UNIVERSITY DEPARTMENT, RAJASTHAN TECHNICAL UNIVERSITY, KOTA

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

PRESENTATION ON RECENT TOPICS

DARK AND DEEP WEB

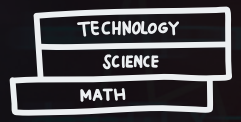
PRESENTED BY

ANISH SONI (21/189)

YATISH JAIN (21/296)

SUBMITTED TO

Dr. Harish Sharma Sir



COMPUTER SCIENCE ENGINEERING

RAJASTHAN TECHNICAL UNIVERSITY

Recent Topics:

DARK AND DEEP WEB

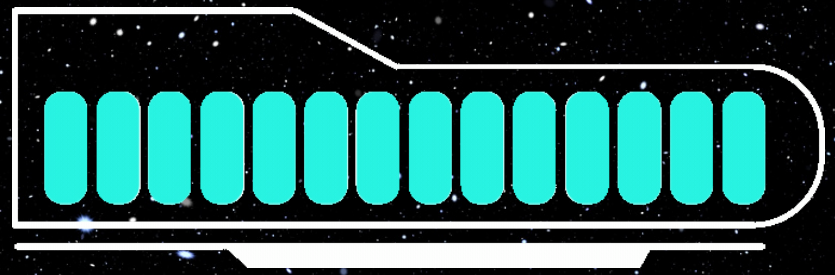
Submitted by

Anish Soni - 21/189
Yatish Jain - 21/296

Submitted to: Dr. Harish Sharma Sir


DARK WEB
EXPLAINED

CONTENTS



LOADING...


SURFACE WEB
EXPLAINED

SITES ON THE SURFACE WEB (OR OPEN WEB) THOSE WHICH ARE VISIBLE TO AN AVERAGE USER WITHOUT THE USE OF TOR OR ANY OTHER SPECIAL BROWSERS OR SOFTWARE.

ALTHOUGH THE SURFACE WEB IS MADE UP OF MANY OF THE MOST POPULAR .COM, .NET, AND .ORG SITES, IT'S ESTIMATED THAT IT REPRESENTS ONLY AROUND 4% OF THE TOTAL CONTENT AVAILABLE ON THE INTERNET, WITH THE REST BEING FOUND ON THE DEEP WEB OR DARK WEB.

EXAMPLE : THE SURFACE WEB CAN BE IMAGINED AS THE TIP OF A LARGE ICEBERG WHOSE BULK REMAINS HIDDEN JUST UNDER THE SURFACE.


DEEP WEB VS DARK WEB
EXPLAINED

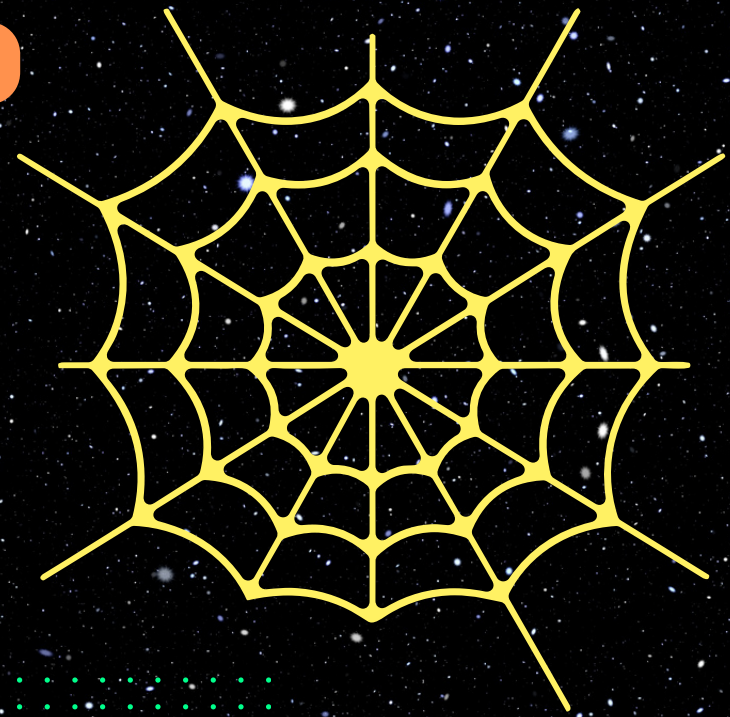
MILLIONS OF REGULAR INTERNET USERS ACCESS PRIVATE DATABASES SUCH AS EMAIL INBOXES AND CREDIT CARD ACCOUNTS DAILY. THESE PAGES ARE NOT INDEXED BY SEARCH ENGINES AND ARE PROTECTED BEHIND SECURITY WALLS, AUTHENTICATION FORMS, AND PASSWORDS ON THE DEEP WEB.

APPROXIMATELY 90% OF ALL WEBSITES ARE ON THE DEEP WEB, AND MANY ARE USED BY ENTITIES SUCH AS CORPORATIONS, GOVERNMENT AGENCIES, AND NON-PROFITS.

DARK WEB EXISTS WITHIN THE DEEP WEB:

IT'S AN AREA OF THE INTERNET THAT IS ONLY ACCESSIBLE BY USERS WHO HAVE BY USERS WHO HAVE A TOR BROWSER INSTALLED. IN GENERAL, MOST AVERAGE INTERNET USERS WILL NEVER NEED TO ACCESS CONTENT ON THE DARK WEB, ALTHOUGH IT IS PERFECTLY LEGAL TO USE TOR.

WHEN & WHY THE DARK WEB ?



THE DARK WEB IS KNOWN TO HAVE BEGUN IN 2000 WITH THE RELEASE OF FREENET.

THE THESIS PROJECT OF UNIVERSITY OF EDINBURGH STUDENT IAN CLARKE, WHO SET OUT TO CREATE A "DISTRIBUTED DECENTRALISED INFORMATION STORAGE AND RETRIEVAL SYSTEM."

CLARKE AIMED TO CREATE A NEW WAY TO ANONYMOUSLY COMMUNICATE AND SHARE FILES ONLINE. THAT GROUNDWORK WAS THE BASIS FOR THE TOR PROJECT, WHICH WAS RELEASED IN 2002 AND LAUNCHED A BROWSER IN 2008.

WITH THE CREATION OF TOR, USERS COULD NOW BROWSE THE INTERNET COMPLETELY ANONYMOUSLY AND EXPLORE SITES THAT WERE DEEMED PART OF THE "DARK WEB."

HOW DOES THE DARK WEB WORK?

ORIGINALLY USED BY THE UNITED STATES DEPARTMENT OF DEFENCE TO COMMUNICATE ANONYMOUSLY, THE DARK WEB HAS NOW BECOME A HUB FOR USERS WISHING TO REMAIN ANONYMOUS AROUND THE WORLD.

PEOPLE USE THE DARK WEB FOR BOTH LEGAL AND ILLEGAL PURPOSES.

IT USES A TECHNOLOGY CALLED "ONION ROUTING," WHICH PROTECTS USERS FROM SURVEILLANCE AND TRACKING THROUGH A RANDOM PATH OF ENCRYPTED SERVERS.

WHEN USERS ACCESS A SITE THROUGH TOR, THEIR INFORMATION IS ROUTED THROUGH THOUSANDS OF RELAY POINTS THAT COVER THE USER'S TRACKS AND MAKE THEIR BROWSING VIRTUALLY IMPOSSIBLE TO TRACE.

LEGAL

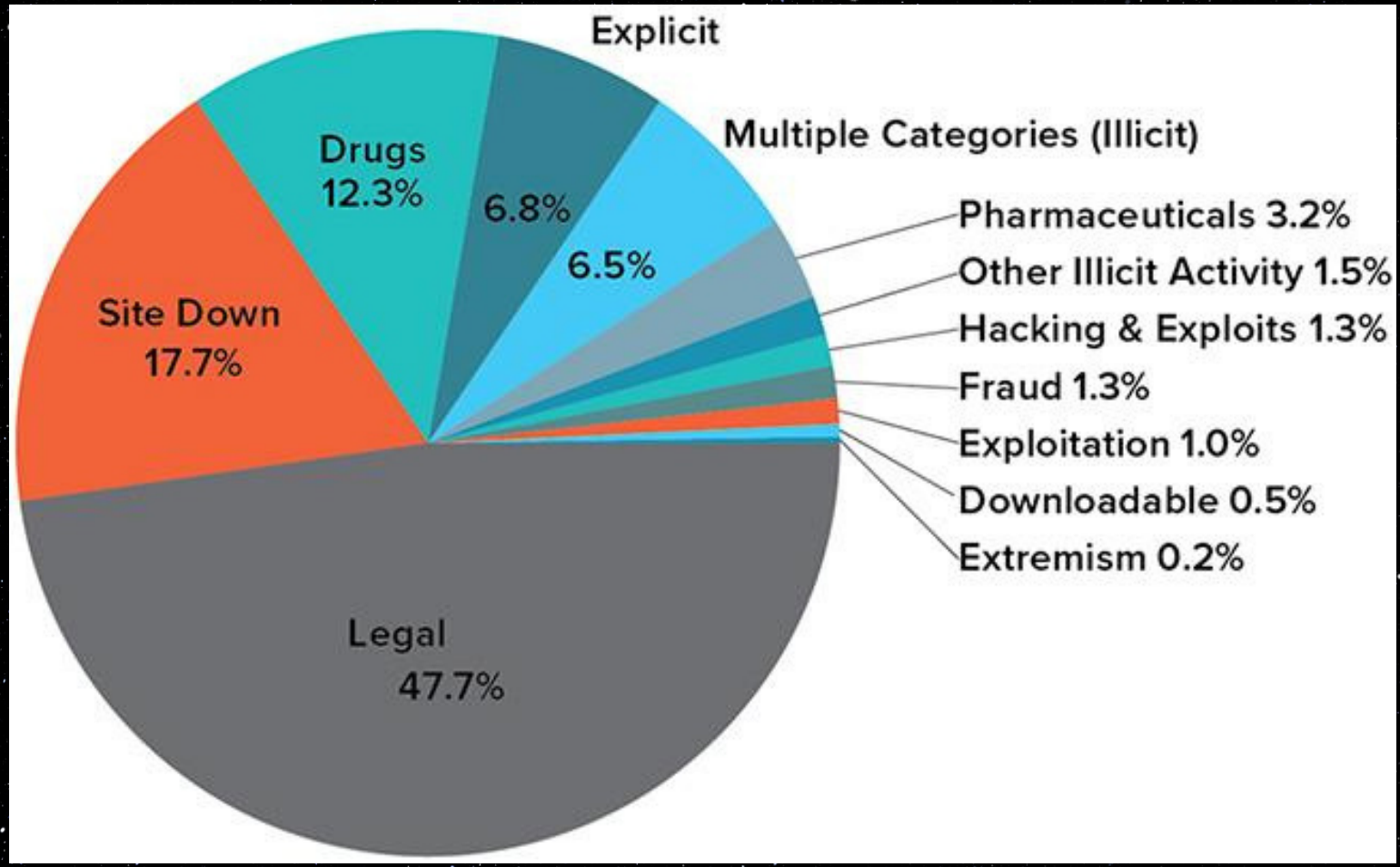
USES OF DARK WEB

WHILE USING THE DARK WEB MAY SEEM SUSPECT ON THE SURFACE, IT IS PERFECTLY LEGAL, AND THERE ARE MANY LEGITIMATE USES OF TOR AND ANONYMOUS BROWSING.

1. GOVERNMENT SURVEILLANCE
2. ANONYMOUS COLLABORATION WITH JOURNALISTS
3. CONTACT THE CIA ANONYMOUSLY
4. SECURE YOUR CRYPTOCURRENCY WALLETS
5. PARTICIPATE IN FORUMS AND CHAT BOARDS, ETC.

DESPITE THESE ADDED LAYERS OF SECURITY, USERS SHOULD STILL BE CAUTIOUS USING THE DARK WEB AND TAKE PROPER SECURITY MEASURES, SUCH AS PERIODICALLY UPDATING THEIR SECURITY SOFTWARE, BROWSING WITH A ROBUST VPN, AND AVOIDING THE USE OF A STANDARD EMAIL ADDRESS.

CATEGORICAL USES



HOW CYBER SECURITY PROFESSIONALS NAVIGATE THE DARK WEB

FOR CYBER SECURITY PERSONNEL, ESPECIALLY THOSE WHO DEAL DIRECTLY WITH PROTECTING SENSITIVE SYSTEMS AGAINST CYBER ATTACKS, AND UNDERSTANDING THE DARK WEB CAN HELP THEM STUDY THE WAYS OF THE ENEMY, SO TO SPEAK-

AI ALGORITHMS CAN SCOUR THE ONION SITES IN SEARCH OF USABLE DATA WHILE SKILLED CYBER SECURITY RESEARCHERS INJECT THEMSELVES INTO THE REALM OF HACKERS AND LEARN FROM THEIR OPPONENTS' DARK WEB ACTIVITIES.

THOSE WHO WORK IN THE CYBERSECURITY INDUSTRY TODAY ARE ENTERING A FIELD WHERE LIFELONG LEARNING PRACTICES ARE VALUABLE. CYBERCRIMINALS MOVE FAST AND INNOVATE NEW HACKS DAILY.

THROUGH THE DARK WEB, HOWEVER, CYBER SECURITY PROFESSIONALS CAN RESEARCH THEIR WAYS AND LEARN HOW TO COUNTER THEIR MOVES BEFORE THEY CAN LAUNCH THEIR ATTACKS.

ALGORITHMS USED FOR SECURITY IN DARK WEB

THE ‘DARK WEB’ USES A COMPLEX SYSTEM THAT ANONYMOUS THE USER’S TRUE IP ADDRESS, MAKING IT VERY DIFFICULT TO WORK OUT WHICH WEBSITE A DEVICE HAS VISITED. IT IS GENERALLY ACCESSED USING DEDICATED SOFTWARE. THE BEST KNOWN IS CALLED TOR (THE ONION ROUTER). AROUND 2.5 MILLION PEOPLE USE TOR EVERY DAY.

THERE ARE BASICALLY TWO TYPES OF ALGORITHMS USED FOR SECURITY PURPOSES:

SECURE SOCKET LAYER (SSL)

ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

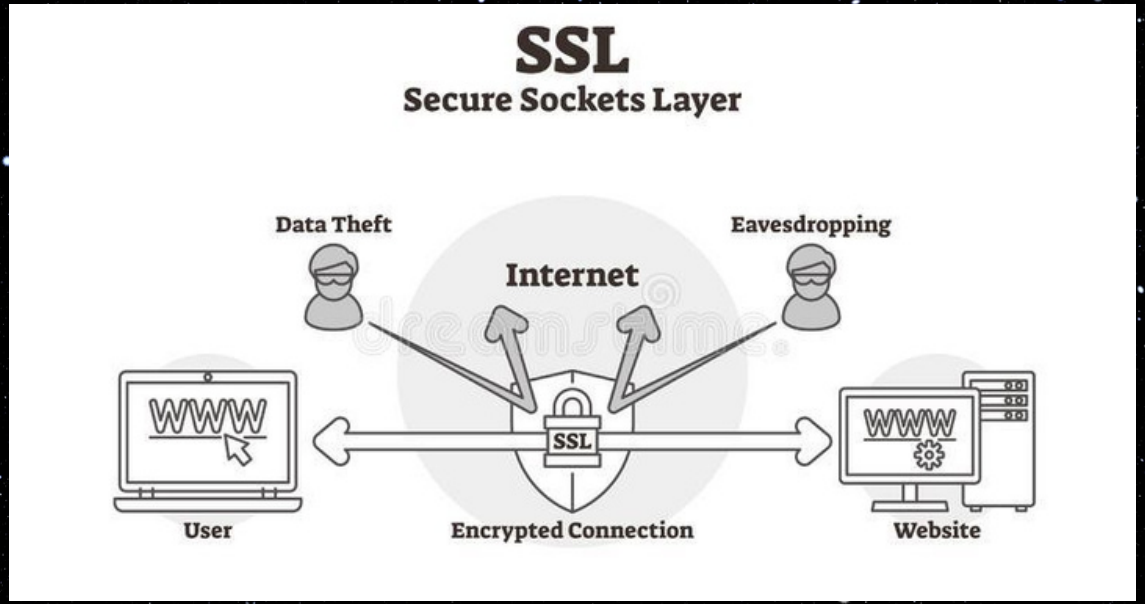
SECURE SOCKET LAYER

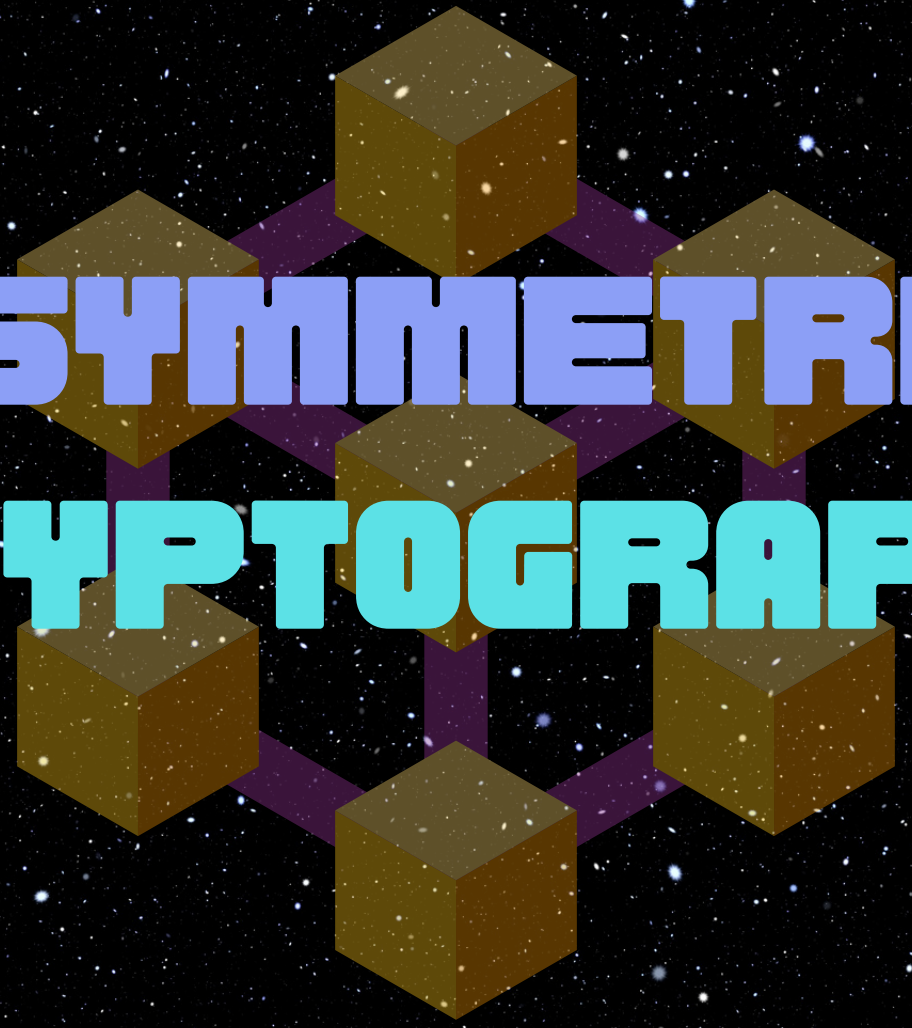
SSL ALGORITHM IS A MACHINE LEARNING ALGORITHM THAT IS USED FOR **DARK WEB** STRUCTURE DATA CLASSIFICATION.

SECURE SOCKET LAYER (SSL)PROVIDES SECURITY TO THE DATA THAT IS TRANSFERRED BETWEEN WEB BROWSER AND SERVER. IT ENCRYPTS THE LINK BETWEEN A WEB SERVER AND A BROWSER WHICH ENSURES THAT ALL DATA PASSED BETWEEN THEM REMAINS PRIVATE AND FREE FROM ATTACK.

SECURE SOCKET LAYER PROTOCOLS:

- SSL RECORDS PROTOCOL
- HANDSHAKE PROTOCOL
- CHANGE-CIPHER SPEC PROTOCOL
- ALERT PROTOCOL





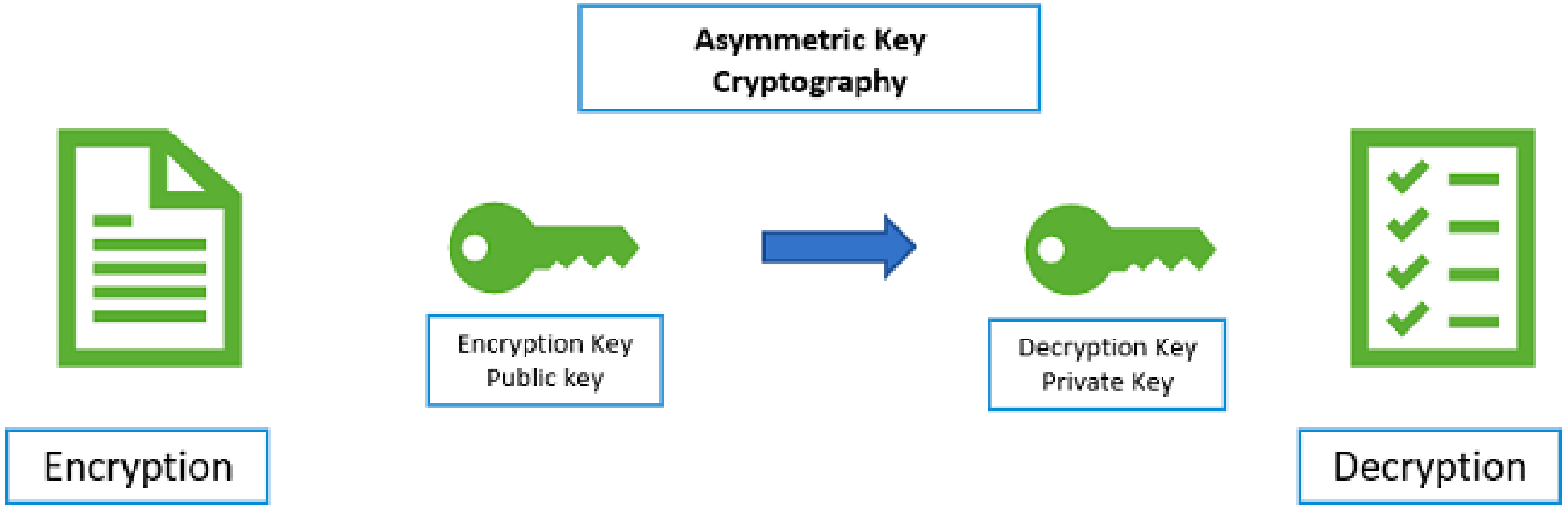
ASYMMETRIC CRYPTOGRAPHY

ASYMMETRIC CRYPTOGRAPHY (ALSO KNOWN AS ASYMMETRIC ENCRYPTION OR PUBLIC KEY CRYPTOGRAPHY) USES A MATHEMATICALLY-RELATED KEY PAIR TO ENCRYPT AND DECRYPT DATA.

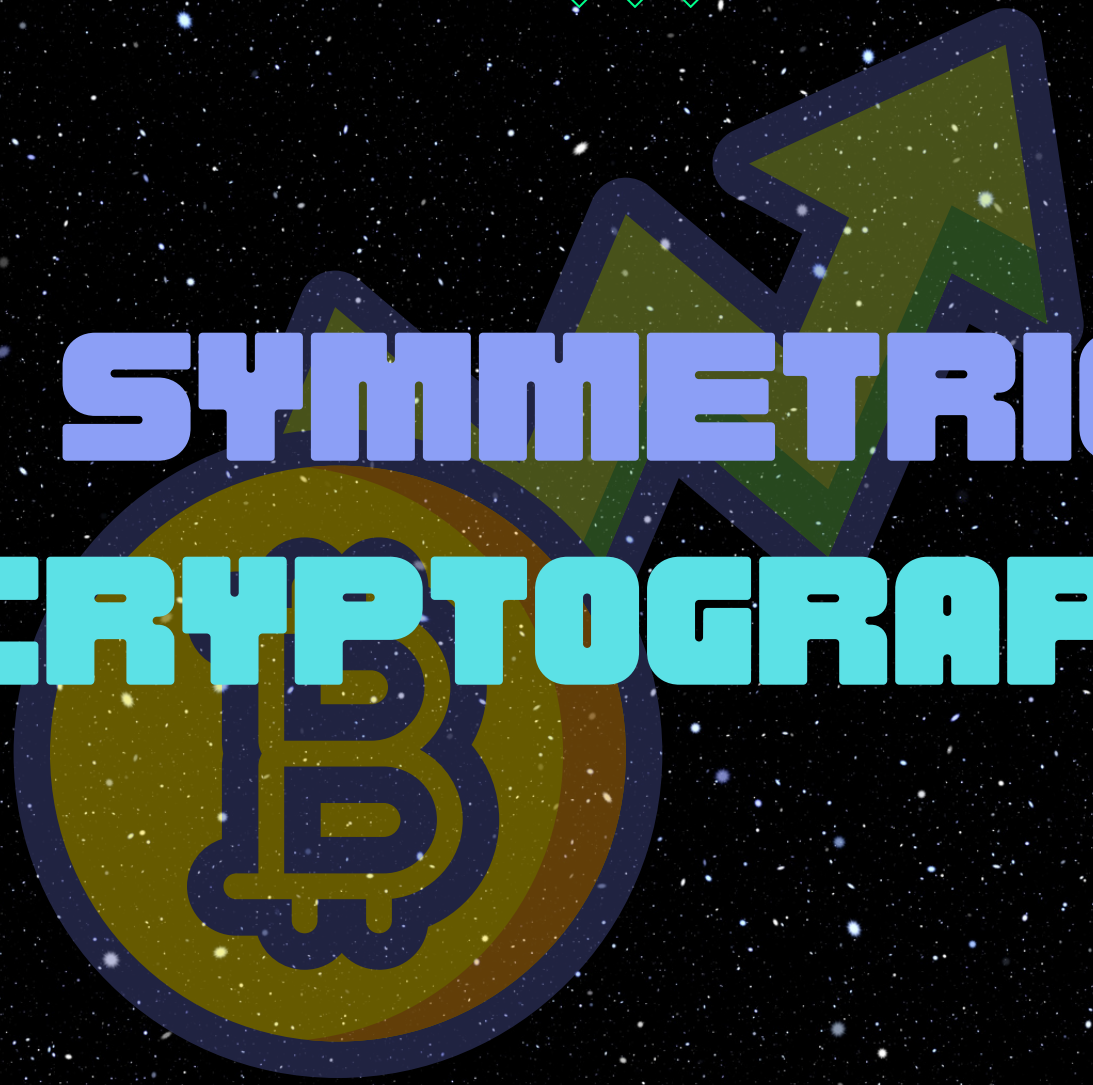
IN A KEY PAIR, ONE KEY IS SHARED WITH ANYONE INTERESTED IN COMMUNICATION. THIS IS CALLED PUBLIC KEY.

THE OTHER KEY IN THE KEY PAIR IS KEPT SECRET AND IS CALLED PRIVATE KEY.

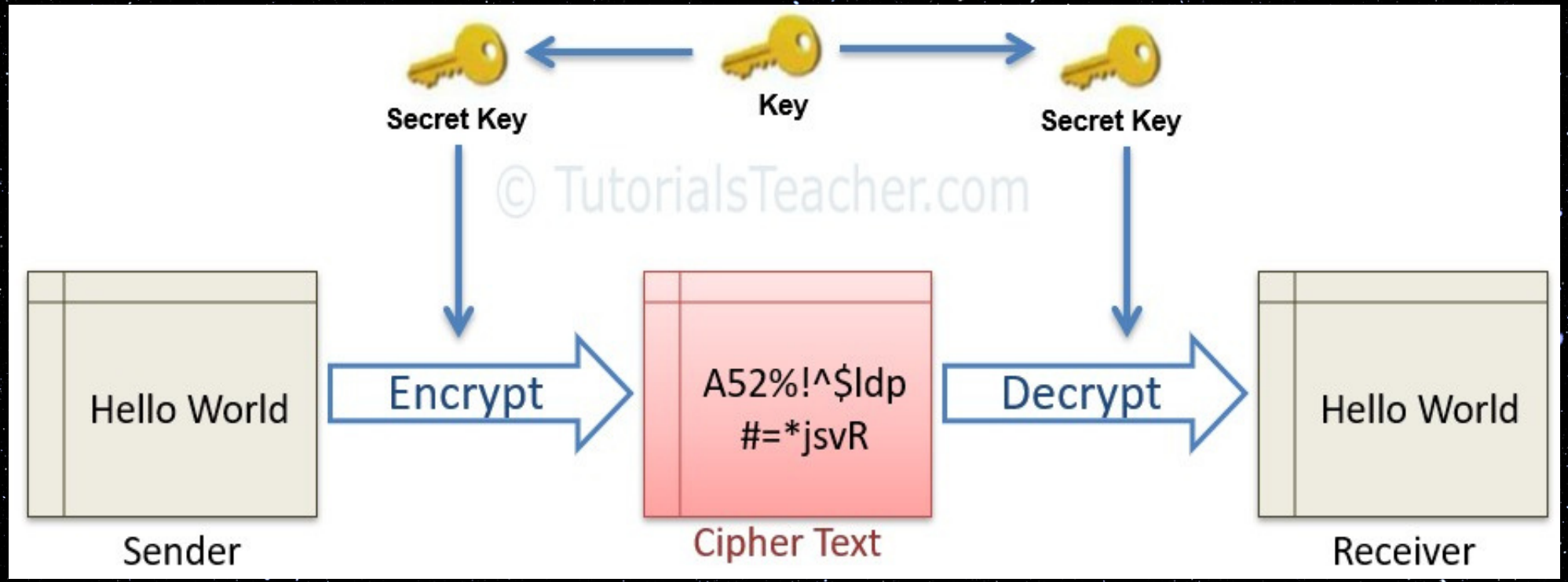
THESE ARE CREATED USING CRYPTOGRAPHIC ALGORITHMS, WHICH ARE BASED ON MATHEMATICAL PROBLEMS TERMED ONE-WAY FUNCTIONS. THESE KEYS ARE USED TO ENCRYPT OR DECRYPT THE DATA.


Asymmetric Key
Cryptography
Encryption Key
Public key
Decryption Key
Private Key
Encryption
Decryption

SYMMETRIC CRYPTOGRAPHY

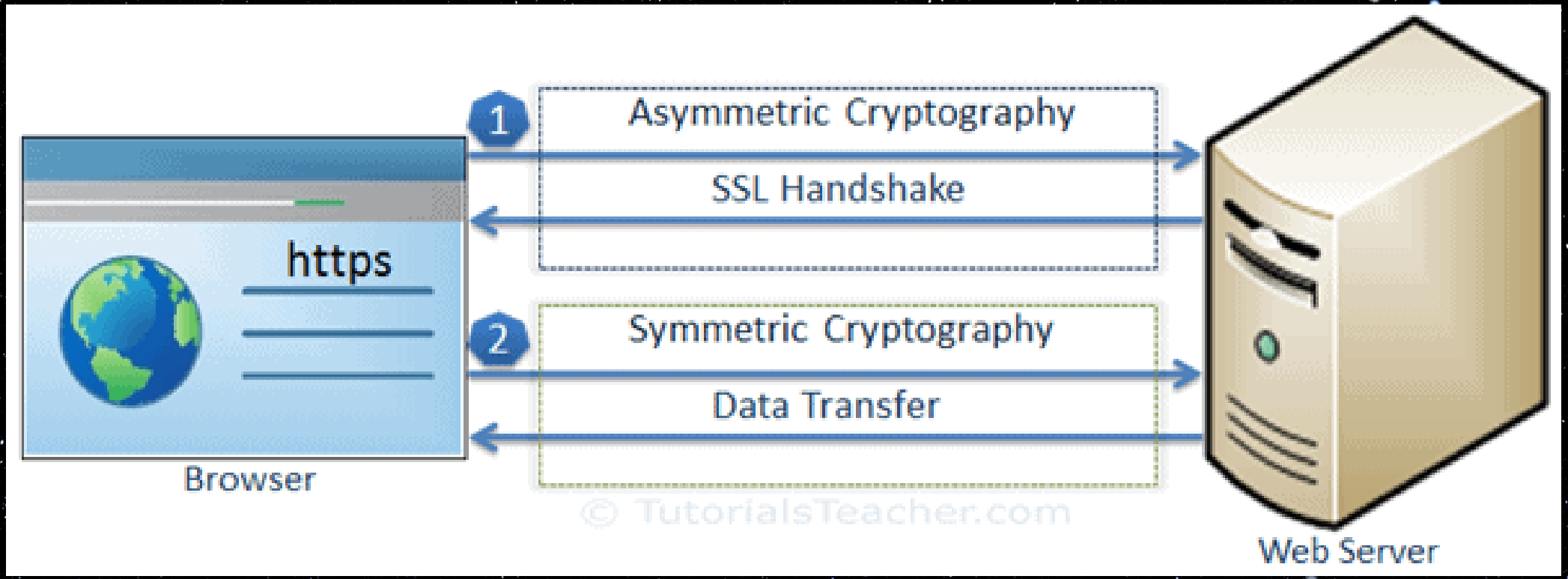


In **symmetric cryptography**, there is only one key that encrypts and decrypts the data. Both sender and receiver should have this key, which is only known to them.



DATA TRANSFER USING SSL

SSL protocol uses asymmetric and symmetric cryptography to transfer data securely. The following figure illustrates the steps of SSL communication:

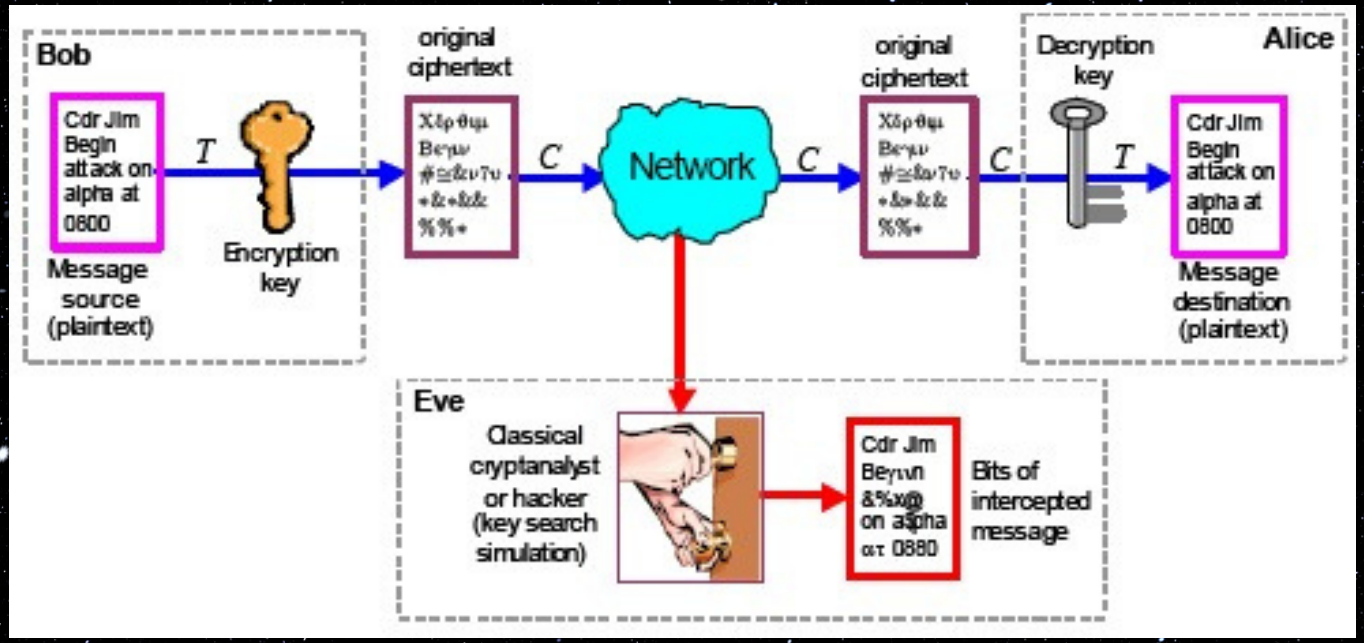


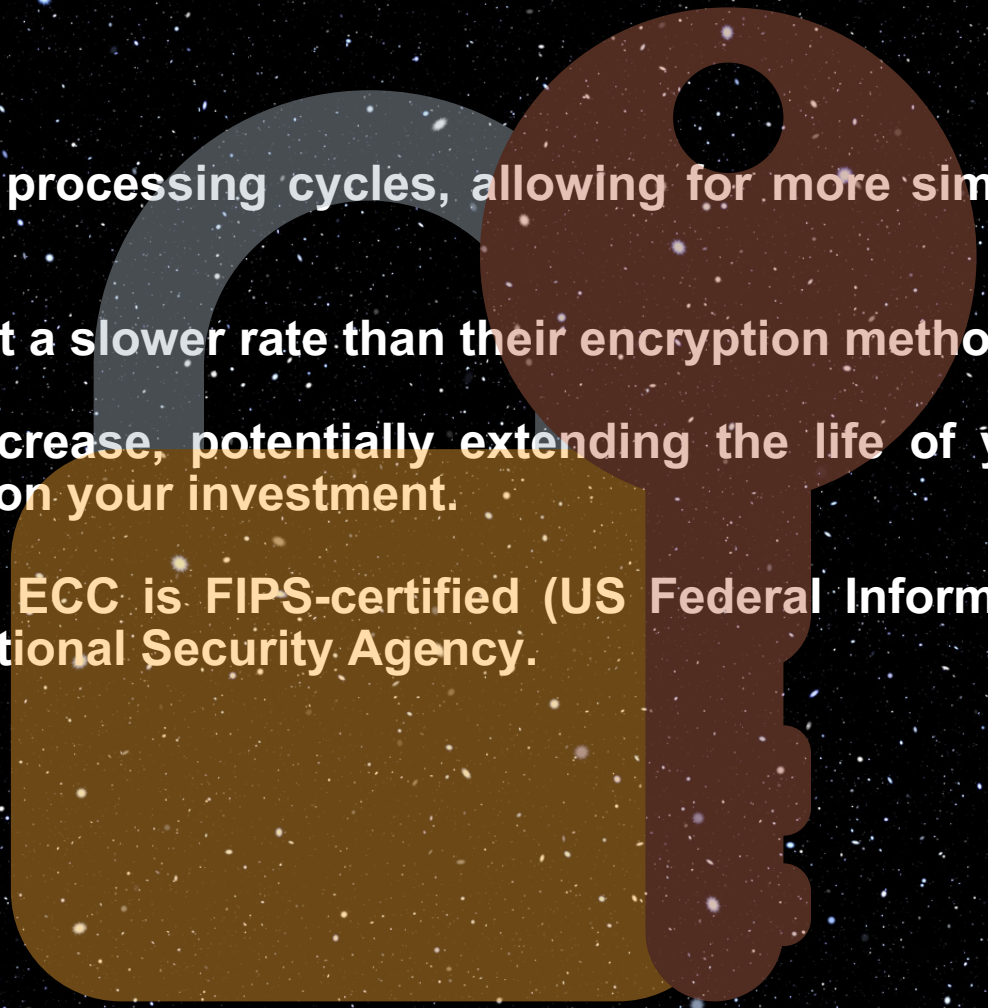
ELLIPTIC CURVE CRYPTOGRAPHY (ECC) ALGORITHM

ECC provides stronger security and increased performance:

it offers better protection than currently adopted encryption methods but uses shorter key lengths (e.g., **256-bit** ECC key provides the same level of **security** as a 3,072 RSA key).

The result: **Stronger security** that can handle the explosion in mobile device and tablet connections.





This requires fewer server processing cycles, allowing for more simultaneous SSL connections and faster processing.

ECC key lengths increase at a slower rate than their encryption methods.

Keys as security levels increase, potentially extending the life of your existing hardware and giving you a greater return on your investment.

US Government approved: ECC is FIPS-certified (US Federal Information Processing Standard) and endorsed by the US National Security Agency.

LAYERS OF DARK WEB


DEEP — DEEPER — DEEPEST

Level 1 —Surface Web: 4% of the total Internet. The internet we normally use.

Level 2 — Bergie Web: Can be accessed through the Tor browser. Basically, there are those websites or data which we can not access on the surface. It is not that difficult to browse on Bergieweb.

Level 3 —Deep Web: Difficult to access and dangerous to browse. Hacking takes place in this layer.

Level 4 and Level 5 — Charter Web: It has two parts –Upper and Lower Charter, and all the illegal activities take place in this layer.

Level 6 and Level 7 –The Fog / Virus Soup: If accessed, all information about the user can be leaked.

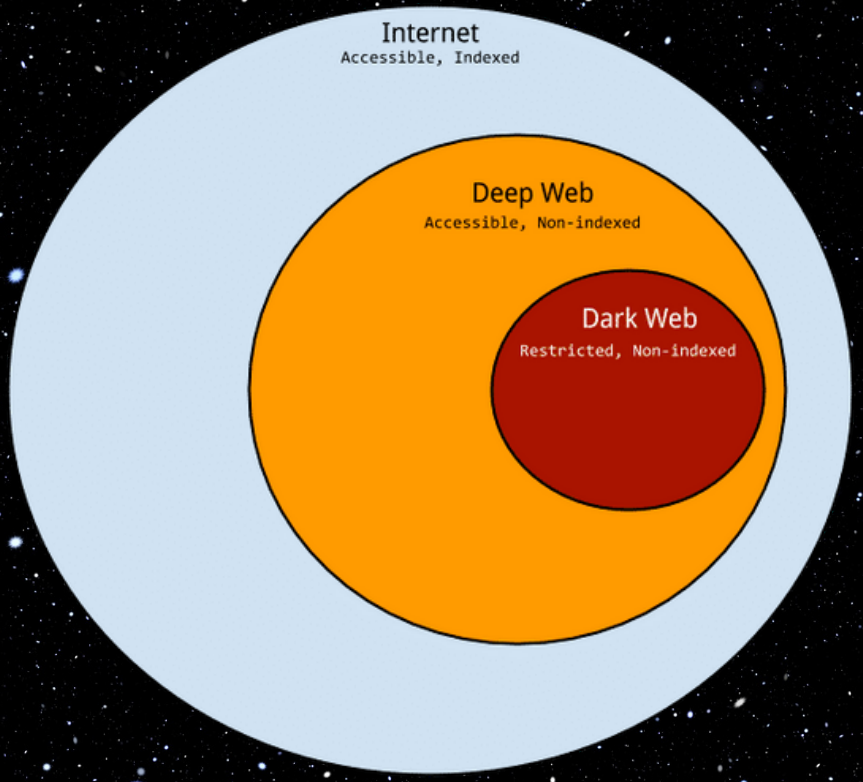
Level 8 —The Primarch System: This level is where government and every big organization operate to share information, where all the data is secured and prevents hacking.

Level 9 — Marianas Web: Nobody has ever accessed the Marianas Web. It’s a total mystery, and it is said that the most secret information about humankind is hidden in Mariana's Web.

CONCLUSION

The whole reason for the dark web is to provide **security**.

So, if we can use that type of security and encryption in the Surface Web; it would be best for the user as the data and information will not be cracked, and it will be secured.



GIVE A MAN A MASK

AND HE WILL SHOW YOU HIS TRUE FACE


THANK YOU

QUESTIONS

2 marks :

Question 1: What is the primary purpose of using specialized software like Tor to access the dark web?

Answer: The primary purpose of using specialized software like Tor to access the dark web is to ensure anonymity and privacy for users. Tor routes internet traffic through a series of encrypted nodes, concealing the user's IP address and making it difficult to trace their online activities.

Question 2: How are websites on the dark web different from traditional websites on the surface web?

Answer: Websites on the dark web use ".onion" domains and can only be accessed through the Tor network. They are intentionally hidden and require special software for access. In contrast, traditional websites on the surface web can be accessed using regular web browsers and search engines.

Question 3 : What is the concept of "onion routing" in the context of the Tor network?
Answer: "Onion routing" is a technique used by the Tor network to anonymize internet traffic. Data is encrypted in layers and routed through a series of nodes. At each node, one layer of encryption is decrypted, revealing the next routing instruction. This process helps in obfuscating the source and destination of the data.

Question 4: Why might individuals in countries with strict internet censorship turn to the dark web?
Answer: Individuals in countries with strict internet censorship might turn to the dark web as a means to access information and communicate freely without the risk of government surveillance or censorship. The anonymity provided by the Tor network enables them to bypass restrictions and access content that is otherwise blocked.

Question 5: What role does encryption play in ensuring privacy on the dark web?
Answer: Encryption plays a crucial role in ensuring privacy on the dark web. Data is encrypted at multiple layers as it passes through the Tor network, making it difficult for anyone to intercept and decipher the information being transmitted. Encryption enhances user anonymity and secures their communication within the network.

5 marks :

Question 1: Explain the concept of the dark web and its relationship with the deep web. How does it differ from the surface web, and what are the key characteristics that define the dark web?

Answer : The dark web is a subset of the deep web, which comprises internet content not indexed by traditional search engines. While the deep web includes password-protected sites, databases, and other non-public content, the dark web is a deliberately hidden part accessed using specialized software like Tor (The Onion Router). It's characterized by its anonymity and the use of ".onion" domains.

Distinguishing it from the surface web, the dark web is intentionally concealed, requires specific software for access, and facilitates anonymous browsing. It's a hub for a wide range of activities, both legal and illegal. Anonymity is its cornerstone; users and website operators remain hidden through layers of encryption, making it challenging to trace their identities or activities.

The dark web is known for hosting markets for illegal goods, forums, and whistleblower platforms. However, it also serves as a refuge for privacy-conscious individuals, activists, and those living in regions with internet censorship.

Question 2: Discuss the technology behind the Tor network and how it ensures user anonymity when accessing the dark web.

Answer : The Tor network, short for "The Onion Router," is instrumental in providing anonymity for users accessing the dark web. It operates through a series of volunteer-operated nodes or relays, which encrypt and route internet traffic in a way that makes it exceedingly challenging to trace the origin of the data.

When a user accesses the Tor network, their data is encrypted in layers, much like the layers of an onion. This multi-layered encryption serves to conceal the source and destination of the data. The data is then routed through several nodes, each of which decrypts one layer, revealing the next node in the chain but no information about the original source.

The use of Tor ensures that users' IP addresses remain hidden, making it difficult for anyone to determine who is accessing the dark web or what they are doing. This anonymity is the cornerstone of the network and is crucial in protecting user privacy.

Question 3: What are the ethical and legal implications of accessing the dark web? How do individuals navigate the fine line between using it for legitimate purposes and engaging in illegal activities?

Answer : Accessing the dark web carries significant ethical and legal considerations. Ethically, individuals need to weigh the potential harm they may contribute to by engaging in illegal activities against the legitimate reasons for using the dark web.

Legally, the dark web is monitored by law enforcement agencies globally due to its association with illegal activities like drug trafficking, cybercrime, and the sale of stolen data. Individuals who engage in such activities may face criminal charges, imprisonment, and severe legal consequences.

To navigate this ethical and legal minefield, users must exercise caution and adhere to the law. Using the dark web for legitimate purposes, such as protecting privacy, accessing uncensored information, or promoting free speech, is acceptable. However, it's essential to avoid involvement in illegal activities or supporting them in any way.

10 marks :

Question 1: Discuss the challenges and strategies associated with investigating and combating criminal activities on the dark web. How do law enforcement agencies and cybersecurity experts navigate the complexities of this hidden online world?

Answer: Investigating and combating criminal activities on the dark web presents unique challenges due to its inherent anonymity and encryption. Law enforcement agencies and cybersecurity experts must employ specialized strategies to navigate this complex online landscape effectively.

Challenges:

1. **Anonymity:** Dark web users and website operators remain hidden behind layers of encryption and the Tor network, making it challenging to trace their identities and locations.
2. **Encryption:** Data transmitted on the dark web is encrypted, making it difficult to intercept and decipher communications.
3. **Jurisdiction:** The international nature of the dark web complicates jurisdictional issues, as illegal activities may span multiple countries.
4. **Rapid Evolution:** Criminals continually adapt to law enforcement efforts, necessitating ongoing adaptation of investigative methods.

Strategies:

1. **Undercover Operations:** Law enforcement agencies conduct undercover operations to infiltrate dark web marketplaces and forums, gathering evidence and identifying key individuals.
2. **Data Analysis:** Experts analyze data leaks, cryptocurrency transactions, and digital footprints to trace illegal activities back to their sourc3
3. **Collaboration:** International cooperation among law enforcement agencies is crucial for addressing cross-border criminal activities on the dark web.
4. **Dark Web Monitoring:** Agencies actively monitor the dark web for emerging threats and trends, enabling proactive responses.
5. **Education and Prevention:** Public awareness campaigns and educational programs aim to reduce the appeal of engaging in criminal activities on the dark web.
6. **Tor Network Vulnerabilities:** Efforts to exploit vulnerabilities in the Tor network can reveal the identities of users involved in illegal activities.
7. **Blockchain Analysis:** For tracking cryptocurrency transactions, blockchain analysis tools help identify financial flows associated with criminal activities.
8. **Legislation and Regulation:** Governments enact legislation to address emerging challenges on the dark web, such as regulating cryptocurrency exchanges.
9. **Cybersecurity Measures:** Implementing advanced cybersecurity measures helps protect individuals and organizations from cyberattacks originating from the dark web.
10. **Infiltration of Criminal Networks:** Law enforcement agencies often work to infiltrate and dismantle criminal networks on the dark web by identifying and arresting key actors.

Question 2: Discuss the ethical and legal implications of using the dark web for activities that fall into the gray area between legitimate and illegal. Provide examples of such activities and explain how individuals might justify their actions in these cases.

Answer: Using the dark web for activities that occupy the gray area between legitimate and illegal presents complex ethical and legal challenges. While the dark web can serve noble purposes, such as protecting privacy or bypassing censorship, it is also a haven for illegal activities like drug trade, cybercrime, and illicit markets.

One common example of a gray area activity on the dark web is the sale of hacking tools or information. Some individuals argue that hacking tools can be used for cybersecurity testing or research, which is a legitimate endeavor. However, these tools are often employed by cybercriminals to commit fraud or cyberattacks.

Another example is the sale of digital goods, such as software licenses or media content. While some might argue that purchasing a discounted software license on the dark web is a way to access expensive software legitimately, the majority of these licenses are pirated or stolen.

The ethical dilemma arises from the dual use of these activities. On one hand, individuals may justify their actions by emphasizing legitimate purposes, such as cybersecurity research or protecting privacy. On the other hand, engaging in activities that can facilitate cybercrime or violate copyright laws is morally and legally questionable.

From a legal standpoint, authorities may view any involvement with the dark web as suspicious, given its association with illegal activities. Users may inadvertently find themselves on the wrong side of the law, even if their intentions were originally ethical. To navigate this gray area, individuals must consider both the intended use of their actions and the potential consequences. While the dark web provides tools and resources for various purposes, users bear a responsibility to ensure that their activities align with ethical and legal standards. Transparency, adherence to laws, and careful consideration of potential harm are essential when operating in this ambiguous space.

In conclusion, the ethical and legal implications of using the dark web for activities in the gray area between legitimate and illegal demand careful thought and consideration. Users must weigh the intended purpose of their actions against potential harm and legality to make informed and responsible decisions.