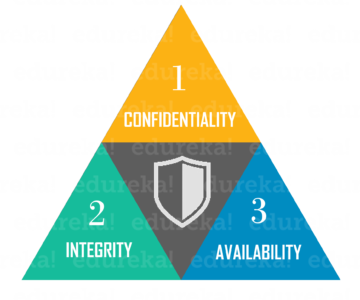
**Idea of Computer Security**

1. The origins of security systems are obscure, but techniques for protecting the household, such as the use of locks and barred windows, are very ancient. As civilizations developed, the distinction between passive and active security was recognized, and responsibility for active security measures was vested in police and fire-fighting agencies.
2. Computer security, also called cybersecurity, the protection of [computer](https://www.britannica.com/technology/computer) systems and information from harm, theft, and unauthorized use. Computer hardware is typically protected by the same means used to protect other valuable or sensitive equipment—namely, serial numbers, doors and locks, and alarms. The protection of information and system access, on the other hand, is achieved through other tactics, some of them quite complex.
3. The security precautions related to computer information and access address four major threats: (1) theft of [data](https://www.britannica.com/dictionary/data), such as that of military secrets from government computers; (2) vandalism, including the destruction of data by a computer virus; (3) fraud, such as employees at a [bank](https://www.britannica.com/topic/bank) channeling funds into their own accounts; and (4) invasion of privacy, such as the illegal accessing of protected personal financial or medical data from a large database. The most basic means of protecting a [computer system](https://www.britannica.com/technology/computer) against theft, vandalism, invasion of privacy, and other irresponsible behaviours is to electronically track and record the access to, and activities of, the various users of a computer system. This is commonly [done](https://www.britannica.com/dictionary/done) by assigning an individual [password](https://www.britannica.com/technology/password-computing) to each person who has access to a system. The computer system itself can then automatically track the use of these passwords, recording such data as which files were accessed under particular passwords and so on.
4. security measure is to store a system’s data on a separate device or medium that is normally inaccessible through the computer system. Finally, data is often encrypted so that it can be deciphered only by holders of a singular encryption [key](https://www.britannica.com/technology/key-lock-device). (See [data encryption](https://www.britannica.com/technology/data-encryption).)
5. Computer security has become increasingly important since the late 1960s, when [modems](https://www.britannica.com/technology/modem) (devices that allow computers to communicate over telephone lines) were introduced. The proliferation of personal computers in the 1980s [compounded](https://www.merriam-webster.com/dictionary/compounded) the problem because they enabled [hackers](https://www.britannica.com/technology/hacking-computing) (irresponsible computerphiles) to illegally access major computer systems from the privacy of their homes. With the tremendous growth of the [Internet](https://www.britannica.com/technology/Internet) in the late 20th and early 21st centuries, computer security became a widespread concern.
6. The development of advanced security techniques aims to diminish such threats, though [concurrent](https://www.merriam-webster.com/dictionary/concurrent) refinements in the methods of [computer crime](https://www.britannica.com/topic/cybercrime) pose ongoing hazards.
7. security and protection system, any of various means or devices designed to guard persons and property against a broad range of hazards, including [crime](https://www.britannica.com/topic/crime-law), fire, accidents, espionage, sabotage, subversion, and attack.
8. Most security and protection systems emphasize certain hazards more than others. In a retail store, for example, the principal security concerns are shoplifting and employee dishonesty (e.g., pilferage, embezzlement, and fraud). A typical set of categories to be protected includes the personal [safety](https://www.britannica.com/topic/safety-condition) of people in the organization, such as employees, customers, or residents; [tangible](https://www.merriam-webster.com/dictionary/tangible) property, such as the plant, equipment, finished products, cash, and securities; and intangible property, such as highly classified national-security information or “proprietary” information (e.g., trade secrets) of private organizations.
9. An important distinction between a security and protection system and public services such as [police](https://www.britannica.com/topic/police) and [fire](https://www.britannica.com/technology/firefighting) departments is that the former employs means that emphasize passive and preventive measures.

### ****The CIA Triad****

Computer security is mainly concerned with three main areas:

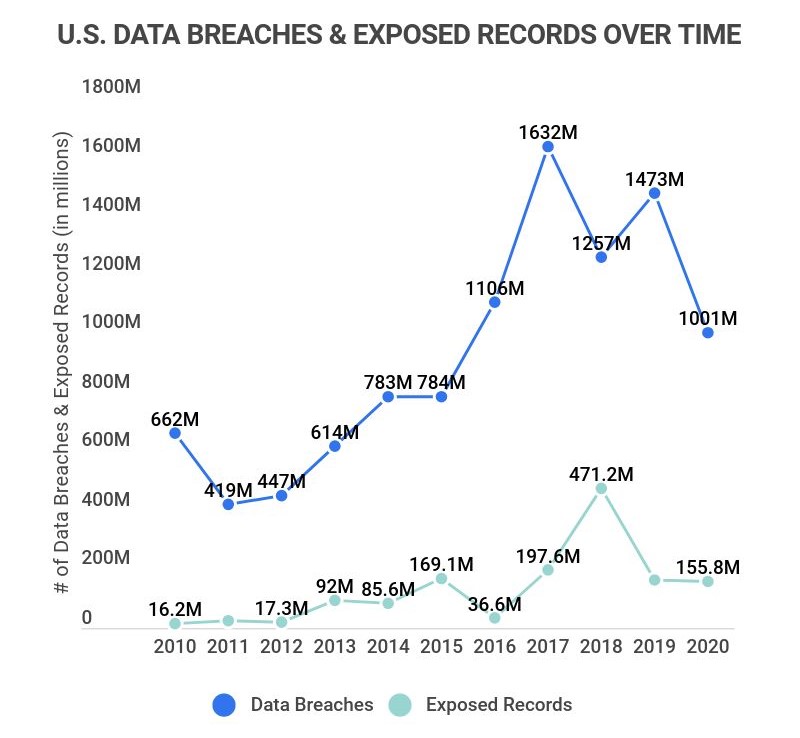
* **Confidentiality** is ensuring that information is available only to the intended audience
* **Integrity** is protecting information from being modified by unauthorized parties
* **Availability** is protecting information from being modified by unauthorized parties



**Need For Computer Security**

* [Computer security](https://www.thenetworkpro.net/index.php/On-Demand-Services/endpoint-security.html) is the process of preventing and detecting unauthorized use of your computer. Prevention measures help you stop unauthorized users (hackers) from accessing any part of your computer system. Detection helps you to determine whether or not someone attempted to break into your system, if they were successful, and what they may have done.
* Our computers have become an extension of everything we do from banking and investing to shopping and communicating with others through email or chat. You may not consider your communications "top secret," most likely you do not want strangers reading your email, using your computer to attack other systems, sending forged email from your computer, or examining personal information stored on your computer.
* Hackers do not care about your identity. Often they want to gain control of your computer so they can use it to launch attacks on other computer systems.
* Having control of your computer gives the hackers the ability to hide their actual location as they launch attacks, often against high-profile computer systems such as government or financial systems.
* Hackers have the ability to watch all your actions on the computer, or cause damage to your computer by reformatting your hard drive or changing your data.
* Unfortunately, hackers are always discovering new vulnerabilities to exploit in computer software. The complexity of software makes increasingly difficult to thoroughly test the security of computer systems.
* Internet Security is the most important aspect that everyone using the internet should understand. [The Network Pro](https://www.thenetworkpro.net/index.php/On-Demand-Services/endpoint-security.html)offers a few important tips to keep yourself secure and protect your Information from Security threats.

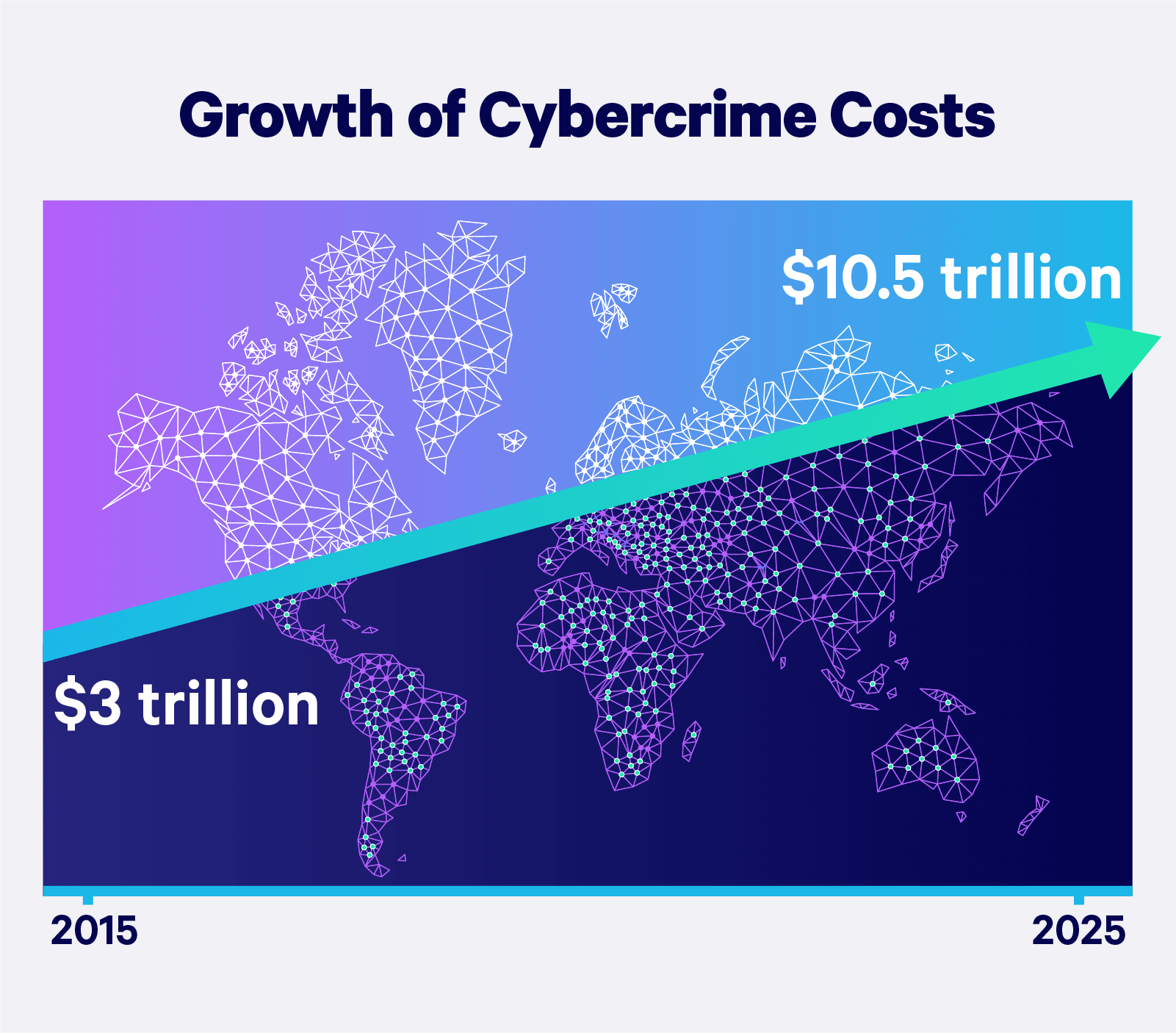
**Stats of Cyber Attacks:-**

****

**Recent Cyber Attacks**

As data breaches become more pervasive in our interconnected world so must our understanding of modern day cyber attacks.

* 2022 – [The ZLoader botnet responsible for distributing the ZLoader malware](https://purplesec.us/security-insights/zloader-malware/) was taken down in a joint effort with Microsoft, ESET, Black Lotus Labs, Palo Alto Networks, HealthISAC, and Financial Services-ISAC.
* 2022 – On May 8th, 2022 the a national emergency was declared due to an ongoing [Conti ransomware attack against several Costa Rican government entities](https://purplesec.us/security-insights/conti-ransomware-attack/).
* 2021 – [Kaseya suffered a ransomware attack](https://purplesec.us/kaseya-ransomware-attack-explained/) compromising up to 1500 companies with a staggering ransom note of $70 million.
* 2021 – [Saudi Aramco experienced a data breach](https://purplesec.us/saudi-aramco-data-breach-explained/) exposing sensitive data on employees and technical specifications of the organization. Threat group ZeroX is demanding a payment of $50 million.
* 2021 – [The Accellion file transfer application (FTA) data breach](https://purplesec.us/accellion-data-breach-explained/) impacted over 100 companies, organizations, universities, and government agencies around the world.
* 2021 – [The Pulse Secure VPN zero-day was exploited](https://purplesec.us/pulse-secure-vpn-breach/) resulting in the breach of several undisclosed defense firms and government organizations in the United States and Europe.
* 2021 – [Solarwinds fell victim to a nation-state supply chain attack](https://purplesec.us/weekly-ingest/prevent-solarwinds-supply-chain-attack/) impacting government agencies and fortune 500 companies.
* 2020 – [Spartanburg County School District](https://www.goupstate.com/news/20200303/spartanburg-school-district-1-hit-with-ransomware-attack) was the victim of a ransomware attack on February 26th. As a result, internet connectivity and network access was shut off for three days. Although no data was compromised, the district did lose all online access.
* 2020 – [Tillamook County](https://www.tillamookheadlightherald.com/news_paid/cyberattack-county-to-negotiate-for-ransomware-key/article_d31f0e00-4168-11ea-a179-cf3d1ff50ef6.html) commissioners negotiate for an encryption key to regain control of the government’s computer systems after falling victim to a ransomware attack.
* 2020 – [Universal Health Services](https://ir.uhsinc.com/news-releases/news-release-details/universal-health-services-inc-reports-information-technology) reports an information technology security incident. Malware, specifically the Ryuk ransomware, which targeted 400 hospitals in the US and the UK. UHS has over 90,000 employees who provide healthcare services to roughly 3.5 million patients every year.
* 2020 – [Duesseldorf University Hospital](https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/krankenhaus-derzeit-nur-sehr-eingeschraenkt-erreichbar-patientenversorgung-eingeschraenkt) is infected with ransomware, resulting in the first death reported following a ransomware attack.
* 2020 – The hotel chain Marriott disclosed a security breach that impacted the data of more than 5.2 million hotel guests who used their company’s loyalty application.
* 2020 – MGM Resorts suffered a massive data breach resulting in the leak of 142 million personal details of hotel guests.
* 2020 – 500,000 stolen Zoom passwords available for sale in dark web crime forums.
* 2020 – Magellan Health was struck by a ransomware attack and data breach stating that 365,000 patients were affected in the sophisticated cyberattack.
* 2020 – Twitter breach well-coordinated scam made attackers swindle $121,000 in Bitcoin through nearly 300 transactions.
* 2019 – Maryland Department of Labor was breached by hackers who illegally accessed names and social security numbers belonging to 78,000 people.
* 2019 – Captical One recently had over 106 million records stolen containing personal and financial information.
* 2018 – After falling victim to the SamSam malware, [the city of Atlanta, Georgia refused to pay the $50,000 ransom](https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/) and instead spent more than $5 million rebuilding its computer network.
* 2018 – Cyber attackers hacked into Marriot international computer systems and compromised five hundred million accounts.
* 2018 – Cathy pacific was hacked and 9.4 million accounts were compromised.
* 2018 – Facebook code was exploited by attackers and 50 million user accounts were compromised.
* 2018 – Quora was hacked and information belonging to 100million users was compromised.
* 2018 – Under Armor reported that its “My Fitness Pal” was hacked, affecting 150 million users.
* 2017 – Uber network was breached compromising data of fifty million riders, seven million drivers and 600,000 US based driver license details.
* 2017 – Cyber attackers hacked into Equifax servers and exposed over 143 million consumers’ personal information.
* 2017 – 412 million user accounts were stolen from Friendfinder’s sites.
* 2017 – 147.9 million consumers were affected by the Equifax Breach.
* 2016 – Peace cyber-attackers hacked Myspace compromising over 360 million accounts.
* 2016 –  Uber reported that hackers stole the information of over 57 million riders and drivers.
* 2015 – Hackers broke into Anthem Inc. servers and stole 37.5 million records consisting of sensitive information.
* 2015 – Peace a Russian based Cyber-attack group infiltrated LinkedIn stealing email and password combinations of over 117 million customers.
* 2014 – Syrian Electronic Army cyber hacking group infiltrated eBay’s network stealing sensitive information of one hundred and forty-five million users.
* 2013 – Cyber criminals hacked Yahoo’s 3 billion email accounts gaining access to sensitive customer information.
* 2013 – Cyber attackers used malware to steal data from Target company point of sale systems compromising information of approximately one hundred and ten million credit/debit carrying customers.

****

**Leading Cyber Security Firms**

* **Microsoft Corporation – Revenue [US$143.02 Billion]**

American tech company, Microsoft provides a comprehensive range of services that offers a complete package of security, identity, and cybersecurity. The services include a broad range of Security and Identity services that include strategy, planning, implementation, and support. These services are designed to assist organizations deploy security solutions that are in line with their business goals. [Microsoft Security Risk Assessment](https://www.microsoft.com/en-us/download/details.aspx?id=12273) (MSRA) is specifically designed to help enterprises overcome the challenges and assess the efficacy of the security strategic deployed by a thorough evaluation of defense-in-depth concept, which is the implementation of layered defenses.

* **McAfee – Revenue [US$2.90 Billion]**

McAfee Corp., based in California, United States, is one of the globally leading security software company. McAfee chiefly develops digital-security tools for personal computers and server devices and mobile devices. McAfee IntruShield, now called [McAfee Network Security Platform](https://www.mcafee.com/enterprise/en-in/security-awareness/cybersecurity.html), is a network-based intrusion prevention sensor appliance majorly used to prevent zero-day, DoS attacks, spyware, and malware threats. McAfee LiveSafe offers antivirus, firewall, and anti-spyware and anti-ransomware capabilities. It offers advanced security solutions that detect, protect, and eliminate threats across any device. McAfee’s Advanced Cyber Threat Services helps organizations combat potential threats, design robust security programs, and protect critical and valuable data.

* **Cisco Systems, Inc. – Revenue [US$49.3 Billion]**

American multinational tech corporation, Cisco Systems designs and commercializes hardware, and equipment for network and telecommunication, and other advanced products. The company specializes in varied tech markets including domain security, IoT, and energy-related services. [Cisco cybersecurity solutions](https://www.cisco.com/c/en_in/products/security/what-is-cybersecurity.html) are specifically designed for SMBs and have rapid detection rate of malware, exploits, and evasions and can detect 100% attacks within 5 minutes. Cisco Start is a customizable suite of security solutions that cover cloud, network, and endpoints. Among these, Cisco Umbrella is a cloud-delivered security service that acts as the first line of defense against malware and other cyber threats. It uses the interface of the Internet and eliminates threats before a strong connection can be established. Cisco Meraki® MX Security Appliances offers a Unified Threat Management (UTM) solution to small and medium enterprises. AMP Solutions protects the businesses and organization before, during, and after a cyberattack.

* **IBM – Revenue [US$76.2 Billion]**

International Business Machines (IBM) Corporations is a multinational company based in the U.S. that specializes in cloud computing, artificial intelligence, and other advanced technologies. IBM has one of the broadest portfolio of consulting and managed security services. [IBM Security Services](https://www.ibm.com/in-en/security/services) offers top-notch assessments and security strategies – including zero trust – to large enterprises. IBM Security Services offers assistance to businesses and organizations in quantifying and understanding the risks, enhance resources, rapid detection and response to threat, and bolster security priorities of organizations to accelerate their business transformation. IBM leverages AI, Machine Learning, and Watson, to detect and respond to cyber threats in real-time and efficiently.

**Hardware:-**

Lenovo Legion y540:-

LENOVO LEGION Y540 (81SY00C3IN) LAPTOP (CORE I5 9TH GEN/8 GB/1 TB 128 GB SSD/WINDOWS 10/4 GB) SPECIFICATIONS

**Multimedia (7)**

|  |  |
| --- | --- |
| **Secondary Camrearfacing** | No |
| **Microphone Type** | Digital Microphone |
| **Inbuilt Microphone** | Yes |
| **Sound Technologies** | Dolby Audio |
| **Webcam** | Yes |
| **Speakers** | Stereo Speakers |
| **Video Recording** | 720p HD |

**Performance (4)**

|  |  |
| --- | --- |
| **Graphics Memory** | 4 GB |
| **Clockspeed** | 2.4 Ghz |
| **Graphic Processor** | NVIDIA GeForce GTX 1650 |
| **Processor** | Intel Core i5-9300H (9th Gen) |

**Memory (6)**

|  |  |
| --- | --- |
| **Memory Layout** | 1x8 Gigabyte |
| **Expandable Memory** | 32 GB |
| **Ram Type** | DDR4 |
| **Memory Slots** | 1 |
| **Ram Speed** | 2400 Mhz |
| **Capacity** | 8 GB |

**Display Details (6)**

|  |  |
| --- | --- |
| **Display Type** | LED |
| **Display Resolution** | 1920 x 1080 Pixels |
| **Display Touchscreen** | No |
| **Display Features** | Full HD LED Backlit Anti-Glare Display |
| **Pixel Density** | 141 ppi |
| **Display Size** | 15.6 Inches (39.62 cm) |

**Peripherals (4)**

|  |  |
| --- | --- |
| **Keyboard** | Standard Notebook Keyboard |
| **Pointing Device** | Touchpad with Multi-Touch Gestures Enabled |
| **Optical Drive** | No |
| **Fingerprint Scanner** | No |

**General Information (7)**

|  |  |
| --- | --- |
| **Dimensions** | 365 x 260 x 24  mm |
| **Operating System Type** | 64-bit |
| **Weight** | 2.3 Kg |
| **Operating System** | Windows 10 Home Basic |
| **Model** | Y540 (81SY00C3IN) |
| **Brand** | Lenovo |
| **Colors** | Black |

**Networking (3)**

|  |  |
| --- | --- |
| **Wireless Lan** | 802.11 a/b/g/n/ac |
| **Bluetooth** | Yes |
| **Bluetooth Version** | 4.2 |

**Storage (4)**

|  |  |
| --- | --- |
| **Hdd Speedrpm** | 5400 RPM |
| **Ssd Capacity** | 128 GB |
| **Hdd Capacity** | 1 TB |
| **Hdd Type** | SATA |

**Battery (4)**

|  |  |
| --- | --- |
| **Power Supply** | 52 W AC Adapter W |
| **Battery Cell** | 3 Cell |
| **Battery Type** | Li-Ion |
| **Battery Life** | 5 Hrs |

**Ports (3)**

|  |  |
| --- | --- |
| **Sd Card Reader** | Yes |
| **Headphone Jack** | Yes |
| **Microphone Jack** | Yes |

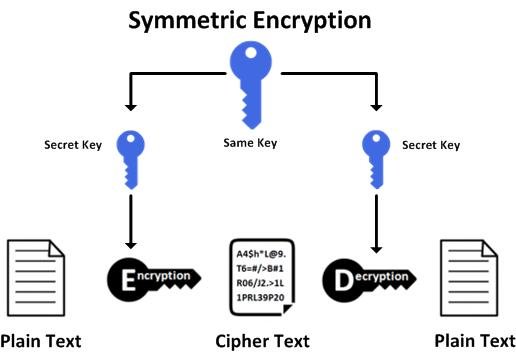
**Software:-**

* **Python** is an interpreted, object-oriented, high-level programming language with dynamic semantics. Its high-level built-in data structures, combined with dynamic typing and dynamic binding, make it very attractive for Rapid Application Development, as well as for use as a scripting or glue language to connect existing components together.
* Python's simple, easy to learn syntax emphasizes readability and therefore reduces the cost of program maintenance. Python supports modules and packages, which encourages program modularity and code reuse. The Python interpreter and the extensive standard library are available in source or binary form without charge for all major platforms and can be freely distributed.
* **Debugging Python** programs is easy: a bug or bad input will never cause a segmentation fault. Instead, when the interpreter discovers an error, it raises an exception. When the program doesn't catch the exception, the interpreter prints a stack trace. A source level debugger allows inspection of local and global variables, evaluation of arbitrary expressions, setting breakpoints, stepping through the code a line at a time.

**Different Encryption Types**

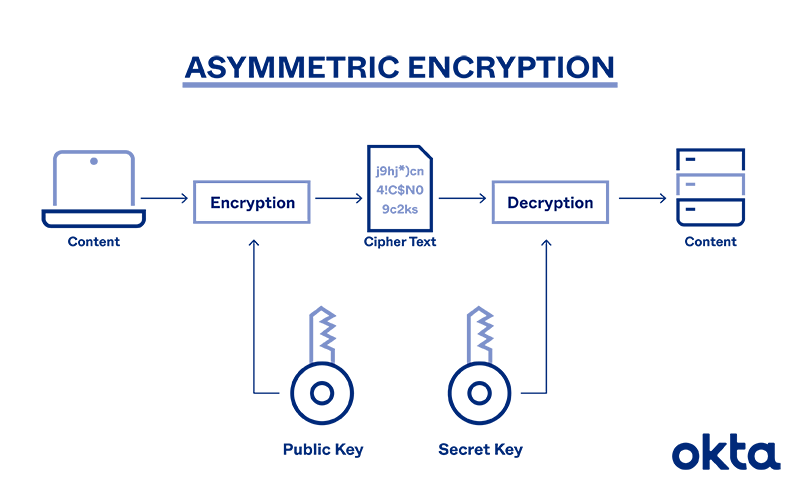
**Symmetric Key Encryption:**

Encryption is a process to change the form of any message in order to protect it from reading by anyone. In Symmetric-key encryption the message is encrypted by using a key and the same key is used to decrypt the message which makes it easy to use but less secure. It also requires a safe method to transfer the key from one party to another.

****

**Asymmetric Key Encryption:**

Asymmetric Key Encryption is based on public and private key encryption techniques. It uses two different key to encrypt and decrypt the message. It is more secure than the symmetric key encryption technique but is much slower.

****

| ****Symmetric Key Encryption**** | ****Asymmetric Key Encryption**** |
| --- | --- |
| It only requires a single key for both encryption and decryption. | It requires two keys, a public key and a private key, one to encrypt and the other one to decrypt. |
| The size of cipher text is the same or smaller than the original plain text  . | The size of cipher text is the same or larger than the original plain text. |
| The encryption process is very fast. | The encryption process is slow. |
| It is used when a large amount of data is required to transfer. | It is used to transfer small amounts of data. |
| It only provides confidentiality. | It provides confidentiality, authenticity, and non-repudiation. |
| The length of key used is 128 or 256 bits | The  length of key used is 2048 or higher |
| In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption. | In asymmetric key encryption, resource utilization is high. |
| It is efficient as it is used for handling large amount of data. | It is comparatively less efficient as it can handle a small amount of data. |
| Security is less as only one key is used for both encryption and decryption purpose. | It is more secure as two keys are used here- one for encryption and the other for decryption. |

**Encryption Algorithms**

### 1. Triple DES

[Triple DES](https://searchsecurity.techtarget.com/tip/Expert-advice-Encryption-101-Triple-DES-explained) was designed to replace the original Data Encryption Standard (DES) algorithm, which hackers eventually learned to defeat with relative ease. At one time, Triple DES was the recommended standard and the most widely used symmetric algorithm in the industry.

Triple DES uses three individual keys with 56 bits each. The total key length adds up to 168 bits, but experts would argue that 112-bits in key strength is more accurate. Despite slowly being phased out, Triple DES has, for the most part, been replaced by the Advanced Encryption Standard (AES).

### 2. AES

The [Advanced Encryption Standard (AES](https://cybernews.com/resources/what-is-aes-encryption/)) is the algorithm trusted as the standard by the U.S. Government and numerous organizations. Although it is highly efficient in 128-bit form, AES also uses keys of 192 and 256 bits for heavy-duty encryption purposes.

AES is largely considered impervious to all attacks, except for brute force, which attempts to decipher messages using all possible combinations in the 128, 192, or 256-bit cipher.

### 3. RSA Security

[RSA](https://searchsecurity.techtarget.com/definition/RSA) is a public-key encryption algorithm and the standard for encrypting data sent over the internet. It also happens to be one of the methods used in PGP and GPG programs. Unlike Triple DES, RSA is considered an asymmetric algorithm due to its use of a pair of keys. You've got your public key to encrypt the message and a private key to decrypt it. The result of RSA encryption is a huge batch of mumbo jumbo that takes attackers a lot of time and processing power to break.

### 4. Blowfish

[Blowfish](https://searchsecurity.techtarget.com/definition/Blowfish) is yet another algorithm designed to replace DES. This symmetric cipher splits messages into blocks of 64 bits and encrypts them individually. Blowfish is known for its tremendous speed and overall effectiveness. Meanwhile, vendors have taken full advantage of its free availability in the public domain.

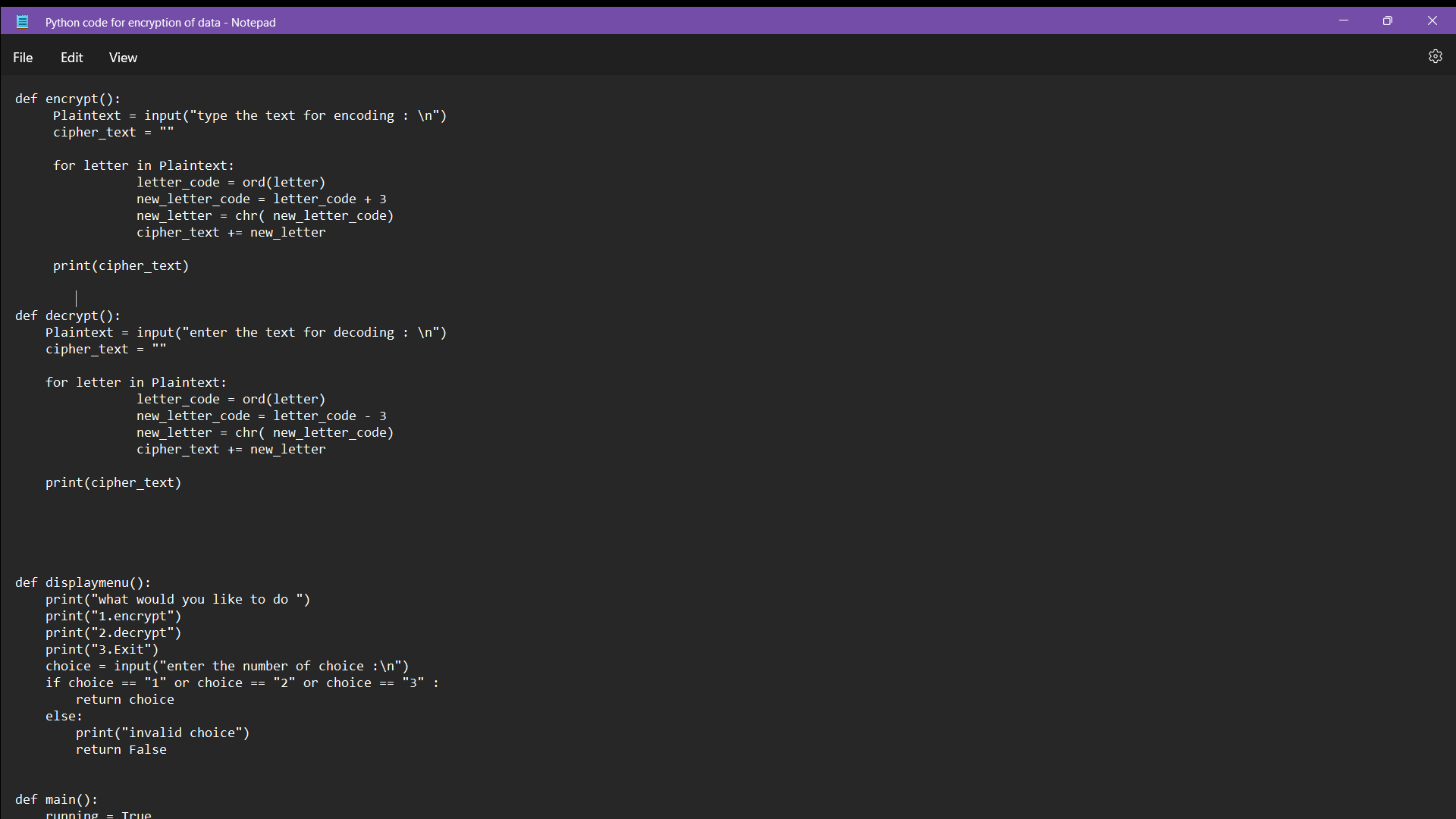
You'll find Blowfish in software categories ranging from e-commerce platforms for securing payments to password management tools, where it protects passwords. It's one of the more flexible encryption methods available.

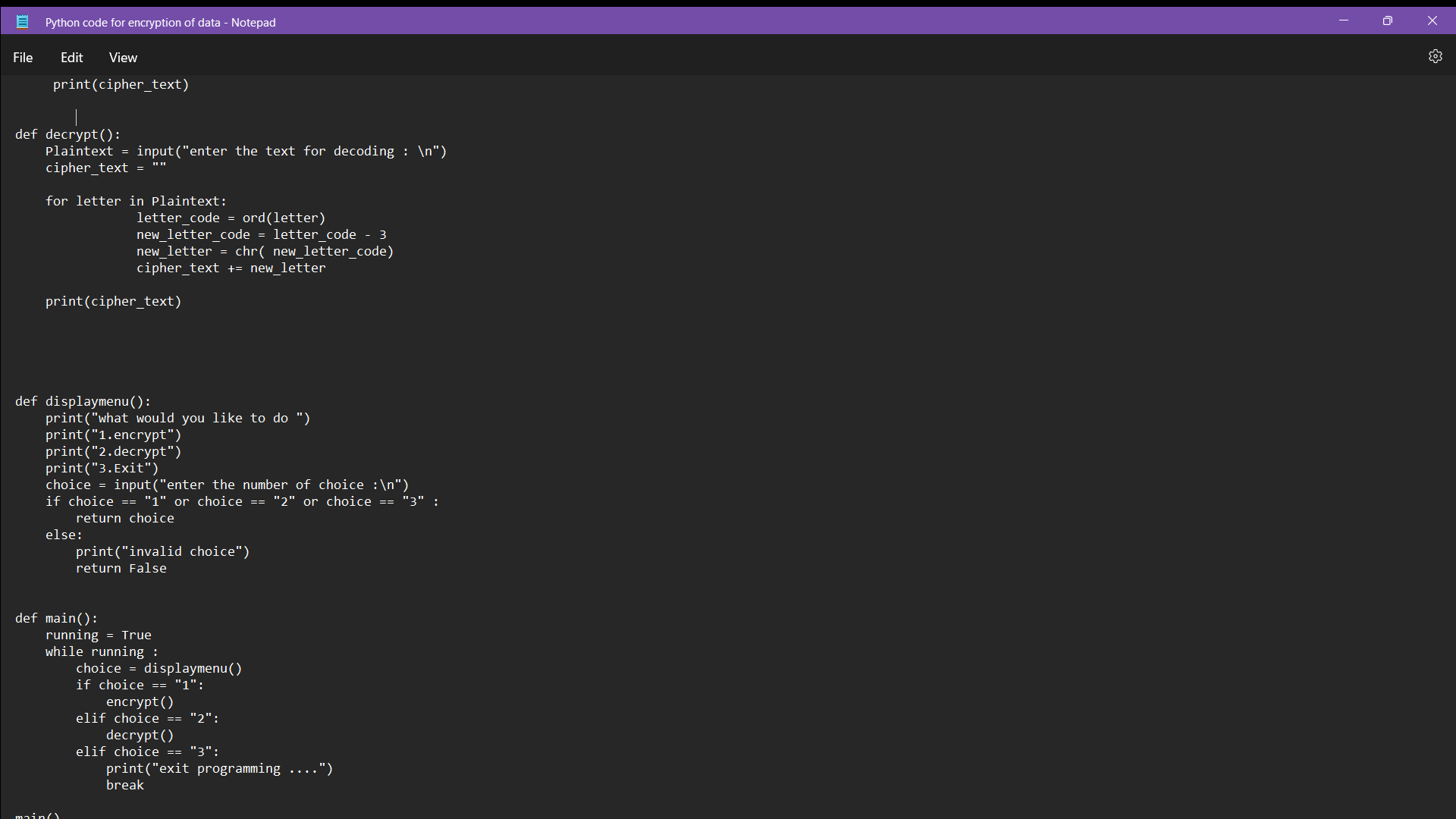
### 5. Twofish

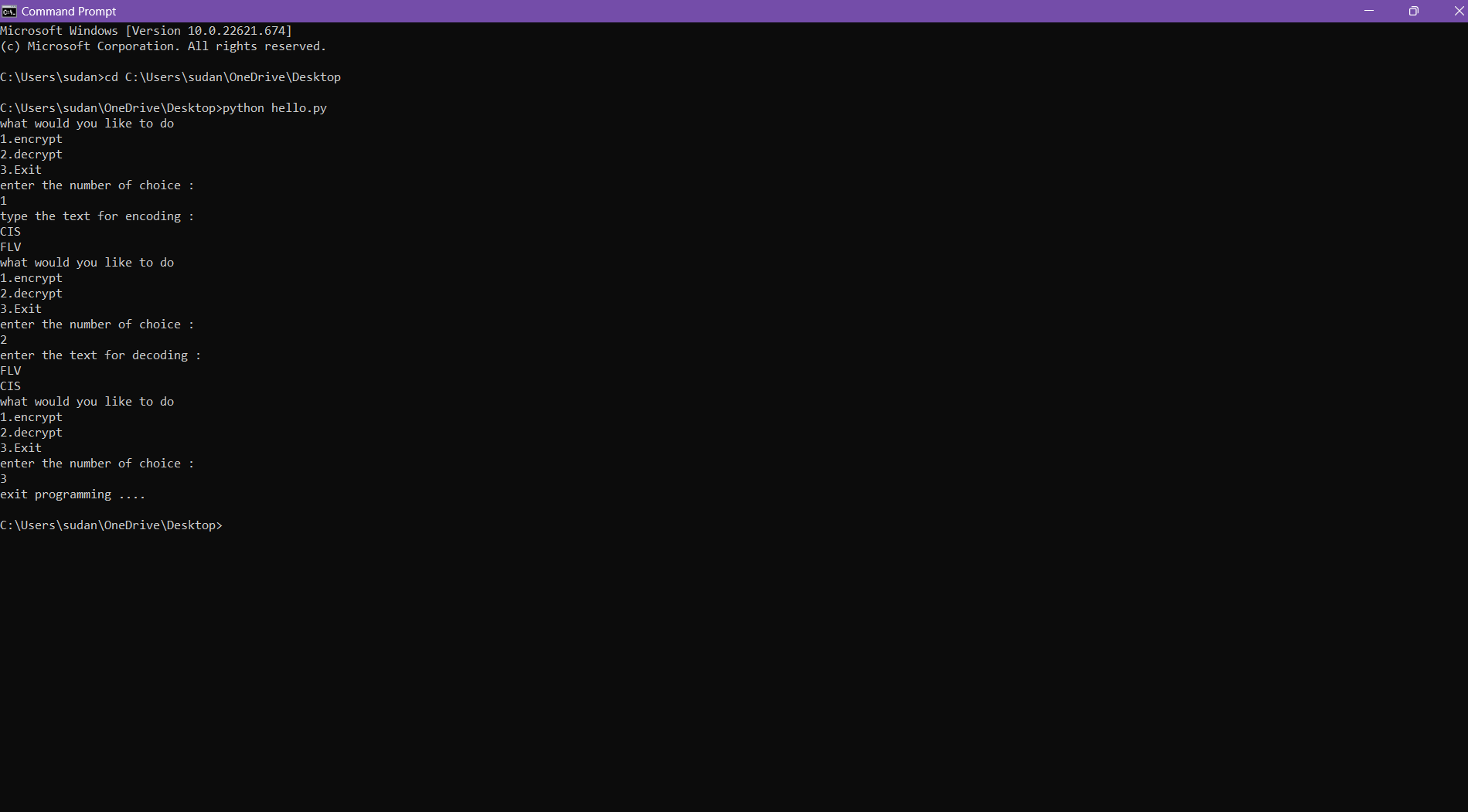
Computer security expert Bruce Schneier is the mastermind behind Blowfish and its successor [Twofish](https://searchsecurity.techtarget.com/definition/Twofish). Keys used in this algorithm may be up to 256 bits in length, and as a symmetric technique, you only need one key. Twofish is one of the fastest of its kind and ideal for use in hardware and software environments. Like Blowfish, Twofish is freely available to anyone who wants to use it.

**Our Encryption Algorithm**

**Input Code**

****

****

**Output**

**References:-**

* <https://en.wikipedia.org/wiki/Java_(programming_language)>
* <https://www.gadgetsnow.com/laptops/Lenovo-Legion-Y540-81SY00C3IN-Laptop-Core-i5-9th-Gen8-GB1-TB-128-GB-SSDWindows-104-GB>
* <https://purplesec.us/resources/cyber-security-statistics/#Recent>
* <https://www.thenetworkpro.net/why-is-computer-security-important/>
* <https://www.britannica.com/technology/computer-security>