2-FACE

IBADULLA , PRINCE , BHANU PRATAP , RAHUL GUPTA

Mentor : MR. AMIT KUMAR PANDEY

DR. AKHILESH DAS GUPTA INSTITUTE OF TECHNOLOGY & MANAGEMENT

(AFFILIATED TO GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY, DELHI)

Course: - Information Technology

Abstract

This Paper is based on two phase one is public and another is private. Public phase is only for public use and its help in reduce criminal activity , smuggling and help in any service. In Private Phase its only for specific person but not for public .For this Purpose I research on Introduction, python, cryptography, criminal activity, political corruption, woman safety, smuggling case, other country intrusion, security of information and unknown important information like missile code, terrorist activity case and Socket programming using python. In research Paper we study Covid19 case and maintaining of social distancing , facial Id of each person,development of country/ Smart Country, Example of Other developed Country and its criminal activity.

Introduction

In research Paper we study Covid19 case and maintaining of social distancing , facial Id of each person, development of country/ Smart Country, Example of Other developed Country and its criminal activity. For this Purpose I research on python, cryptography, criminal activity, political corruption, woman safety, smuggling case, other country intrusion, security of information and unknown important information like missile code, terrorist activity case and Socket programming using python. It consist two phase one is public and another is private. Public phase is only for public use and its help in reduce criminal activity , smuggling and help in any service. In Private Phase its only for specific person but not for public .

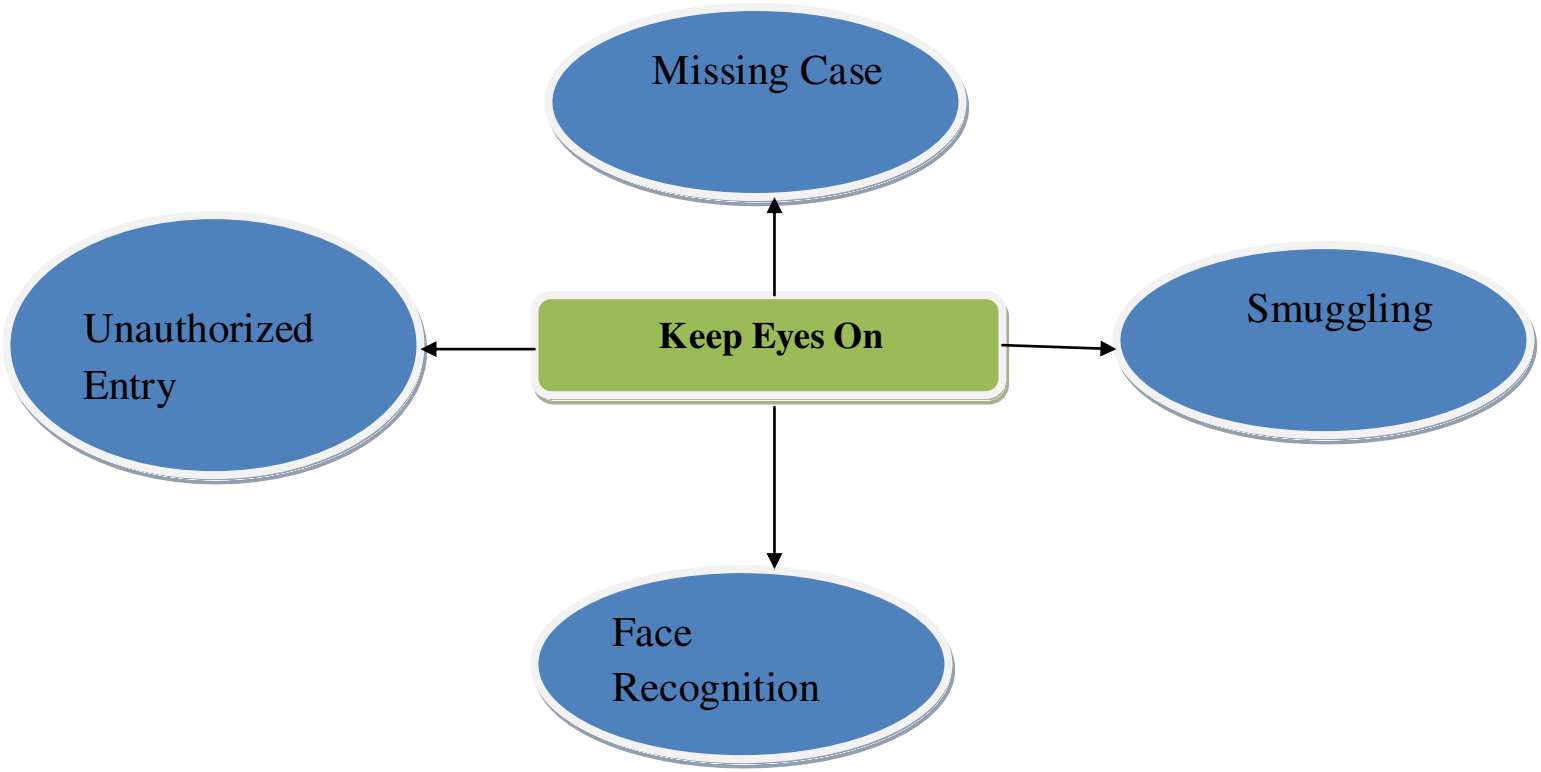
Security is freedom from, or resilience against, potential harm (or other unwanted coercive change) caused by others. Beneficiaries (technically referents) of security may be of persons and social groups, objects and institutions, ecosystems or any other entity or phenomenon vulnerable to unwanted change. Law is a system of rules created and enforced through social or governmental institutions to regulate behavior, with its precise definition a matter of longstanding debate Stocks, bonds, preferred shares, and ETFs are among the most common examples of marketable securities. Money market instruments, futures, options, and hedge fund investments can also be marketable securities. The overriding characteristic of marketable securities is their liquidity. Human rights are moral principles or norms for certain standards of human behaviour and are regularly protected in municipal and international law. Data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle. ... Data security involves deploying tools and technologies that enhance the organization's visibility into where its critical data resides and how it is used. Smuggling is the illegal transportation of objects, substances, information or people, such as out of a house or buildings, into a prison, or across an international border, in violation of applicable laws or other regulations. There are various motivations to smuggle.

Criminal Activity

Crime in India has been recorded since the British Raj, with comprehensive statistics now compiled annually by the National Crime Records Bureau (NCRB), under the Ministry of Home Affairs (India) (MHA).As of 2019, a total of 51.5 lakh cognizable crimes comprising 32.2 lakh Indian Penal Code (IPC) crimes and 19.4 lakh Special and Local Laws (SLL) crimes were registered nationwide. Showing a 1.6% annual increase in the registration of cases (50.7 lakh cases), the crime rate per 100,000 population has increased from 383.5 in 2018 to 385.5 in 2019. More than a fifth of all registered crime (10.5 lakh) were classified as offences affecting the human body, which included violent acts such as murder, kidnapping, assault and death by negligence.

- Arrest data show a clear pattern of arrests in terms of race, gender, and class. For instance, as mentioned above, young, urban, poor, and racial minorities are arrested and convicted more than others for personal and property crimes. To sociologists, the question posed by this data is whether this reflects actual differences in committing crimes among different groups, or whether this reflects differential treatment by the criminal justice system.Studies show that the answer is “both.” Certain groups are in fact more likely to commit crimes than others because crime often looked to as a survival strategy, is linked to patterns of inequality in the United States. However, the process of prosecution in the criminal justice system is also significantly related to patterns of race, class, and gender inequality. We see this in the official arrest statistics, in treatment by the police, in sentencing patterns, and in studies of imprisonment.
- Organized crime is committed by structured groups typically involving the distribution and sale of illegal goods and services. Many people think of the Mafia when they think of organized crime, but the term can refer to any group that exercises control over large illegal enterprises (such as the drug trade, illegal gambling, prostitution, weapons smuggling, or money laundering).

- A key sociological concept in the study or organized crime is that these industries are organized along the same lines as legitimate businesses and take on a corporate form. There are typically senior partners who control profits, employees who manage and work for the business, and clients who buy the goods and services that the organization provides.
- Examples of cognizable crimes include rape, murder, and theft. Among the cognizable crimes committed in 2006, there were 18,78,293 Indian Penal Code (IPC) crimes and 32,24,167 Special & Local Laws (SLL) crimes.



Woman Safety System

In the past decade, women have progressively earned a higher standard in the workplace. Women are now gaining higher positions and form a big/huge section of any working sector around the globe. Women now are more independent in every sense. They are competent enough to take care of themselves and their families. They are more able to make their own life choices and live in their own terms. However, everyday women are mistreated in the workplace by their co-workers. After the **#metoo** and **#timesup** movement in the U.S, more women are coming forward to tell their horror stories. Susan Fowler, an ex-employee from Uber claimed how her team manager harassed her on the very first day at her work. The incident led her to leave her team and eventually Uber. Following the incident, many other harassment complaints were filed. In the mid-2017, Uber fired 20 employees after investigating into the sexual harassment claims and workplace culture.The statistics on sexual harassment in the workplace is very shocking. And it varies from place to place. According to the survey, 81 percent of women have faced some form of sexual

harassment in their lives.Sexual harassment can lead to anxiety, depression, lower self-esteem, alienation and overall degradation of their physical and mental health. It's a disturbing fact that women in work still face sexual harassment, which is why many of them even quit their jobs.

- **Crimes against Women in India**

Not a day goes by where you don't hear of the news of a crime against women in India. In fact, there are at least five news articles that tell us about the horrific details of the various crimes. It is extremely painful to watch the status of women's safety in India, especially in a country where women are given the stature of goddesses.The list of crimes against women is quite long, to say the least. Acid attack is becoming very normal is various parts of the country. The criminal throws acid on the face of the victim to destroy their lives completely. Nonetheless, India has a lot of strong acid attack survivors who are battling for their lives and trying to lead their lives independently.Furthermore, domestic violence and honor killings are very common. The wife stays in an abusive relationship because of the fear of society. The family kills their daughters in the name of honor to keep up with the reputation of their family. Similarly, female feticides is yet another common crime. Due to the regressive thinking, people kill daughters before they are born.The list continues as crimes against women are on the rise. Other crimes also include child marriages, child abuse, rape, dowry deaths, trafficking and many more.

- **Ways to Ensure Women Safety**

Although the list of crimes is very long, we can take measures to ensure women's safety in our country. Firstly, the government must make stringent laws that ensure the punishment of criminals immediately. Fast track courts must be set so the victim gets justice instantly. This will serve as a great example for other men to not commit crimes against women.Most importantly, men must be taught to respect women from an early age. They must consider women as equals so they don't even think of harming them. When you consider someone inferior, you tend to oppress them. If this thinking goes away, half of the crimes will automatically end.In short, crimes against women are stopping the growth of our country. We must not put the blame on women and ask them to be extra careful. Instead, we must ask the men to change their thinking and work to make the world a safer place for women.

- **Some Women Law**

1. The Prohibition of Child Marriage Act, 2006
2. Special Marriage Act, 1954
3. Dowry Prohibition Act, 1961
4. Indian Divorce Act, 1969
5. Medical Termination of Pregnancy Act,1971
6. Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013
7. Indecent Representation of Women(Prevention) Act,1986
8. National Commission for Women Act, 1990
9. Equal Remuneration Act, 1976

Women's rights are the rights and entitlements claimed for women and girls worldwide. They formed the basis for the women's rights movement in the 19th century and the feminist movements during the 20th and 21st centuries. In some countries, these rights are institutionalized or supported by law, local custom, and behavior, whereas in others, they are ignored and suppressed. They differ from broader notions of human rights through claims of an inherent historical and traditional bias against the exercise of rights by women and girls, in favor of men and boys. Issues commonly associated with notions of women's rights include the right to bodily integrity and autonomy, to be free from sexual violence, to vote, to hold public office, to enter into legal contracts, to have equal rights in family law, to work, to fair wages or equal pay, to have reproductive rights, to own property, and to education.

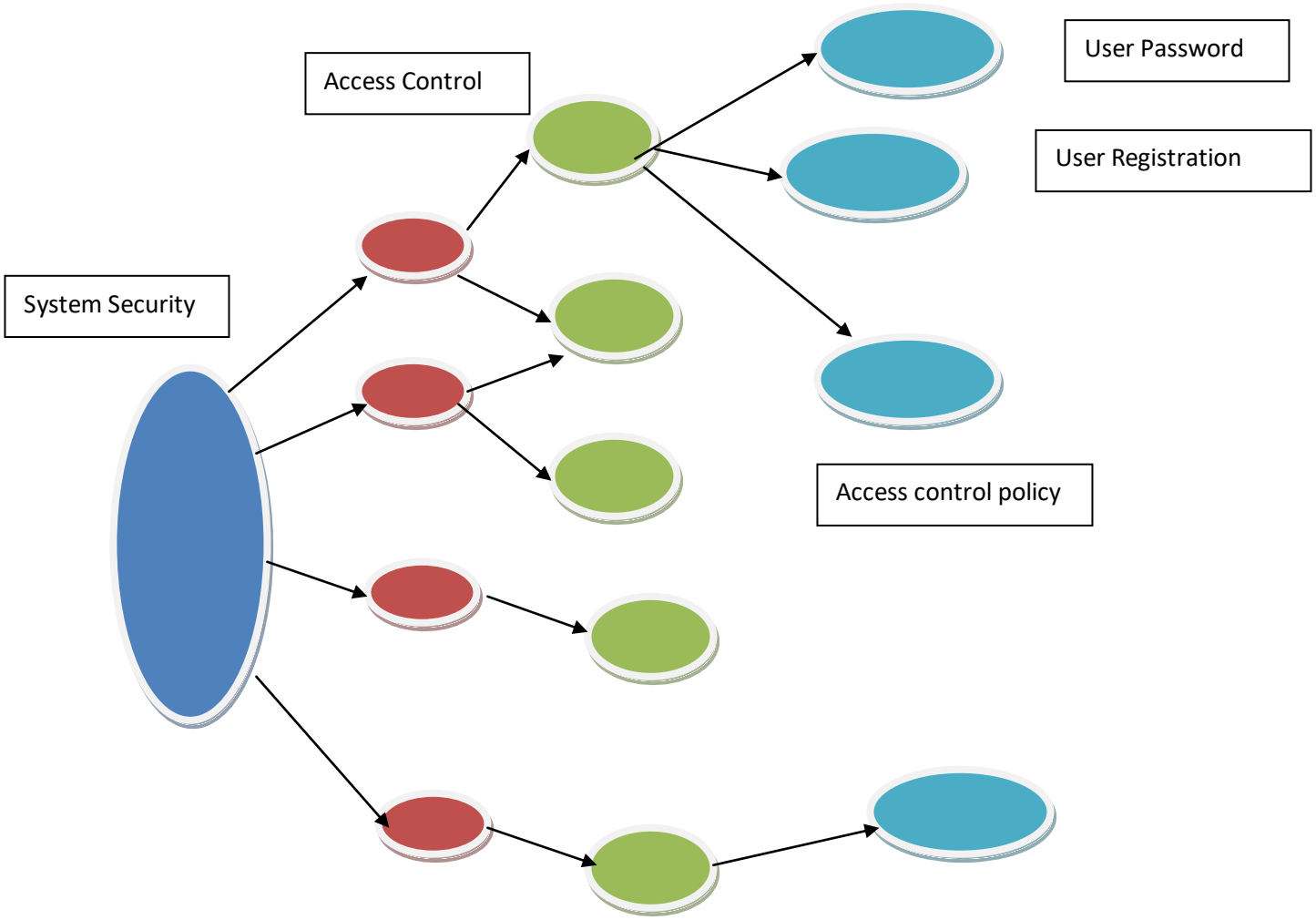
Security of Data and Information

Security is freedom from, or resilience against, potential harm (or other unwanted coercive change) caused by others. Beneficiaries (technically referents) of security may be of persons and social groups, objects and institutions, ecosystems or any other entity or phenomenon vulnerable to unwanted change. Information systems security is a hot topic in the news and at the water cooler these days. It is not uncommon to read about breaches in the security of large companies in the news daily. Target's major breach during Black Friday in 2013 left consumers concerned for their personal information. Earlier this year, The New York Times reported a data breach at White Lodging Services Corporation, which works with 168 hotels in 21 states. This breach resulted in the fraudulent use of hundreds of credit and debit cards for payment at Marriott hotels between March and December of 2013. Recently, Bloomberg Businessweek reported that the hackers that attacked the Neiman Marcus Group in late 2013 were part of a Russian syndicate that stole more than 160 million credit-card numbers from retailers over the course of seven years.

According to the dictionary of Military and Associated Terms of the US Department of Defense, information systems security is "The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security."At its most basic level information systems security is keeping confidential information, confidential.Businesses in the United States are seeing new rules and regulations that will need to be managed to protect consumer confidentiality. According to data from the Nilson report, the United States accounts for only 27% of credit card transactions in the world, but are the victims of 47% of fraud.Breaches such as these have reduced consumer confidence, and have moved the topic of the safety of personal information to the forefront for many organizations, which are promising to keep the data of its customers secure from hackers.

The question though is: As hackers become increasingly sophisticated, how organizations stay a step ahead to ensure their information systems security?

Generally information systems can be broken up into two main groups, IT security and information assurance. IT security is the security applied to technology, usually the computer system. IT security specialists are responsible for keeping all the technology in companies safe from cyber attacks. Information assurance is the act of ensuring data is not lost when issues arise, including natural disasters, computer/server malfunction, or theft. IT security specialists generally provide information assurance by having off-site backups of data to combat these problems.Cyber security and information systems security degrees are becoming increasingly popular. As cyber threats grow, demand for trained professionals continues to grow. Most recently, the need has emerged for not only technology experts but professionals who possess the technological capabilities and are well versed in business leadership and strategy.George Mason's Masters in Management of Secure Information Systems is a unique cyber security degree that provides IT professionals with the leadership skills and business fundamentals to address growing information systems security challenges. The multidisciplinary program includes courses taught by faculty from the School of Management, School of Engineering, and School of Public Policy. These faculty are not only experts in the field but seasoned professionals with first-hand knowledge and application of their subjects.



Types of Information Security

- Application security. Application security is a broad topic that covers software vulnerabilities in web and mobile applications and application programming interfaces (APIs).
- Cloud security.
- Cryptography.
- Infrastructure security.
- Incident response.
- Vulnerability management.

Information Security Goals in an Organization

- Confidentiality—prevents unauthorized users from accessing information to protect the privacy of information content. ...
- Integrity—ensures the authenticity and accuracy of information. ...
- Availability—ensures that authorized users can reliably access information.

Socket Programming Using Python

Socket programming is a way of connecting two nodes on a network to communicate with each other. One socket (node) listens on a particular port at an IP, while other socket reaches out to the other to form a connection. Server forms the listener socket while client reaches out to the server. They are the real backbones behind web browsing. In simpler terms there is a server and a client. Socket programming is started by importing the socket library and making a simple socket.

import socket

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

Here we made a socket instance and passed it two parameters. The first parameter is AF_INET and the second one is SOCK_STREAM. AF_INET refers to the address family ipv4. The SOCK_STREAM means connection oriented TCP protocol.
Now we can connect to a server using this socket.

Connecting to a server:
Note that if any error occurs during the creation of a socket then a socket.error is thrown and we can only connect to a server by knowing it's ip. You can find the ip of the server by using this :
You can also find the ip using python:
import socket

ip = socket.gethostbyname('www.google.com')

print ip

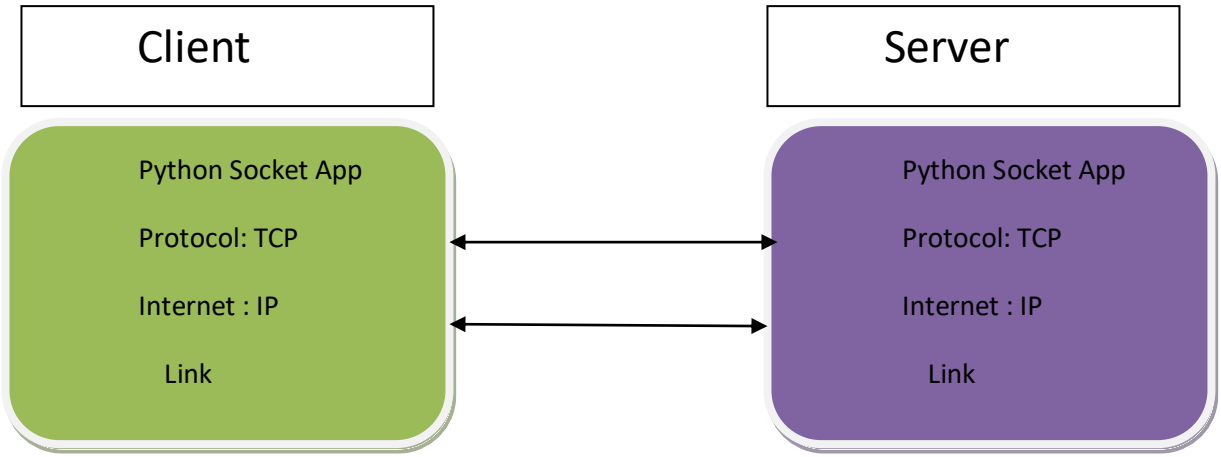
Why should you use TCP? The Transmission Control Protocol (TCP):

- Is reliable: packets dropped in the network are detected and retransmitted by the sender.
- Has in-order data delivery: data is read by your application in the order it was written by the sender.

In contrast, User Datagram Protocol (UDP) sockets created with socket. SOCK_DGRAM aren't reliable, and data read by the receiver can be out-of-order from the sender's writes.

Why is this important?

Networks are a best-effort delivery system. There's no guarantee that your data will reach its destination or that you'll receive what's been sent to you.Network devices (for example, routers and switches), have finite bandwidth available and their own inherent system limitations. They have CPUs, memory, buses, and interface packet buffers, just like our clients and servers. TCP relieves you from having to worry about packet loss, data arriving out-of-order, and many other things that invariably happen when you're communicating across a network.



TCP (Transmission Control Protocol) is a standard that defines how to establish and maintain a network conversation through which application programs can exchange data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other. Together, TCP and IP are the basic rules defining the Internet. The Internet Engineering Task Force (IETF) defines TCP in the Request for Comment (RFC) standards document number 793.

How Transmission Control Protocol works

TCP is a connection-oriented protocol, which means a connection is established and maintained until the application programs at each end have finished exchanging messages. It determines how to break application data into packets that networks can deliver, sends packets to and accepts packets from the network layer, manages flow control and -- because it is meant to provide error-free data transmission -- handles retransmission of dropped or garbled packets and acknowledges all packets that arrive. In the Open

Systems Interconnection (OSI) communication model, TCP covers parts of Layer 4, the transport layer, and parts of Layer 5, the session layer.

For example, when a web server sends an HTML file to a client, it uses the hypertext transfer protocol (HTTP) to do so. The HTTP program layer asks the TCP layer to set up the connection and send the file. The TCP stack divides the file into data packets, numbers them and then forwards them individually to the IP layer for delivery. Although each packet in the transmission has the same source and destination IP address, packets may be sent along multiple routes. The TCP program layer in the client computer waits until all the packets have arrived, then acknowledges those it receives and asks for the re-transmission of any it does not -- based on missing packet numbers. The TCP layer then assembles the packets into a file and delivers the file to the receiving application.

Cryptography and Encryption

Cryptography is the science of keeping information secure by transforming it into form that unintended recipients cannot understand. In cryptography, an original human readable message, referred to as *plaintext,* is changed by means of an *algorithm,* or series of mathematical operations, into something that to an uninformed observer would look like gibberish; this gibberish is called *ciphertext*.

Cryptographic systems require some method for the intended recipient to be able to make use of the encrypted message — usually, though not always, by transforming the ciphertext back into plaintext.

Cryptogeraphy vs Encryption

Encryption is what we call the process of turning plaintext into ciphertext. (C*rypt* may make you think of tombs, but it comes from a Greek word that means "hidden" or "secret.") Encryption is an important part of cryptography, but doesn't encompass the entire science. Its opposite is *decryption.*One important aspect of the encryption process is that it almost always involves both an algorithm and a *key*. A key is just another piece of information, almost always a number, that specifies how the algorithm is applied to the plaintext in order to encrypt it. Even if you know the method by which some message is encrypted, it's difficult or impossible to decrypt without that key.

History of cryptography

This is all very abstract, and a good way to understand the specifics of what we're talking about is to look at one of the earliest known forms of cryptography. It's known as the *Caesar cipher,* because Julius Caesar used it for his confidential correspondence; as his biographer Suetonius described it, "if he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet ... If anyone wishes to decipher these, and get at their meaning, he must substitute the fourth letter of the alphabet, namely D, for A, and so with the others."

Suetonius's description can be broken down into the two cryptographic elements we've discussed, the algorithm and the key. The algorithm here is simple: each letter is replaced by another letter from later in the alphabet. The key is how *many* letters later in the alphabet you need to go to create your

ciphertext. It's three in the version of the cipher Suetonius describes, but obviously other variations are possible — with a key of four, A would become E, for instance.A few things should be clear from this example. Encryption like this offers a fairly simple way to secretly send any message you like. Contrast that with a system of code phrases where, say, "Let's order pizza" means "I'm going to invade Gaul." To translate that sort of code, people at both ends of the communication chain would need a book of code phrases, and you'd have no way to encode new phrases you hadn't thought of in advance. With the Caesar cipher, you can encrypt any message you can think of. The tricky part is that everyone communicating needs to know the algorithm and the key in advance, though it's much easier to safely pass on and keep that information than it would be with a complex code book.The Caesar cipher is what's known as a *substitution cipher,* because each letter is substituted with another one; other variations on this, then, would substitute letter blocks or whole words. For most of history, cryptography consisted of various substitution ciphers deployed to keep government and military communications secure. Medieval Arab mathematicians pushed the science forward, particularly the art of decryption — once researchers realized that certain letters in a given language are more common than others, it becomes easier to recognize patterns, for instance. But most pre-modern encryption is incredibly simple by modern standards, for the obvious reason that, before the advent of computers, it was difficult to perform mathematical transformations quickly enough to make encryption or decryption worthwhile.In fact, the development of computers and advances in cryptography went hand in hand. Charles Babbage, whose idea for the Difference Engine presaged modern computers, was also interested in cryptography. During World War II, the Germans used the electromechanical Enigma machine to encrypt messages — and, famously, Alan Turing led a team in Britain that developed a similar machine to break the code, in the process laying some of the groundwork for the first modern computers. Cryptography got radically more complex as computers became available, but remained the province of spies and generals for several more decades. However, that began to change in the 1960s.

Cryptography in network security

It was the formation of the first computer networks that started civilians thinking about the importance of cryptography. Computers were talking to each other over the open network, not just via direct connections to one another; that sort of networking was transformative in many great ways, but also made it trivially easy to snoop on data traveling across the network. And with financial services being an early use case for computer communication, it was necessary to find a way to keep information secret.IBM led the way in the late 1960s with an encryption method known as "Lucifer", which was eventually codified by the US National Bureau of Standards as the first Data Encryption Standard (DES). As the internet began to grow in importance, more and better encryption was needed, and today a significant portion of data flying around the world is encrypted using varying techniques that we'll discuss in more detail in a moment.

What is cryptography used for?

We've already discussed some of the specific applications of cryptography, from keeping military secrets to transmitting financial data safely across the internet. In the bigger picture, though, there are some broad cyber security goals that we use cryptography to help us achieve, as cyber security consultant Gary Kessler explains. Using cryptographic techniques, security pros can:

- Keep the contents of data confidential
- Authenticate the identity of a message's sender and receiver
- Ensure the integrity of the data, showing that it hasn't been altered

- Demonstrate that the supposed sender really sent this message, a principle known as non-repudiation

Cryptography examples and techniques

There are numerous techniques and algorithms that implement each of the three types of encryption discussed above. They are generally quite complex and beyond the scope of this article; we've included links here where you can learn more about some of the most commonly used examples.

Secret key encryption:

- Triple DES, the modern successor to DES discussed above
- Advanced Encryption Standard (AES)
- Blowfish and its successor Two fish, both from security legend Bruce Schneier

Public key encryption:

- Diffie-Hellman key exchange
- RSA
- ElGamal

Hash functions:There are a wide range of hash functions with different specialized purposes.

Example of Developed Country

- **Dubai**

Dubai has some of the lowest crime rates—for both violent and non-violent crimes—of any city in the world and is ranked as one of the best places for personal safety.[4] Even petty theft like pickpocketing is rare in Dubai and violent crimes are almost nonexistent.The biggest risk to foreigners traveling to Dubai, and the UAE in general, is unwittingly breaking one of the country's stringent laws. Dubai severely punishes acts that many Western travelers would never even imagine are illegal, including drinking alcohol without a permit, holding hands, sharing a room

with someone of the opposite sex other than your spouse, taking pictures of other people, offensive language or gestures, and unsanctioned social media posts, for example.The truth is that many of these laws are broken every single day and no one cares; bars will sell you an alcoholic beverage even if you don't have a permit, hotels will give rooms to couples without asking for a marriage license, and travelers will take selfies that have other people in the background. It usually isn't a problem, until it is. A nearby plainclothes police officer or an upset individual who reports you can quickly turn your harmless mistake into a punishable offense.Established in 2017, Smart System stands proud as the leading provider of innovative smart products in Dubai. We aim to design, develop, and install intelligent systems that will enhance the outlook of your home and office spaces. Other than following a strict manual, we seek to incorporate the ideas and vision of our customers, in each of our projects. Our interactive glass division is skilled at manufacturing functional and intelligent glass products which offer complete privacy and security.

Contact us today to learn more about smart system technology and how it can help to improve your residential or commercial setting.

- **America**

The topic of crime in the United States is very broad, technically covering any action that is punishable under a state or federal law. Any analysis of the topic therefore requires division into further sub-categories. One common way to do this is to limit analysis to crimes involving jail time (i.e. misdemeanors and felonies, which generally differ through the length of jail time involved), then differentiate between violent crimes and property crimes. Violent crimes are defined as offenses which involve force or the threat of force, while property crime includes offences involving the taking of money or property, but where there is no force or threat of force against the victims. Property crimes outnumbered violent crimes in the U.S. in 2018, numbering 7.2 million and 1.2 million respectively. Larceny was the most common property crime with 5.2 million incidents, while aggravated assaults accounted for around two thirds of violent crimes.

Crime statistics in different U.S. states

- Looking only at the number of crimes in a geographic region does not show the full picture as a higher population generally produces a higher overall number of crimes. Considering the crime rate per 100,000 residents is more useful, as it more accurately reflects the underlying likelihood of being involved in a crime. For both the property crime rate by state and the violent crime rate in U.S. states in 2018, New Mexico and Alaska saw the highest rates, while states in New England generally saw the least. Note that while Washington D.C. technically topped both crime rate lists, this is a misleading result due to its strictly urban geography; comparison to the violent crime rate of U.S. cities sees Washington D.C. far behind places like Detroit and Memphis.

Is crime increasing?

While surveys on the public perception of crime trends in the U.S. show a majority believe crime is increasing every year, statistically this is not the case. Both the overall property crime rate and the violent crime rate in the U.S. have decreased by around half since the early 1990's. While there is disagreement over why this has occurred – with suggestions ranging from higher levels of incarceration, to the effect of legalized abortion in reducing the number of children born into socioeconomic circumstances likely to lead to crime – it is clear that crime is not in fact increasing, regardless of the general perception to the contrary.

Conclusion

In this whole research paper we studied about python, cryptography, criminal activity, political corruption, woman safety, smuggling case, other country intrusion, security of information and unknown important information like missile code, terrorist activity case and Socket programming using python. After all in project we used these all aspect and factor and made project name 2-Face. In 2-Face, we will make 2-phase one is public and another is private . Public phase is only for public use and its help in reduce criminal activity, smuggling and help in any service. In Private Phase its only for specific person but not for public .We conclude that by this project we reduce criminal activity , security of data and help in developed country in digital era called digitalization.

Reference

1. The True Crime Activity by Olivia lanae.
2. A Handbook of Applied Cryptography by Alfred J. Menezes, Paul C. Van Oorschot and Scott A. Vanstone,
3. Pseudo randomness and Cryptographic Application by Michael Luby Princeton University 1996.
4. The Pocket Guide to TCP/IP Sockets Book by Kenneth Leonard Calvert and Michael J. Donahoo.
5. Automate the Boring Stuff with Python, 2nd Edition: Practical Programming for Total Beginners Book by Al Sweigart.
6. https://www.statista.com/topics/2153/crime-in-the-united-states/
7. https://www.gfmag.com/global-data/non-economic-data/worlds-safest-countries-2019
8. https://www.csoonline.com/article/3583976/what-is-cryptography-how-algorithms-keep-information-secret-and-safe.html