard your data and yourself from malicious software by being aware of these risks and taking precautions.
-

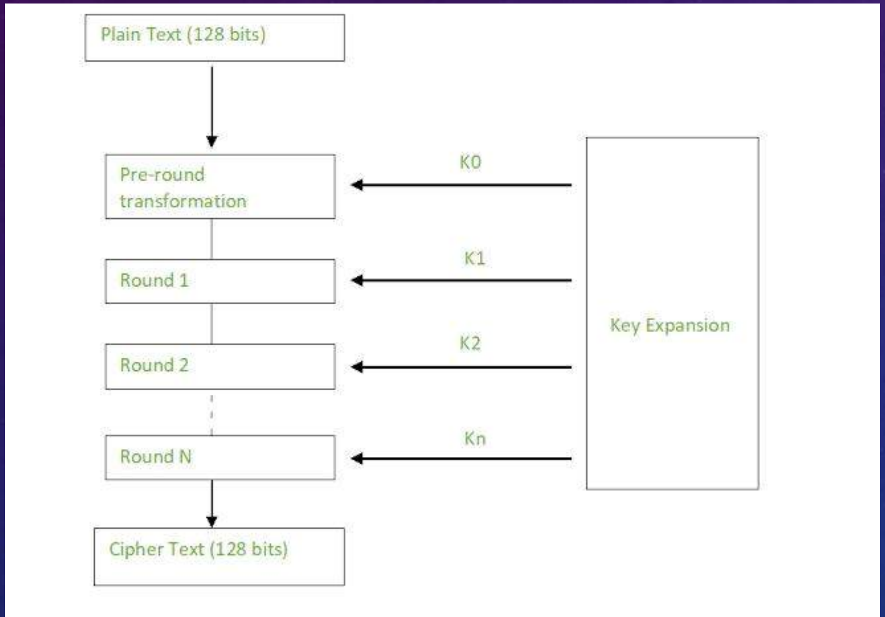
PROVIDE COMPARATIVE ANALYSIS ON DES, AES, RSA.

FIFTH QUESTION

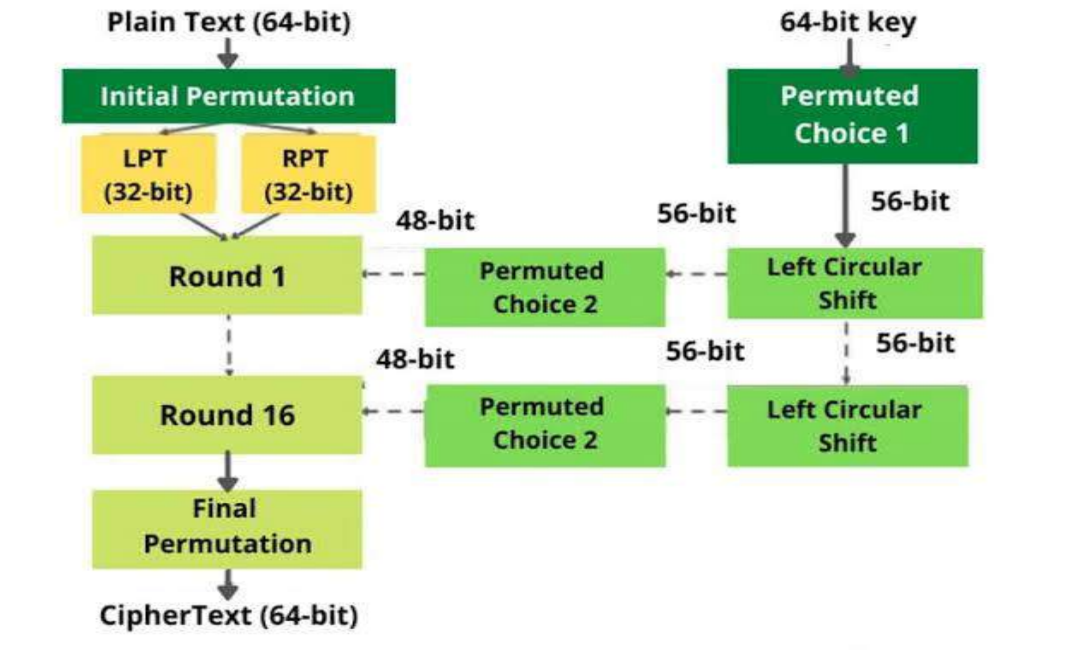
ANALYSIS OF DES, AES, AND RSA ENCRYPTION ALGORITHMS

- DES, AES, and RSA are all important encryption algorithms used to secure data, but they differ in their key types, speeds, and ideal applications
- **DES (Data Encryption Standard):**
- **Type:** Symmetric, meaning the same secret key is used for both encryption and decryption.
- **Key length:** 56 bits (considered weak by today's standards).
- **Speed:** Relatively slow.
- **Application:** Due to its age and weak key length, DES is rarely used for new applications. It's mainly found in legacy systems, though sometimes as an enhanced variant called Triple-DES (3DES).

DES

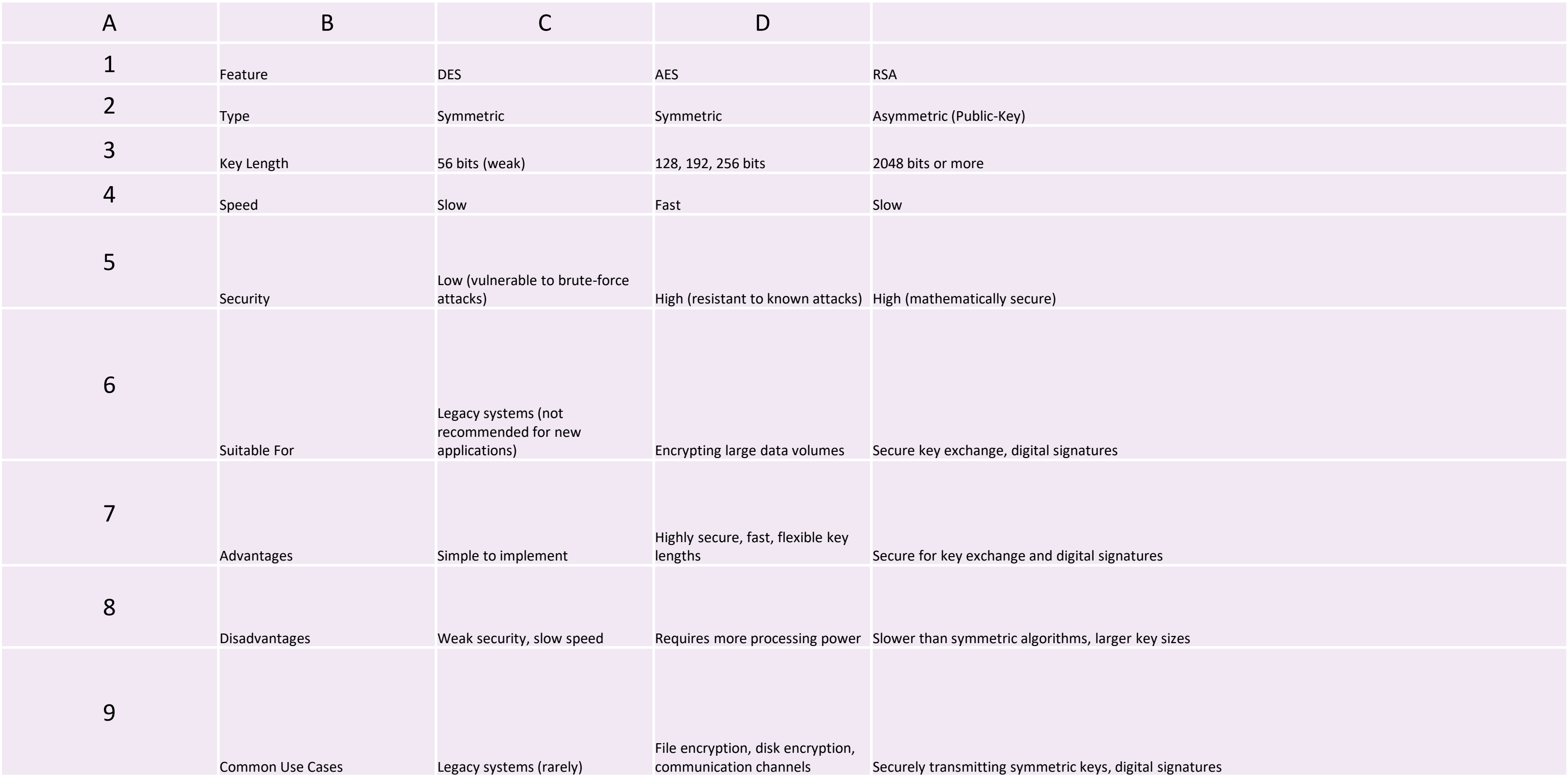

Plain Text (128 bits)
Pre-round transformation
Round 1
Round 2
Round N
Cipher Text (128 bits)
K0
K1
K2
Kn
Key Expansion

Aes


Plain Text (64-bit)
Initial Permutation
LPT (32-bit)
RPT (32-bit)
Round 1
Round 16
Final Permutation
CipherText (64-bit)
64-bit key
Permuted Choice 1
56-bit
Left Circular Shift
56-bit
Left Circular Shift
56-bit
Permuted Choice 2
56-bit
Permuted Choice 2
48-bit
48-bit

- DES (Data Encryption Standard):
- Type: Symmetric, meaning the same secret key is used for both encryption and decryption.
- Key length: 56 bits (considered weak by today's standards).
- Speed: Relatively slow.
- Application: Due to its age and weak key length, DES is rarely used for new applications. It's mainly found in legacy systems, though sometimes as an enha
- nced variant called Triple-DES (3DES).
- **Application:** Primarily used for secure key exchange (e.g., sending an AES key securely) and digital signatures (verifying the authenticity of data). Due to its slower speed, it's not suitable for encrypting large amounts of data directly.

COMPARATIVE ANALYSIS ON DES, AES, RSA.



A	B	C	D	
1	Feature	DES	AES	RSA
2	Type	Symmetric	Symmetric	Asymmetric (Public-Key)
3	Key Length	56 bits (weak)	128, 192, 256 bits	2048 bits or more
4	Speed	Slow	Fast	Slow
5	Security	Low (vulnerable to brute-force attacks)	High (resistant to known attacks)	High (mathematically secure)
6	Suitable For	Legacy systems (not recommended for new applications)	Encrypting large data volumes	Secure key exchange, digital signatures
7	Advantages	Simple to implement	Highly secure, fast, flexible key lengths	Secure for key exchange and digital signatures
8	Disadvantages	Weak security, slow speed	Requires more processing power	Slower than symmetric algorithms, larger key sizes
9	Common Use Cases	Legacy systems (rarely)	File encryption, disk encryption, communication channels	Securely transmitting symmetric keys, digital signatures

SELECTING AES, RSA, DES

- Data sensitivity: Highly sensitive data requires stronger algorithms like AES or RSA.
- Data size: For large volumes, fast encryption like AES is preferred.
- Performance requirements: Real-time applications demand faster algorithms like AES.
- Security needs: If key exchange or digital signatures are crucial, RSA is suitable.
- **Key Management:** For symmetric algorithms like DES and AES, secure key management is crucial.
- **Standardization:** AES is the current standard for symmetric encryption, while RSA is a widely used public-key algorithm.
- **Performance:** For real-time applications, AES's speed is often essential. For tasks like digital signatures, security takes priority over speed, making RSA suitable.
- **Hybrid Cryptosystems:** Combining symmetric and asymmetric algorithms can leverage their individual strengths for optimal security and performance.

THANK YOU