edureka!

MASTERING CYBERSECURITY WITH EDUREKA

Getting Started with Cybersecurity

Don't just Learn it, Master it!

TABLE OF CONTENTS

TABLE OF CONTENTS

Chapter 1

INTRODUCTION TO CYBERSECURITY

Cybercrime is a global problem that's been dominating the news cycle. It poses a threat to individual security and an even bigger threat to large international companies, banks, and governments. Today's organized cybercrimes out shadow lone hackers of the past, now large organized crime rings function like start-ups and often employ highly-trained developers who are constantly innovating online attacks. With so much data to exploit out there, Cybersecurity has become essential.

1.1 What is Cybersecurity?

Cybersecurity refers to a set of techniques used to protect the integrity of networks, programs and data from attack, damage or unauthorized access. From a computing point of view, security comprises cybersecurity and physical security — both are used by enterprises to protect against unauthorized access to data centers and other computerized systems.

Information security, which is designed to maintain the confidentiality, integrity, and availability of data, is a subset of Cybersecurity. The term 'Cybersecurity' refers to techniques and practices designed to protect digital data. Effective cybersecurity reduces the risk of cyber-attacks and protects organizations and individuals from the unauthorized exploitation of systems, networks, and technologies.

1.2 Need for Cybersecurity

With each passing year, the sheer volume of threats is increasing rapidly. According to the report by McAfee, cybercrime now stands at over $400 billion, while it was $250 billion two years ago.

1. Cyberattacks can be extremely expensive for businesses to endure. In addition to financial damage suffered by the business, a data breach can also inflict untold reputational damage.
2. Cyberattacks these days are becoming progressively destructive. Cybercriminals are using more sophisticated ways to initiate cyber attacks.
3. Regulations such as GDPR are forcing organizations into taking better care of the personal data they hold.

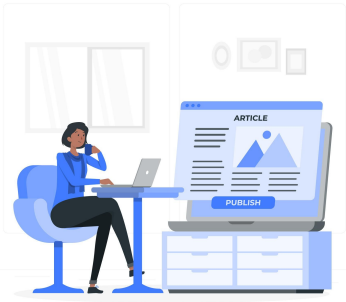
CYBERSECURITY BENEFITS

Business Protection

Protection For Data And Networks

Prevention Of Unauthorized User Access

Improved Recovery Time



Protection For End Users

Regulatory Compliance

Chapter 2

CIA TRIAD

Confidentiality, Integrity, and Availability, also known as the CIA Triad, is a model designed to guide companies and organizations to form their security policies. It is also known as the AIC triad to avoid confusion with Central Intelligence Agency (CIA). The components of the triad are considered to be the most important and fundamental components of security.

2.1 Confidentiality

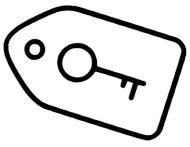
Confidentiality is about preventing the disclosure of data to unauthorized parties. It also means trying to keep the identity of authorized parties involved in sharing and holding data private and anonymous. Often confidentiality is compromised by cracking poorly encrypted data, Man-in-the-middle (MITM) attacks, and disclosing sensitive data. Standard measures to establish confidentiality include:

CONFIDENTIALITY MEASURES

Data Encryption

Biometric Verification

Two-Factor Authentication



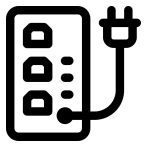
Security Tokens

2.2 Integrity

Integrity refers to protecting information from being modified by unauthorized parties. It is a requirement that information and programs are changed only in a specified and authorized manner. Challenges that could endanger integrity include turning a machine into a “zombie computer”, embedding malware into web pages, etc. Standard measures to guarantee integrity include:

INTEGRITY MEASURES

Cryptographic Checksums



Uninterrupted Power Supplies

Using File Permissions

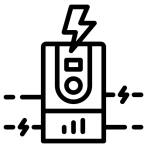
Data Backups

2.3 Availability

Availability is making sure that authorized parties are able to access the information when needed. Data only has value if the right people can access it at the right time. Information unavailability can occur due to security incidents such as DDoS attacks, hardware failures, programming errors, human errors. Standard measures to guarantee availability include:

AVAILABILITY MEASURES

Backing up Data to External Drives



Having Backup Power Supplies

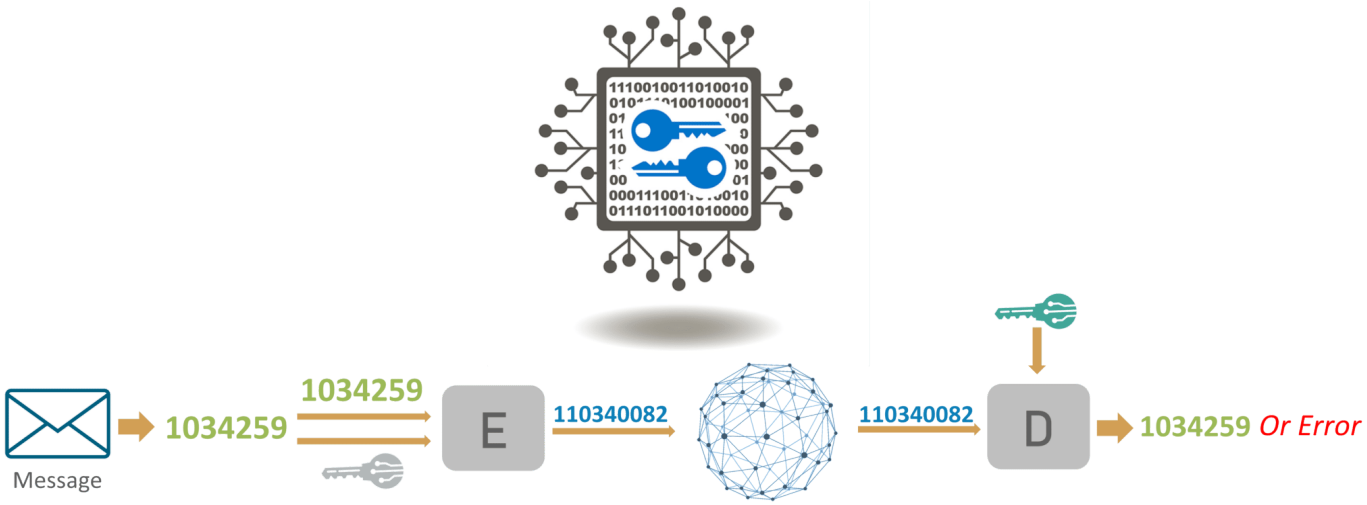
Implementing Firewalls

Data Redundancy

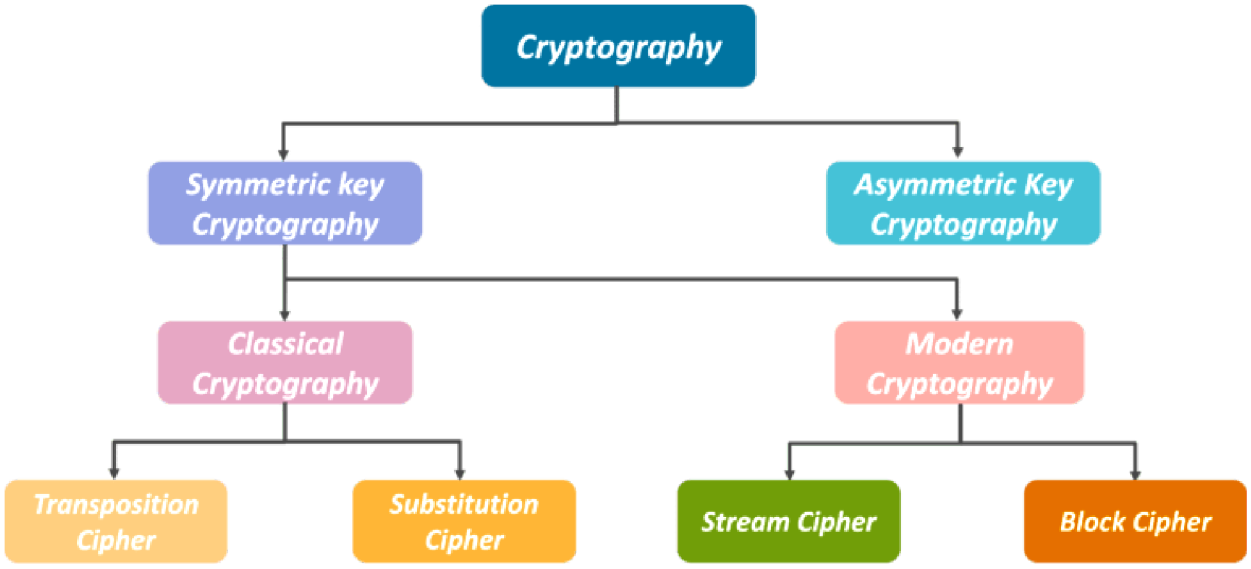
Chapter 3

INTRODUCTION TO CRYPTOGRAPHY

Cryptography is the practice and study of techniques for securing communication and data in the presence of adversaries.



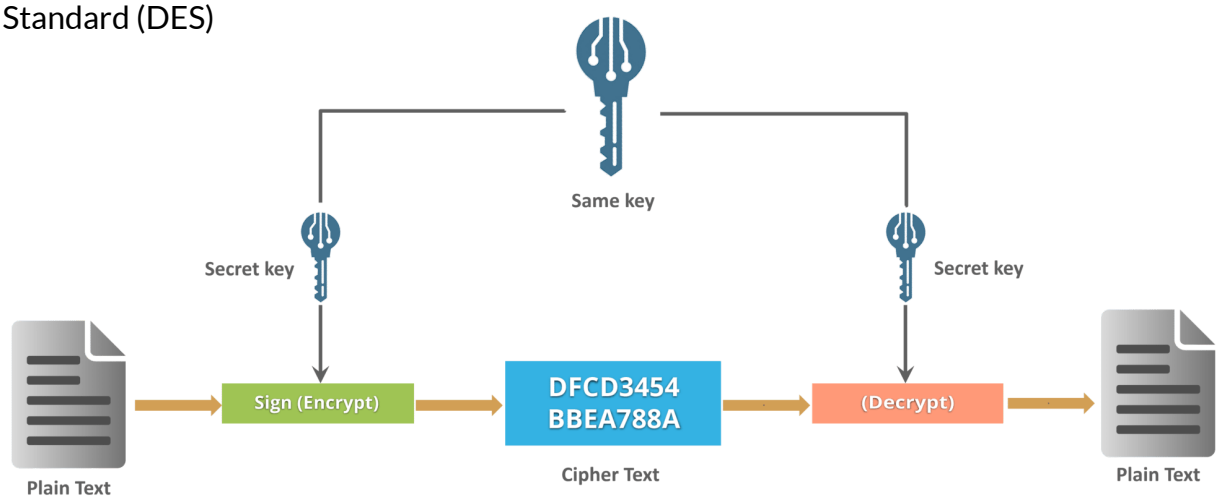
Based on the type of keys and encryption algorithms, cryptography is classified under various categories. Cryptography is broadly classified into two categories: Symmetric key Cryptography and Asymmetric key Cryptography (popularly known as public-key cryptography).



So, let's understand these algorithms with examples.

3.1 Symmetric Key Encryption

An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. The most popular symmetric–key system is the Data Encryption Standard (DES)



1 TRANSPOSITION CIPHERS

In Cryptography, a Transposition Cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system so that the ciphertext constitutes a permutation of the plaintext. That is, the order of the units is changed (the plaintext is reordered). Mathematically, a bijective function is used on the characters' positions to encrypt and an inverse function to decrypt.

1	2	3	4	5	6
M	E	E	T	M	E
A	F	T	E	R	P
A	R	T	Y		

4	2	1	6	3	5
T	E	M	E	E	M
E	F	A	P	T	R
Y	R	A		T	

Plain Text: MEET ME AFTER PARTY

Key Used: 421635

Cipher Text: TEMEEMEFAPTRYRAT

2 SUBSTITUTION CIPHER

Method of encryption by which units of plaintext are replaced with ciphertext, according to a fixed system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth.

Plaintext Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ

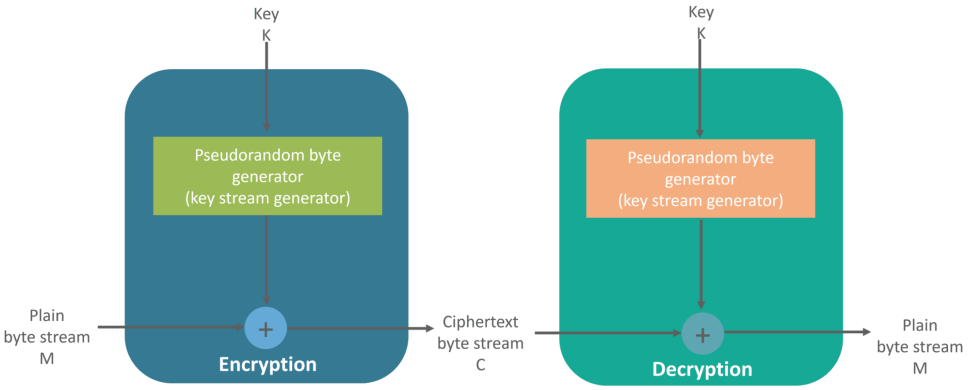
Keyword: Zebras

Ciphertext Alphabet: ZEBRASCDFGHIJKLMNOPQTUVWXY

A message of: flee at once. We are discovered!
enciphers to: SIAA ZQ LKBA. VA ZOA RFPBLUAOAR!
SIAAZ QLKBA VAZOA RFPBL UAOAR

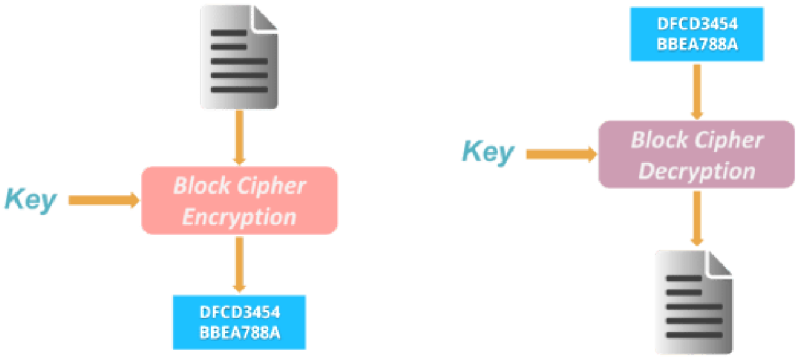
3 STREAM CIPHER

Symmetric or secret-key encryption algorithm that encrypts a single bit at a time. With a Stream Cipher, the same plaintext bit or byte will encrypt to a different bit or byte every time it is encrypted.



4 BLOCK CIPHER

An encryption method that applies a deterministic algorithm along with a symmetric key to encrypt a block of text, rather than encrypting one bit at a time as in stream ciphers.

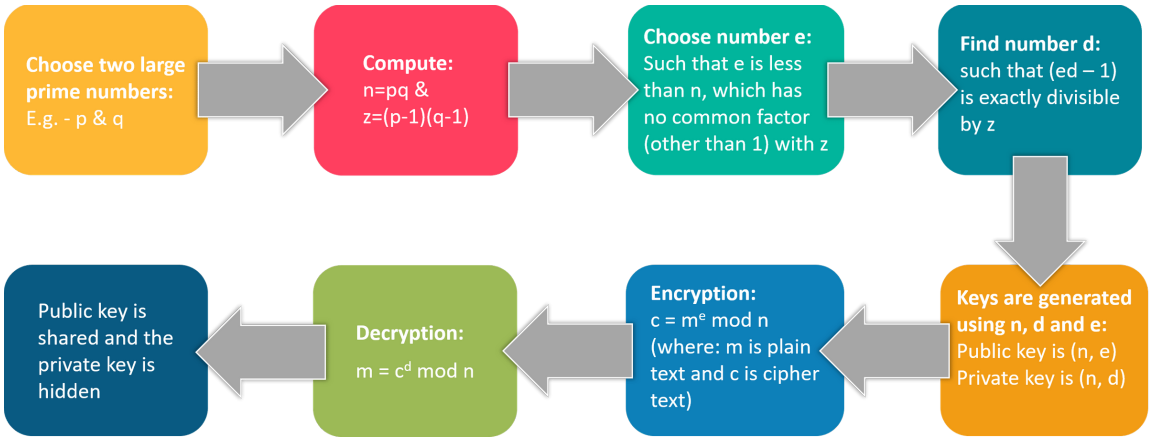


3.2 Asymmetric Key Encryption

The encryption process where different keys are used for encrypting and decrypting the information. Keys are different but are mathematically related, such that retrieving the plain text by decrypting ciphertext is feasible.

RSA ALGORITHM

RSA stands for Rivest, Shamir, and Adelman, inventors of this technique. Both public and private key are interchangeable. Variable Key Size (512, 1024, or 2048 bits)



Chapter 4

ETHICAL HACKING

Hacking is the process of finding vulnerabilities in a system and using these found vulnerabilities to gain unauthorized access into the system to perform malicious activities ranging from deleting system files to stealing sensitive information. Hacking is illegal and can lead to extreme consequences if you are caught in the act. People have been sentenced to years of imprisonment because of hacking. Nonetheless, hacking can be legal if done with permission. Computer experts are often hired by companies to hack into their systems to find vulnerabilities and weak endpoints so that they can be fixed. This is done as a precautionary measure against legitimate hackers who have malicious intent. Such people, who hack into a system with permission, without any malicious intent, are known as Ethical Hackers and the process is known as Ethical Hacking.

4.1 Types of Ethical Hackers

WHITE HAT HACKER
It is another name for an Ethical Hacker. They hack into a system with prior permission to find out vulnerabilities so that they can be fixed before a person with malicious intent finds them.

BLACK HAT HACKER
They are also known as Crackers, who hack in order to gain unauthorized access to a system & harm its operations or steal sensitive information. It's always illegal because of its malicious intent which includes stealing corporate data, violating the privacy, damaging the system, etc.

GREY HAT HACKER
They are a blend of both Black Hat and White Hat Hackers. They mostly hack for fun and exploit a security weakness in a computer system or network without the owner's permission or knowledge. Their intent is to bring the weakness to the attention of the owners & earning some bug bounty.

SUICIDE HACKER

A Suicide Hacker is a person who works with the intent to bring down major corporations and infrastructure. These kinds of hackers are not scared of the consequences of their actions as they mostly work with a vengeance in their minds. These people are also known as hacktivists.

4.2 Types of Hacking

Now that we have discussed the various types of Hackers, let's go over the different types of hacking. We can segregate hacking into different types depending on what the hacker is trying to achieve.

1. **WEBSITE HACKING**

   Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.

2. **NETWORK HACKING**

   Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. with the intent to harm the network system and hamper its operation.

3. **EMAIL HACKING**

   This includes gaining unauthorized access to an Email account and using it without taking the consent of its owner for sending out spam links, third-party threats, and other such harmful activities.

4. **PASSWORD HACKING**

   This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.

5. **COMPUTER HACKING**

   This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.

Chapter 5

PHASES OF ETHICAL HACKING

Ethical hacking has 6 distinct phases which are not strict rules, but more like a guidelines to be followed.

PHASE 1

RECONNAISSANCE

Reconnaissance is the process of information gathering. In this phase, the hacker gathers relevant information regarding the target system. These include detecting services, operating systems, packet-hops to reach the system, IP configuration, etc. Various tools like Nmap, Hping, Google Dorks, etc are used for reconnaissance purposes.

PHASE 2

SCANNING

In the scanning phase, the hacker begins to actively probe the target machine or network for vulnerabilities that can be exploited. Tools like Nessus, Nexpose, and NMAP are widely used by hackers in this process.

PHASE 3

GAINING ACCESS

In this phase, the vulnerability located during scanning is exploited using various methods and the hacker tries to enter the target system without raising any alarms. The primary tool that is used in this process is Metasploit.

PHASE 4

MAINTAINING ACCESS

This is one of the most integral phases. In this phase, the hacker installs various backdoors and payloads onto the target system. Just in case you don't know, Payload is a term used for activities performed on a system after gaining unauthorized access. Backdoors help the hacker gaining quicker access onto the target system in the future.

PHASE 5

CLEARING TRACKS

This process is an unethical activity. It has to do with the deletion of logs of all the activities that take place during the hacking process. Nonetheless, Ethical Hackers still have to perform this phase to demonstrate how a Black Hat Hacker would go about his activities.

PHASE 6

REPORTING

Reporting is the last step of finishing the ethical hacking process. Here the Ethical Hacker compiles a report with his findings and the job that was done such as the tools used, the success rate, vulnerabilities found, and the exploit processes.

Chapter 6

CYBERSECURITY FRAMEWORKS

The Framework is voluntary guidance, based on existing guidelines, and practices for organizations to better manage and reduce cybersecurity risk. Developed through coordinated effort amongst business and government, the intentional Framework comprises measures, rules, and practices to showcase the safety of imperative foundation. The organized, adaptable, repeatable, and effective approach of the Framework helps house proprietors and administrators of critical foundations to oversee cybersecurity-related hazards. The shown image represents the objectives of the Cybersecurity Framework.

6.1 Types of Cybersecurity Framework

1. **PCI DSS (PAYMENT CARD INDUSTRY DATA SECURITY STANDARD)**
   It is a set of security controls required to implement to protect payment account security. It is designed to protect credit card, debit card, and cash card transactions.

2. **ISO 27001/27002 (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION)**
   Best practice recommendations for information security management and information security program elements.

3. **CIS CRITICAL SECURITY CONTROLS**
   A prescribed arrangement of activities for cyber protection that give particular and noteworthy approaches to stop the present most inescapable and perilous attacks. A key advantage of the Controls is that they organize and center fewer activities with high outcomes.

4. **NIST FRAMEWORK**
   A Framework for improving critical infrastructure Cybersecurity with a goal to improve organization's readiness for managing cybersecurity risk by leveraging standard methodologies and processes.

6.2 Components of Cybersecurity Framework

01 Framework Core	02 Implementation tiers	03 Profiles
It gives an arrangement of required Cybersecurity exercises and results utilizing normal understandable language. The Core guides associations in overseeing and decreasing their Cybersecurity chances in a way that supplements an association's current Cybersecurity and risk management processes.	It helps associations setting instructions on how an association should see Cybersecurity risk management. The tiers manage associations to consider the suitable level of thoroughness for their cybersecurity program and are regularly utilized as a specialized device to talk about hazard hunger, mission need, and spending plan.	Profiles are an association's novel arrangement of their organizational prerequisites, goals, and assets against the coveted results of the Framework Core. Profiles are principally used to recognize and organize open doors for enhancing Cybersecurity at an association.

6.3 Cybersecurity Framework's Functions

1. **IDENTIFY**
   The Identify Function helps with building up a hierarchical comprehension in overseeing cybersecurity to frameworks, individuals, resources, information, and capacities.

2. **PROTECT**
   The Protect Function diagrams proper shields to guarantee the conveyance of basic foundation administrations. This underpins the capacity to restrict or contain the effect of a potential Cybersecurity occasion.

3. **DETECT**
   The Detect Function characterizes the fitting exercises to recognize the event of a Cybersecurity occasion. This empowers opportune revelation of Cybersecurity occasions.

4. **RESPOND**
   The Respond Function incorporates proper activities to make a move in regards to a distinguished Cybersecurity occurrence. It bolsters the capacity to contain the effect of a potential Cybersecurity occurrence.

5. **RECOVER**
   The Recover Function distinguishes proper exercises to keep up plans for versatility and to re-establish any abilities or administrations that were impeded because of a Cybersecurity event.

Chapter 7

CYBERSECURITY AND ETHICAL HACKING TOOLS

Threats are constantly evolving and, just like everything else, tend to follow certain trends. The best defenses need to mirror those trends so users get the most robust protection against the newest wave of threats. This chapter lists the Cybersecurity tools that have stood still through thick and thin against various kinds of cyber-attacks. Since there is a multitude of tools spread out across the various domains of Cybersecurity, here we have listed down one tool from each domain.

BEST TOOLS

Chapter 8

CYBER THREATS AND STATE OF OUR DIGITAL PRIVACY

Cybercrime is a global problem that's been dominating the news cycle. It poses a threat to individual security and an even bigger threat to large international companies, banks, and governments. Today's organized cybercrime out shadow lone hackers of the past, now large organized crime rings function like start-ups and often employ highly-trained developers who are constantly innovating online attacks. Cybersecurity is a domain that has stayed in the shadows for most of its lifetime. Only a handful of leading organizations have dedicated teams that preserve their privacy and secure their systems. But, there was never a large-scale global adoption of cybersecurity as a profession or even as an IT domain. Until as recently as 2010, security and privacy of data in organizations was the responsibility of each and every professional working there. Unfortunately, this approach has become outdated in today's fast-paced world where hackers are years ahead when compared to tech professionals.

8.1 Types of Cyber Threats

Chapter 9

FREQUENTLY ASKED INTERVIEW QUESTIONS

Cybersecurity is the only domain in IT that has not faced a recession yet. With the increased demand, there is also competition, and to get a job as **Cybersecurity Professional**, you need to be one of the best. While having the necessary Cybersecurity skills is half job done, cracking the interview is another chapter altogether. To help you crack the Cybersecurity interview, we've compiled this list of top Cybersecurity interview questions.

1. What is Cryptography?
2. What is the difference between Symmetric and Asymmetric Encryption?
3. What is the difference between IDS and IPS?
4. Explain CIA Triad.
5. How is Encryption different from Hashing?
6. What is a Firewall and why is it used?
7. What is the difference between VA(Vulnerability Assessment) and PT(Penetration Testing)?
8. What is a three-way handshake?
9. What are the response codes that can be received from a Web Application?
10. What is a traceroute? Why is it used?
11. What is the difference between HIDS and NIDS?
12. What are the steps to set up a firewall?
13. Explain SSL Encryption.
14. What steps will you take to secure a server?
15. Explain Data Leakage.
16. What are some of the common Cyberattacks?
17. What is a Brute Force Attack? How can you prevent it?
18. What is Port Scanning?
19. What are the different layers of the OSI model?
20. What is a VPN?
21. What do you understand by Risk, Vulnerability & Threat in a network?
22. How can Identity Theft be prevented?
23. What are Black Hat, White Hat and Grey Hat Hackers?
24. How often should you perform Patch management?
25. How would you reset a password-protected BIOS configuration?
26. Explain the MITM attack and how to prevent it?
27. Explain DDOS attack and how to prevent it?
28. Explain XSS attack and how to prevent it?
29. What is an ARP and how does it work?
30. What is port blocking within LAN?
31. What protocols fall under TCP/IP internet layer?
32. What is a Botnet?
33. What are Salted Hashes?
34. Explain SSL and TLS.
35. What is Data Protection in Transit vs Data Protection at rest?

CAREER GUIDANCE

WHO IS A CYBERSECURITY PROFESSIONAL?
Cybersecurity Professional is somebody who is trained to find weaknesses in networks, databases, hardware, firewalls, encryption, etc. Their main priority is to prevent attacks by 'fixing' potential threats before they are exploited by malicious users.

Cybersecurity Specialists

By monitoring, detecting, investigating, analyzing, and responding to security events, **Cybersecurity Specialists** protect systems from cybersecurity risks, threats, and vulnerabilities. Cybersecurity specialists work in IT teams that are dedicated to protecting the integrity of the business's network and data.

Cybersecurity Engineers

Cybersecurity Engineers, sometimes called information security engineers, identify threats and vulnerabilities in systems and software, then apply their skills to developing and implementing high-tech solutions to defend against hacking, malware and ransomware, insider threats and all types of cybercrime.

Cybersecurity Architects

The job of **Cybersecurity Architect** is a senior-level position responsible for planning, designing, testing, implementing and maintaining an organization's computer and network security infrastructure.

Security Administrator

A **Security Administrator** is the point person for a cybersecurity team. They are typically responsible for installing, administering and troubleshooting an organization's security solutions. They also write up security policies and training documents about security procedures for colleagues.

Penetration Testers

A **Penetration Tester**, often known as an IT Pen Tester or Ethical Hacker, is responsible for probing and exploiting any IT security vulnerabilities in a client's IT networks, systems and websites.

EDUREKA CYBERSECURITY PROGRAMS

CYBERSECURITY CERTIFICATION COURSE

Weekend/Weekday | Live Class | 24 x 7 Technical Assistance

www.edureka.co/cybersecurity-certification-training

COMPTIA SECURITY+ TRAINING

Weekend/Weekday | Live Class | 24 x 7 Technical Assistance

www.edureka.co/comptia-security-plus-certification-training

ADVANCED EXECUTIVE PROGRAM IN CYBERSECURITY

Weekend | Live Class/SP | NIT Rourkela | Edureka

www.edureka.co/post-graduate/cybersecurity

LEARNER'S REVIEWS

Abdulaziz ★★★★★

Had great time at Classes. Cybersecurity is such a complicated course. Instrcutor-Fahad is well-resourced and Excellent communication which made the Learning Easier

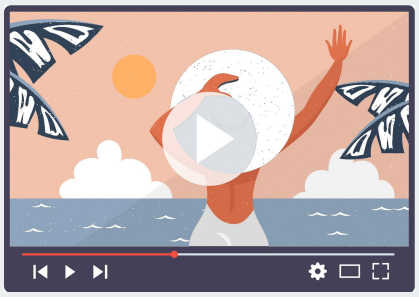
Farhan K ★★★★★

"Edureka aptly named, gives the students a Eureka" Moment during the course. Learning is a world to explore and Edureka provides us with the navigation maps. I never for a minute felt that I am doing this course online away from the faculty and the staff.

Mohan BS ★★★★★

Detailed and extensive course content, Harsha has depth of knowledge of subject with practical experience, explaining the content and demo, also the support team are awesome providing necessary and support as and when needed, definitely recommend to some one, who is looking forward to sharpen skill set.

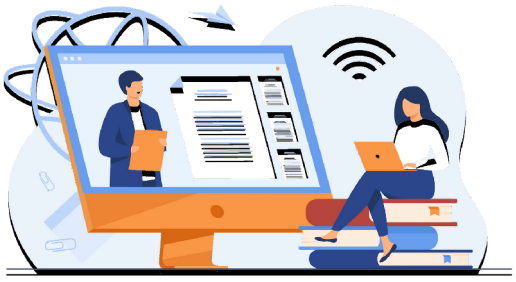
Free Resources



3000+
Video Tutorials on
YouTube

2500+ Technical
Blogs

Active
Community



30+
Free Monthly
Webinars

About Us

There are countless online education marketplaces on the internet. And there's us. We are not the biggest. We are not the cheapest. But we are the fastest growing. We have the highest course completion rate in the industry. We aim to become the largest online learning ecosystem for continuing education, in partnership with corporates and academia. To achieve that we remain ridiculously committed to our students. Be it constant reminders, relentless masters or 24 x 7 online technical support - we will absolutely make sure that you run out of excuses to not complete the course.

Contact Us

IndiQube ETA, 3rd Floor,
No.38/4,
Adjacent to Dell EMC2,
Dodanekundi,
Outer Ring Road, Bengaluru,
Karnataka - 560048

IN: 08035068110 | US: +1415 682 6002
www.instagram.com/edureka.co/
www.facebook.com/edurekaIN
www.linkedin.com/company/edureka/
www.youtube.com/user/edurekaIN
t.me/s/edurekaupdates
twitter.com/edurekaIN
in.pinterest.com/edurekaco/

News & Media

INDIA TODAY

Edureka partners with **NIT Warangal** to upskill IT professionals in **AI and Machine Learning**

Deloitte.

Edureka (Brain4ce Education Solutions) tops Deloitte Tech Fast 50 2014 rankings

edureka!