**ASSESSMENT 28**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | 18-06-2020 | **Name:** | Sheela Golasangi |
| **Course:** | Introduction to Cyber Security | **USN:** | 4AL16EC068 |
| **Topic:** | * Ciphers and encryption * Block chain and cyber security * Relevance | **Semester & Section:** | VIII  ‘B’ |
| **Github Repository:** | Sheela-Course |  |  |

|  |
| --- |
| Forenoon Session Details **Image of the session** C:\Users\india\Pictures\Screenshots\Screenshot (458).pngCipher In cryptology, the discipline concerned with the study of cryptographic algorithms, a cipher is an [algorithm](https://whatis.techtarget.com/definition/algorithm) for encrypting and decrypting data. [Symmetric key encryption](https://searchsecurity.techtarget.com/definition/secret-key-algorithm), also called secret key encryption, depends on the use of ciphers, which operate symmetrically. With symmetric algorithms, the same cipher and encryption [key](https://searchsecurity.techtarget.com/definition/key) are applied to data in the same way, whether the objective is to convert plaintext to ciphertext or ciphertext to plaintext. A cipher transforms data by processing the original, plaintext characters (or other data) into ciphertext, which should appear to be random data.  Traditionally, ciphers used two main types of transformation: transposition ciphers, which keep all the original bits of data in a byte but mix their order, and substitution ciphers, which replace specific data sequences with other specific data sequences. For example, one type of substitution would be to transform all bits with a value of 1 to a value of 0, and vice versa. The data output by either method is called the ciphertext.  Modern ciphers enable private communication in many different networking protocols, including the Transport Layer Security ([TLS](https://searchsecurity.techtarget.com/definition/Transport-Layer-Security-TLS)) protocol and others that offer encryption of network traffic. Many communication technologies, including phones, digital television and ATMs, rely on ciphers to maintain security and privacy. How ciphers work A cipher uses a system of fixed rules -- an algorithm -- to transform plaintext, a legible message, into ciphertext, an apparently random string of characters. Ciphers can be designed to encrypt or decrypt bits in a stream ([stream ciphers](https://searchsecurity.techtarget.com/definition/stream-cipher)), or they can process ciphertext in uniform blocks of a specified number of bits ([block ciphers](https://searchsecurity.techtarget.com/definition/block-cipher)).  Modern cipher implementations depend on the cipher algorithm and a secret key, which is used by the cipher algorithm to modify data as it is encrypted. Ciphers that use longer keys, measured in bits, can be more secure from [brute-force attacks](https://searchsecurity.techtarget.com/definition/brute-force-cracking), because the longer the key length, the more brute-force attempts are necessary to expose the plaintext. While cipher strength is not always dependent on the length of the key, experts recommend modern ciphers be configured to use keys of at least 128 bits to 1,024 bits or more, depending on the algorithm and the use case.  A key is an essential part of a cipher algorithm -- so much so that, in real-world ciphering, the key is kept secret, not the algorithm. Strong ciphers are designed so that, even if someone knows the algorithm, it should be virtually impossible to decipher a ciphertext without knowing the appropriate key. Consequently, before a cipher can work, both the sender and receiver must have a key or set of keys.  **What is Encryption? A Non-Technical Overview** Encryption is a means of encoding data such as words, numbers, and images, using mathematical algorithms in order to make that data undecipherable to unauthorized viewers. Over the past several decades encryption has evolved and changed to meet the demands of evolving technology. Today the encryption algorithm accepted as the highest standard is the Advanced Encryption Standard (AES). AES is a formal encryption method adopted by the National Institute of Standards and Technology (NIST) of the US Government, and is accepted worldwide.In the process of encrypting data, an encryption key is created that allows users to encrypt and decrypt the data when it needs to be accessed. The encryption key must be protected in order to prevent access to the data from malicious or unauthorized users. Encryption key management is essential to a successful encryption solution, and it is often required or strongly recommended by most industry regulations.  **Blockchain Context**: Blockchains (or distributed ledger technology) evolution has been compared to the early rising of the internet with comments and arguments of the technology’s potential to disrupt multiple industries including Healthcare, Public Sector, Energy, Manufacturing and particularly Financial Services, where it is predicted to be the beating heart of finance and the ultimate provider of a new industry fabric. According to David Schatsky, Managing Director at Deloitte U.S., “the technology provides a way of recording transactions or any digital interaction in a way that is secure, transparent, highly resistant to outages, auditable, and efficient” . Such is the interest in the technology that in 2016 alone over $1.billion was invested in blockchain by financial services and technology firms globally & such investments are predicted to increase exponentially over the next five years. According to a 2016 Gartner report, the technology is at the peak of a hype cycle5 and it has become a priority for industry leaders to understand how it can transform their Introduction Blockchain is gaining traction today, but critics who question the scalability, security, and sustainability of the technology remain. Deloitte member firms across the globe are continuing to collaborate to build blockchain capabilities to develop world class solutions and services for clients. Blockchain&Cybersecurity Point of View 4 business models and alter value chains to gain competitive advantage and perhaps more fundamentally to remain relevant. However, today the technology remains at the peak of inflated expectation and is about to dive down into the trough of disillusionment. Milan Sallaba, Deloitte Germany’s Technology-Sector Leader points out “some of the early use cases we have seen were deploying blockchain for the sake of it, without sufficiently focusing on the core attributes of the technology, which indeed has the potential to generate substantial process efficiencies across many industries and is likely to contribute to entirely new business models.” For this reason the blockchain industry is now moving beyond proof of concepts to production pilots with business cases being built to identify just how beneficial the technology is. A fundamental component of such reviews is a focus on security and privacy which must be addressed and tested if this technology is to become the real catalyst for social and industrial change that so many think it can be.  **Cyber Security Context**:The high level of dependency on technology and the internet today has resulted in new business models and revenue streams for organizations but with this comes new gaps and opportunities for cyber attackers to exploit. Cyber-attacks have become increasingly targeted and complex due to more sophisticated pieces of malware being leveraged and the increasing threat of professional cyber organizations. These cyber criminals are attempting to steal valuable data, such as intellectual property (IP), personal identifiable information (PII), health records, financial data, and are resorting to highly profitable strategies such as \ monetizing data access through the use of advanced ransomware techniques or by disrupting overall business operations through Distributed Denial of Service (DDoS) attacks . In October 2016, one of the biggest domain name service (DNS) providers Dyn experienced a major distributed denial of service (DDoS) attack that disrupted the service of several high traffic websites such as Twitter, Netflix, and Spotify. Deloitte’s cyber risk professionals suggest organizations follow the secure, vigilant and resilient approach when managing cyber regardless of the type of technology adopted. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | 18-06-2020 | **Name:** | Sheela Golasangi |
| **Course:** | Introduction to Ethical Hacking | **USN:** | 4AL16EC068 |
| **Topic:** | * What is Ethical hacking? * Why is it a necessary skill? * Domains and process implementation under ethical hacking * Ethical hacking in web applications – Demonstration | **Semester & Section:** | VIII  ‘B’ |
| **Github Repository:** | Sheela-Course |  |  |

|  |
| --- |
| Image of the sessionWhat is Ethical Hacking? Ethical Hacking is an authorized practice of bypassing system security to identify potential data breaches and threats in a network. The company that owns the system or network allows [Cyber Security experts](https://www.simplilearn.com/cyber-security-expert-master-program-training-course) to perform such activities in order to test the system’s defenses. Thus, unlike malicious hacking, this process is planned, approved, and more importantly, legal.  [Ethical hackers](https://www.simplilearn.com/roles-of-ethical-hacker-article) aim to investigate the system or network for weak points that malicious hackers can exploit or destroy. They collect and analyze the information to figure out ways to strengthen the security of the system/network/applications. By doing so,  they can improve the security footprint so that it can better withstand attacks or divert them.  **Ethical Hackers check for key vulnerabilities include but are not limited to:**   * Injection attacks * Changes in security settings * Exposure of sensitive data * Breach in authentication protocols * Components used in the system or network that may be used as access points    Types of Hackers The practice of ethical hacking is called “**White Hat”** hacking, and those who perform it are called White Hat hackers. In contrast to Ethical Hacking**, “Black Hat**” hacking describes practices involving security violations. The [Black Hat hackers use illegal techniques](https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html) to compromise the system or destroy information.  Unlike White Hat hackers, “**Grey Hat”** hackers don’t ask for permission before getting into your system. But Grey Hats are also different from Black Hats because they don’t perform hacking for any personal or third-party benefit. These hackers do not have any malicious intention and hack systems for fun or various other reasons, usually informing the owner about any threats they find. Grey Hat and Black Hat hacking are both illegal as they both constitute an unauthorized system breach, even though the intentions of both types of hackers differ.  **Roles and Responsibilities of an Ethical Hacker**  Ethical Hackers must follow certain guidelines in order to perform hacking legally. A good hacker knows his or her responsibility and adheres to all of the ethical guidelines. Here are the most important rules of Ethical Hacking:   * An ethical hacker must seek authorization from the organization that owns the system. Hackers should obtain complete approval before performing any security assessment on the system or network. * Determine the scope of their assessment and make known their plan to the organization. * Report any security breaches and vulnerabilities found in the system or network. * Keep their discoveries confidential. As their purpose is to secure the system or network, ethical hackers should agree to and respect their non-disclosure agreement. * Erase all traces of the hack after checking the system for any vulnerability. It prevents malicious hackers from entering the system through the identified loopholes.     **Skills Required to Become an Ethical Hacker**  An ethical hacker should have in-depth knowledge about all the systems, networks, program codes, security measures, etc. to perform hacking efficiently. Some of these skills include:   * Knowledge of programming - It is required for security professionals working in the field of application security and Software Development Life Cycle (SDLC). * Scripting knowledge - This is required for professionals dealing with network-based attacks and host-based attacks. * Networking skills - This skill is important because threats mostly originate from networks. You should know about all of the devices present in the network, how they are connected, and how to identify if they are compromised. * Understanding of databases - Attacks are mostly targeted at databases. Knowledge of database management systems such as SQL will help you to effectively inspect operations carried out in databases. * Knowledge of multiple platforms like Windows, Linux, Unix, etc. * The ability to work with different hacking tools available in the market. * Knowledge of search engines and servers. |