18 June 2020

|  |  |  |  |
| --- | --- | --- | --- |
| Date: | 18 June 2020 | Name: | Srinidhi J C |
| Course: | **Introduction to Cyber Security** | USN: | 4al16ec078 |
| Topic: | |  | | --- | | Ciphers and encryption | | Block chain and cyber security | | Semester & Section: | 8th & b |
| Github Repository: | SrinidhiJC078 |  |  |
| FORENOON SESSION DETAILS | | | | | |
| Image of session | | | | | |

Report:

In [cryptography](https://en.wikipedia.org/wiki/Cryptography), a **cipher** (or **cypher**) is an [algorithm](https://en.wikipedia.org/wiki/Algorithm) for performing [encryption](https://en.wikipedia.org/wiki/Encryption) or [decryption](https://en.wikipedia.org/wiki/Decryption)—a series of well-defined steps that can be followed as a procedure. An alternative, less common term is *encipherment*. To encipher or encode is to convert information into cipher or code. In common parlance, "cipher" is synonymous with "[code](https://en.wikipedia.org/wiki/Code_(cryptography))", as they are both a set of steps that encrypt a message; however, the concepts are distinct in cryptography, especially [classical cryptography](https://en.wikipedia.org/wiki/Classical_cryptography).

Codes generally substitute different length strings of character in the output, while ciphers generally substitute the same number of characters as are input. There are exceptions and some cipher systems may use slightly more, or fewer, characters when output versus the number that were input.

Codes operated by substituting according to a large [codebook](https://en.wikipedia.org/wiki/Codebook) which linked a random string of characters or numbers to a word or phrase. For example, "UQJHSE" could be the code for "Proceed to the following coordinates." When using a cipher the original information is known as [plaintext](https://en.wikipedia.org/wiki/Plaintext), and the encrypted form as [ciphertext](https://en.wikipedia.org/wiki/Ciphertext). The ciphertext message contains all the information of the plaintext message, but is not in a format readable by a human or computer without the proper mechanism to decrypt it.

The operation of a cipher usually depends on a piece of auxiliary information, called a [key](https://en.wikipedia.org/wiki/Key_(cryptography)) (or, in traditional [NSA](https://en.wikipedia.org/wiki/NSA) parlance, a *cryptovariable*). The encrypting procedure is varied depending on the key, which changes the detailed operation of the algorithm. A key must be selected before using a cipher to encrypt a message. Without knowledge of the key, it should be extremely difficult, if not impossible, to decrypt the resulting ciphertext into readable plaintext.

Most modern ciphers can be categorized in several ways

* By whether they work on blocks of symbols usually of a fixed size ([block ciphers](https://en.wikipedia.org/wiki/Block_cipher)), or on a continuous stream of symbols ([stream ciphers](https://en.wikipedia.org/wiki/Stream_cipher)).
* By whether the same key is used for both encryption and decryption ([symmetric key algorithms](https://en.wikipedia.org/wiki/Symmetric_key_algorithm)), or if a different key is used for each ([asymmetric key algorithms](https://en.wikipedia.org/wiki/Asymmetric_key_algorithm)). If the algorithm is symmetric, the key must be known to the recipient and sender and to no one else. If the algorithm is an asymmetric one, the enciphering key is different from, but closely related to, the deciphering key. If one key cannot be deduced from the other, the asymmetric key algorithm has the public/private key property and one of the keys may be made public without loss of confidentiality.

In [cryptography](https://en.wikipedia.org/wiki/Cryptography), **encryption** is the process of encoding information. This process converts the original representation of the information, known as [plaintext](https://en.wikipedia.org/wiki/Plaintext), into an alternative form known as [ciphertext](https://en.wikipedia.org/wiki/Ciphertext). Only authorized parties can decipher a ciphertext back to plaintext and access the original information. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor. For technical reasons, an encryption scheme usually uses a [pseudo-random](https://en.wikipedia.org/wiki/Pseudo-random) encryption [key](https://en.wikipedia.org/wiki/Key_(cryptography)) generated by an [algorithm](https://en.wikipedia.org/wiki/Algorithm). It is possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users. Historically, various forms of encryption have been used to aid in cryptography. Early encryption techniques were often utilized in military messaging. Since then, new techniques have emerged and become commonplace in all areas of modern computing. Modern encryption schemes utilize the concepts of [public-key](https://en.wikipedia.org/wiki/Public-key_cryptography) and [symmetric-key](https://en.wikipedia.org/wiki/Symmetric-key_algorithm).[[2]](https://en.wikipedia.org/wiki/Encryption#cite_note-:1-2) Modern encryption techniques ensure security because modern computers are inefficient at cracking the encryption.

A **blockchain**,originally **block chain**, is a growing list of [records](https://en.wikipedia.org/wiki/Record_(computer_science)), called *blocks*, that are linked using [cryptography](https://en.wikipedia.org/wiki/Cryptography). Each block contains a [cryptographic hash](https://en.wikipedia.org/wiki/Cryptographic_hash_function) of the previous block, a [timestamp](https://en.wikipedia.org/wiki/Trusted_timestamping), and transaction data (generally represented as a [Merkle tree](https://en.wikipedia.org/wiki/Merkle_tree)).

By design, a blockchain is resistant to modification of the data. It is "an open, [distributed ledger](https://en.wikipedia.org/wiki/Distributed_ledger) that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a [peer-to-peer](https://en.wikipedia.org/wiki/Peer-to-peer) network collectively adhering to a [protocol](https://en.wikipedia.org/wiki/Protocol_(communication)) for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. Although blockchain records are not unalterable, blockchains may be considered [secure by design](https://en.wikipedia.org/wiki/Secure_by_design) and exemplify a distributed computing system with high [Byzantine fault tolerance](https://en.wikipedia.org/wiki/Byzantine_fault_tolerance). [Decentralized](https://en.wikipedia.org/wiki/Decentralized) consensus has therefore been claimed with a blockchain.

Blockchain was invented by a person (or group of people) using the name [Satoshi Nakamoto](https://en.wikipedia.org/wiki/Satoshi_Nakamoto) in 2008 to serve as the public transaction [ledger](https://en.wikipedia.org/wiki/Ledger) of the [cryptocurrency](https://en.wikipedia.org/wiki/Cryptocurrency) [bitcoin](https://en.wikipedia.org/wiki/Bitcoin).[[1]](https://en.wikipedia.org/wiki/Blockchain#cite_note-te20151031-1) The identity of Satoshi Nakamoto remains unknown to date. The invention of the blockchain for bitcoin made it the first digital currency to solve the [double-spending](https://en.wikipedia.org/wiki/Double-spending) problem without the need of a trusted authority or central [server](https://en.wikipedia.org/wiki/Server_(computing)). The bitcoin design has inspired other applications, and blockchains that are readable by the public are widely used by [cryptocurrencies](https://en.wikipedia.org/wiki/Cryptocurrencies). Blockchain is considered a type of [payment rail](https://en.wikipedia.org/wiki/Payment_rail). Private blockchains have been proposed for business use. Sources such as *Computerworld* called the marketing of such blockchains without a proper security model "[snake oil](https://en.wiktionary.org/wiki/snake_oil)".

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date: | 18 June 2020 | Name: | Srinidhi J C | |
| Course: | Ethical Hacking | USN: | 4al16ec078 | |
| 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: | 8th & b | |
| AFTERNOON SESSION DETAILS | | | |
| Image of session  A picture containing bird  Description automatically generatedA screenshot of a cell phone  Description automatically generated | | | |

Report:

# Ethical Hacking Tutorial

Top of Form

Bottom of Form

Hacking has been a part of computing for almost five decades and it is a very broad discipline, which covers a wide range of topics. The first known event of hacking had taken place in 1960 at MIT and at the same time, the term "Hacker" was originated. In this tutorial, we will take you through the various concepts of Ethical Hacking and explain how you can use them in a real-time environment.

Hacking has been a part of computing for almost five decades and it is a very broad discipline, which covers a wide range of topics. The first known event of hacking had taken place in 1960 at MIT and at the same time, the term "Hacker" was originated.

Hacking is the act of finding the possible entry points that exist in a computer system or a computer network and finally entering into them. Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer.

Hacking is usually legal as long as it is being done to find weaknesses in a computer or network system for testing purpose. This sort of hacking is what we call **Ethical Hacking**.

A computer expert who does the act of hacking is called a "Hacker". Hackers are those who seek knowledge, to understand how systems operate, how they are designed, and then attempt to play with these systems.

## Types of Hacking

We can segregate hacking into different categories, based on what is being hacked. Here is a set of examples −

* **Website Hacking** − Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.
* **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.
* **Email Hacking** − It includes getting unauthorized access on an Email account and using it without taking the consent of its owner.
* **Ethical Hacking** − Ethical hacking involves finding weaknesses in a computer or network system for testing purpose and finally getting them fixed.
* **Password Hacking** − This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.
* **Computer Hacking** − This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.

## Advantages of Hacking

Hacking is quite useful in the following scenarios −

* To recover lost information, especially in case you lost your password.
* To perform penetration testing to strengthen computer and network security.
* To put adequate preventative measures in place to prevent security breaches.
* To have a computer system that prevents malicious hackers from gaining access.

## Disadvantages of Hacking

Hacking is quite dangerous if it is done with harmful intent. It can cause −

* Massive security breach.
* Unauthorized system access on private information.
* Privacy violation.
* Hampering system operation.
* Denial of service attacks.
* Malicious attack on the system.

## Purpose of Hacking

There could be various positive and negative intentions behind performing hacking activities. Here is a list of some probable reasons why people indulge in hacking activities −

* Just for fun
* Show-off
* Steal important information
* Damaging the system
* Hampering privacy
* Money extortion
* System security testing
* To break policy compliance
* Hackers can be classified into different categories such as white hat, black hat, and grey hat, based on their intent of hacking a system. These different terms come from old Spaghetti Westerns, where the bad guy wears a black cowboy hat and the good guy wears a white hat.

## White Hat Hackers

* White Hat hackers are also known as **Ethical Hackers**. They never intent to harm a system, rather they try to find out weaknesses in a computer or a network system as a part of penetration testing and vulnerability assessments.
* Ethical hacking is not illegal and it is one of the demanding jobs available in the IT industry. There are numerous companies that hire ethical hackers for penetration testing and vulnerability assessments.

## Black Hat Hackers

* Black Hat hackers, also known as **crackers**, are those who hack in order to gain unauthorized access to a system and harm its operations or steal sensitive information.
* Black Hat hacking is always illegal because of its bad intent which includes stealing corporate data, violating privacy, damaging the system, blocking network communication, etc.

## Grey Hat Hackers

* Grey hat hackers are a blend of both black hat and white hat hackers. They act without malicious intent but for their fun, they 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 and getting appreciation or a little bounty from the owners.

## Miscellaneous Hackers

* Apart from the above well-known classes of hackers, we have the following categories of hackers based on what they hack and how they do it −

### Red Hat Hackers

* Red hat hackers are again a blend of both black hat and white hat hackers. They are usually on the level of hacking government agencies, top-secret information hubs, and generally anything that falls under the category of sensitive information.

### Blue Hat Hackers

* A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch. They look for loopholes that can be exploited and try to close these gaps. Microsoft also uses the term **BlueHat** to represent a series of security briefing events.

### Elite Hackers

* This is a social status among hackers, which is used to describe the most skilled. Newly discovered exploits will circulate among these hackers.

### Script Kiddie

* A script kiddie is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept, hence the term **Kiddie**.

### Neophyte

* A neophyte, "n00b", or "newbie" or "Green Hat Hacker" is someone who is new to hacking or phreaking and has almost no knowledge or experience of the workings of technology and hacking.

### Hacktivist

* A hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denialof-service attacks.