**DAILY ASSESSMENT FORMAT**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **18-June-2020** | **Name:** | **Bhuvanesh M** |
| **Course:** | **Introduction to Cyber Security** | **USN:** | **4AL16EC015** |
| **Topic:** | **Ciphers and encryption** | **Semester & Section:** | **8th sem & ‘A’ section** |
| **Github Repository:** | **Bhuvan** |  |  |

|  |
| --- |
| **FORENOON SESSION DETAILS** |
| **Image of session** |
| **Report –**  In my first session today I have studied about - Ciphers and encryption What ciphers are used for Symmetric ciphers are most commonly used to secure online communications and are incorporated into many different network protocols to be used to encrypt exchanges. For example, Secure Sockets Layer (SSL) and TLS use ciphers to encrypt application layer data, especially when used with HTTP Secure ([HTTPS](https://searchsoftwarequality.techtarget.com/definition/HTTPS)).  Virtual private networks (VPNs) that connect remote workers or remote branches into corporate networks use protocols with symmetric ciphers to protect data communications. Symmetric ciphers protect data privacy in most Wi-Fi networks, online banking and e-commerce services, and mobile telephony.  Other protocols, including Secure Shell ([SSH](https://searchsecurity.techtarget.com/definition/Secure-Shell)), OpenPGP and Secure/Multipurpose Internet Mail Extensions (S/MIME), use asymmetric cryptography to encrypt and authenticate endpoints but also for the secure exchange of symmetric keys to encrypt session data. While public key cryptography is considered more secure than symmetric encryption, it is also more computationally intensive. For performance reasons, protocols often rely on ciphers to encrypt session data. Difference between codes and ciphers Codes and ciphers are different ways to encrypt a message. A code is a method of changing a message by replacing each word with another word that has a different meaning.  On the other hand, a cipher converts the message using the cipher's algorithm to transform the data representing the letters and words in the message. Ciphers are easier to implement and use with computers because cipher algorithms are automated and easily programmed. Types of ciphers Ciphers can be characterized in a number of different ways, including:   * Block ciphers encrypt uniformly sized blocks of data, while stream ciphers can be applied to streams of data such as are often received and sent over a network. * Ciphers can depend on traditional keys used directly to key ciphertext or on elliptical curve cryptography ([ECC](https://searchsecurity.techtarget.com/definition/elliptical-curve-cryptography)), which, when used with a 160-bit key, can provide the security of a traditional cipher like that used in the Rivest-Shamir-Adleman (RSA) cryptosystem using a key of 1,024 bits in length.   Modern-day ciphers are designed to be able to withstand attacks even when the attacker knows what cipher is being used; historically, ciphers have been less secure against attack because they needed to be used for ciphering by hand and thus can be more easily analyzed and broken with computer power.   * **Caesar cipher** is one of the simplest and earliest known ciphers; some attribute the use of this cipher to Caesar, who is said to have used it to communicate securely with his generals. The Caesar cipher is a simple type of substitution cipher where each letter in the plaintext is "shifted" a specific number of places down the alphabet; traditionally, the shift number used by Caesar was three. Substitution ciphers, like the Caesar cipher, are often used by writing down the plaintext alphabet, with the ciphertext alphabet written above the plaintext letters, shifted by the number agreed upon by those communicating. A shift of three puts the ciphertext letter D above the plaintext A, E above B and so on. The number of characters shifted is considered a simple form of a key. * **Atbash cipher** is a substitution cipher in which the plaintext alphabet is mapped onto itself, but in reverse order. In other words, the plaintext letter A is mapped to ciphertext Z, B is mapped to Y, C to X and so on. The Atbash cipher is named after the two first and two last letters in the Hebrew alphabet, and it is thought to have been in use for hundreds of years. * **Simple substitution cipher** has also been used for hundreds of years and substitutes every plaintext character for a different ciphertext character, resulting in what is effectively a 26-character key. It differs from the Caesar cipher because the cipher alphabet is the alphabet completely jumbled, rather than simply shifted by a uniform number of places. * **Vigenère cipher** is a form of polyalphabetic substitution, meaning a cipher based on substitution, using multiple substitution alphabets. The Vigenère cipher uses a series of interwoven Caesar ciphers, based on the letters of a keyword. The original text is encrypted using what is known as the Vigenère square or Vigenère table. * **Homophonic substitution cipher** is a substitution cipher in which several different ciphertext letters replace single plaintext letters. This type of cipher is typically much more difficult to break than standard substitution ciphers. |