FINAL YEAR MINI PROJECT PRESENTATION ON DIGITAL SIGNATURES

Submitted to

DEPARTMENT OF COMPUTER APPLICATIONS

KIET Group of Institutions, Ghaziabad

Uttar Pradesh-201206

DIGITAL SIGNATURES

PRESENTATION FLOW.....

- OBJECTIVE OF PROJECT
- CRYPTOGRAPHY

i. FEATURES
ii. TYPES OF CRYPTOGRAPY
iii. CRYPTANALYSIS
iv. TYPES OF CRYPTANALYTIC ATTACKS

- BLOCKCHAIN
  - BENEFITS
  - KEY CHALLENGES IN BLOCKCHAIN
  - ISSUES
- DIGITAL SIGNATURES
  - INTRODUCTION
  - IMPORTANCE OF DIGITAL SIGNATURE
  - WORKING
  - MERITS
  - DEMERITS

- Applications of digital signature
- FUTURE SCOPE OF PROJECT

OBJECTIVE OF PROJECT

- This project has been developed keeping in view the security features that need to be implemented in the networks following the fulfillment of these objectives:
- To develop an application that deals with the security threats that arise in the network.
- To enable the end-users as well as the organizations come out with a safe messaging communication without any threats from intruders or unauthorized people.
- To deal with the four inter-related areas of network security namely Secrecy, Authentication, Non-repudiation and Integrity

- Digital signatures work by proving that a digital message or document was not modified—intentionally or unintentionally—from the time it was signed. Digital signatures do this by generating a unique hash of the message or document and encrypting it using the sender's private key. The hash generated is unique to the message or document, and changing any part of it will completely change the hash.
- Once completed, the message or digital document is digitally signed and sent to the recipient. The recipient then generates their own hash of the message or digital document and decrypts the sender's hash (included in the original message) using the sender's public key. The recipient compares the hash they generate against the sender's decrypted hash; if they match, the message or digital document has not been modified and the sender is authenticated.
- Source authentication ' can be achieved by Digital signatures in cryptography. Researchers have proposed many digital signatures to achieve authentication. A method that allows a group member to make sign on a message on behalf of the group anonymously, is known as Group signature scheme (GSS). This concept was firstly introduced by David Chaum in 1991.

Digital Signatures

I agree

efcc61c1c03db8d8ea8569545c073c814a0ed755

My place of birth is at Gwalior.

fe1188eecd44ee23e13c4b6655edc8cd5cdb6f25

I am 62 years old.

0e6d7d56c4520756f59235b6ae981cdb5f9820a0

I am an Engineer.

ea0ae29b3b2c20fc018aaca45c3746a057b893e7

I am a Engineer.

01f1d8abd9c2e6130870842055d97d315dff1ea3

- These are digital signatures of same person on different documents

---

- Digital Signatures are numbers
- They are document content dependent

CRYPTOGRAPHY

- Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”.
- In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

- In today’s age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

....

- This means if one block in one chain was changed, it would be immediately apparent it had been tampered with. If hackers wanted to corrupt a blockchain system, they would have to change every block in the chain, across all of the distributed versions of the chain.
- Blockchains such as Bitcoin and Ethereum are constantly and continually growing as blocks are being added to the chain, which significantly adds to the security of the ledge

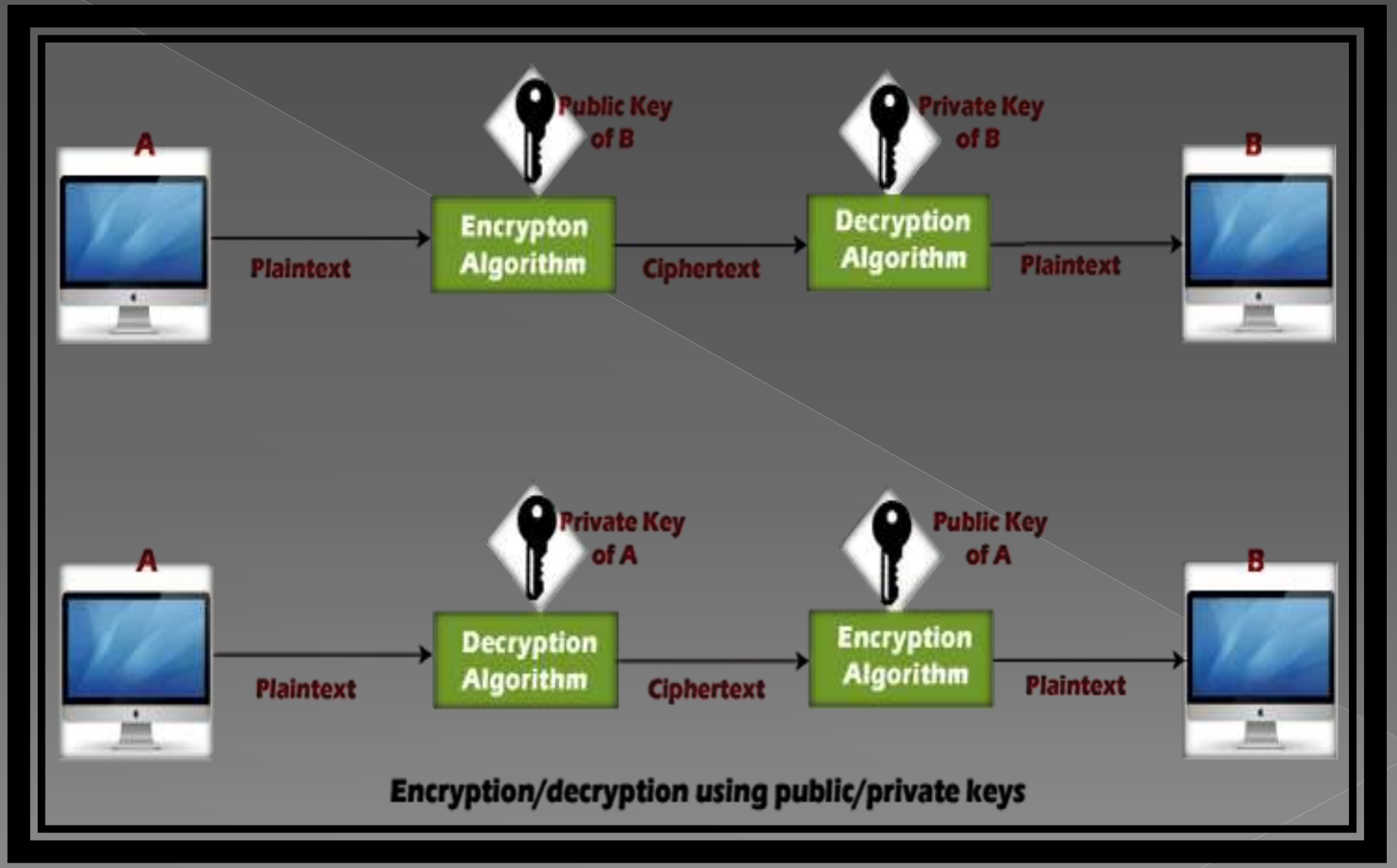
FEATURES OF CRYPTOGRAPHY ARE AS FOLLOWS

- **Confidentiality:**
  Information can only be accessed by the person for whom it is intended and no other person except him can access it.
- **Integrity:**
  Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
- **Non-repudiation:**
  The creator/sender of information cannot deny his or her intention to send information at later stage.
- **Authentication:**
  The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

TYPES OF CRYPTOGRAPHY:

- **Symmetric Key Cryptography:**
  It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).
- **Hash Functions:**
  There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.
- **Asymmetric Key Cryptography:**
  Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

The Public key algorithm operates in the following manner:

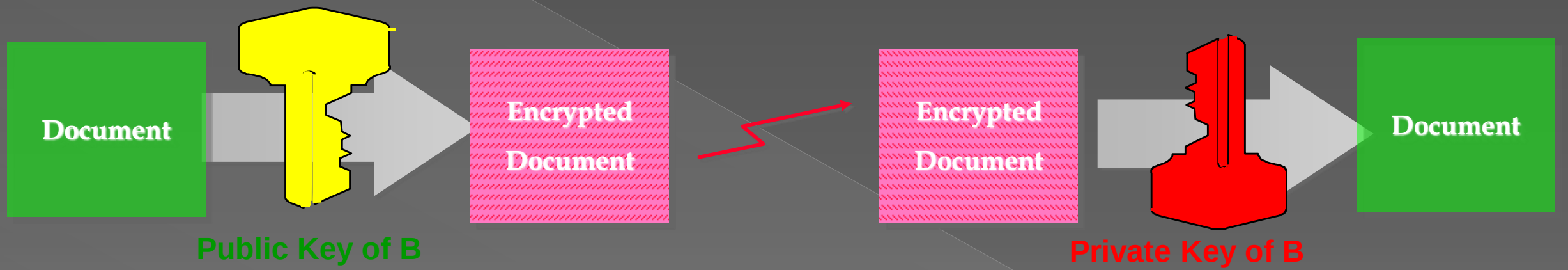


..

The data to be sent is encrypted by sender **A** using the public key of the intended receiver
B decrypts the received ciphertext using its private key, which is known only to B. B replies to A encrypting its message using A's public key.
A decrypts the received ciphertext using its private key, which is known only to him.

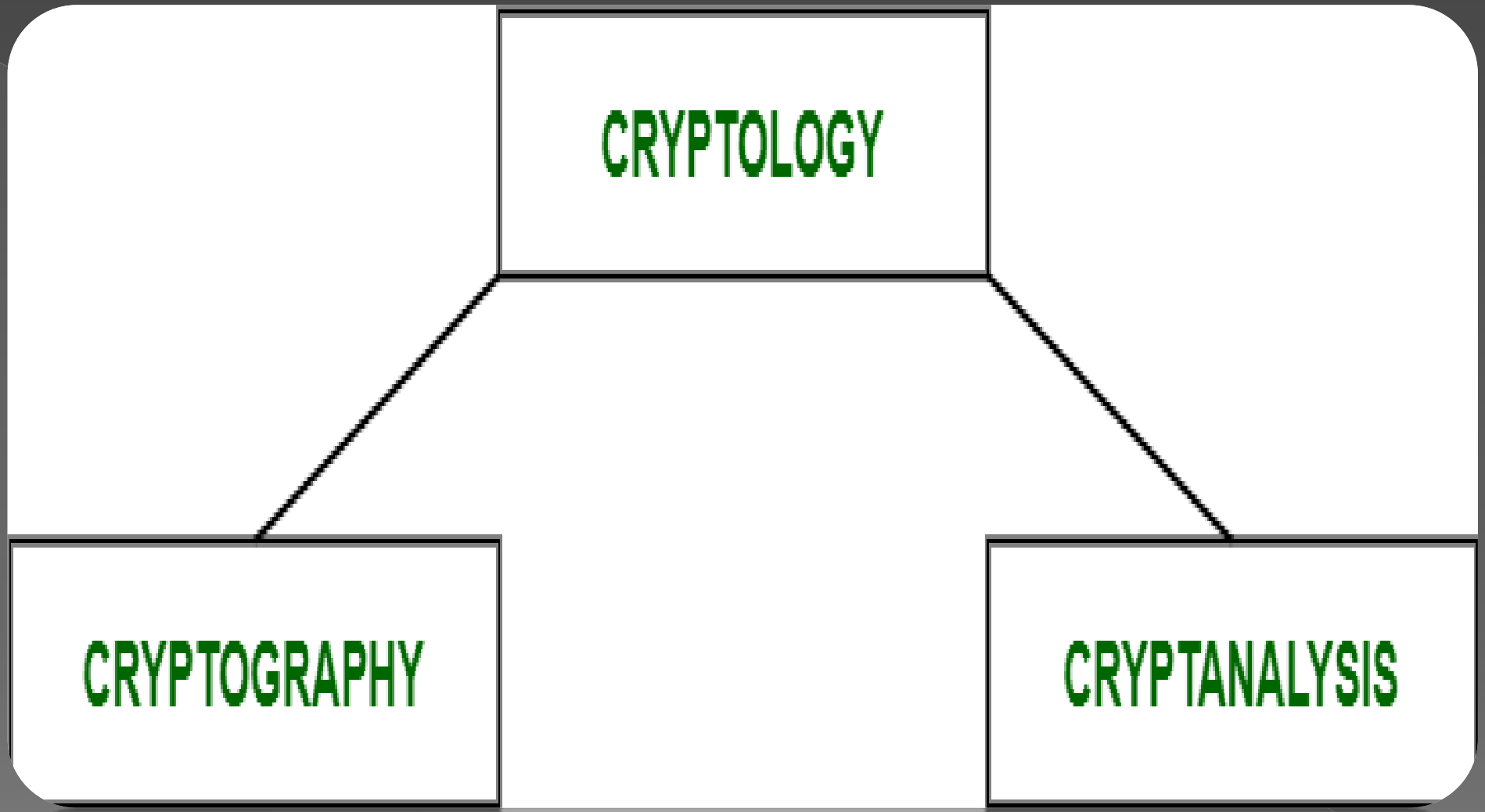
Public Key Cryptography
Encryption Technologies

Confidentiality



CRYPTANALYSIS

- Cryptology has two parts namely, cryptography which focuses on creating secret codes and cryptanalysis which is the study of the cryptographic algorithm and the breaking of those secret codes.
- The person practicing cryptanalysis is called a cryptanalyst. It helps us to better understand the cryptosystems and also helps us improve the system by finding any weak point and thus work on the algorithm to create a more secure secret code.
- For example, a cryptanalyst might try to decipher a cipher text to derive the plaintext. It can help us to deduce the plaintext or the encryption key.


CRYPTOLOGY
CRYPTOGRAPHY
CRYPTANALYSIS

TYPES OF CRYPTANALYTIC ATTACKS

- **Known-Plaintext Analysis (KPA) :**
  In this type of attack, some plaintext-ciphertext pairs are already known. Attacker maps them in order to find the encryption key. This attack is easier to use as a lot of **Chosen-Plaintext Analysis (CPA) :**
  In this type of attack, the attacker chooses random plaintexts and obtains the corresponding ciphertexts and tries to find the encryption key. Its very simple to implement like KPA but the success rate is quite low information is already available.

..

- **Ciphertext-Only Analysis (COA) :**
  In this type of attack, only some cipher-text is known and the attacker tries to find the corresponding encryption key and plaintext. Its the hardest to implement but is the most probable attack as only ciphertext is required.
- **Man-In-The-Middle (MITM) attack :**
  In this type of attack, attacker intercepts the message/key between two communicating parties through a secured channel
- **Adaptive Chosen-Plaintext Analysis (ACPA) :**
  This attack is similar CPA. Here, the attacker requests the cipher texts of additional plaintexts after they have ciphertexts for some texts.

WHAT IS BLOCKCHAIN?

- Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system.
- A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger. The decentralised database managed by multiple participants is known as Distributed Ledger Technology (DLT).
- Blockchain is a type of DLT in which transactions are recorded with an immutable cryptographic signature called a hash.

BENEFITS OF BLOCKCHAIN

- Here's a list of key benefits you can expect to achieve when adopting Blockchain technology into your business:
- It is an immutable public digital ledger, which means when a transaction is recorded, it cannot be modified
- Due to the encryption feature, Blockchain is always secure
- The transactions are done instantly and transparently, as the ledger is updated automatically
- As it is a decentralized system, no intermediary fee is required
- The authenticity of a transaction is verified and confirmed by participant

KEY CHALLENGES IN BLOCKCHAIN

- Undoubtedly, many business leaders, organizations, and policymakers are ready to adopt this technology. Still, there are a few sets of challenges that are responsible for the slow adoption of this technology. Out of all, here, we have listed the critical problems associated with this technology.

SCALABILITY

- The first and major issue related to its adoption is its scalability. Though transaction networks are capable of processing thousands of transactions per second without any failure, when it comes to Bitcoin (roughly, 3 to 7 transactions per second,) and Ethereum (15 to 20 transactions), there is a remarkable slowdown in processing the transactions, making Blockchain unviable for large-scale applications.

INTEROPERABILITY

- Interoperability is the second big issue that needs to be addressed, as this is one of the core reasons why organizations are still not adopting this technology. Most of the blockchains work in silos and do not communicate with other peer networks as they are incapable of sending and receiving information from another blockchain-based system.
- To overcome, various projects have landed up to eradicate this problem. Ark uses SmartBridges architecture to bridge the gap of communication between the networks. This project claims to offer universal transmission and transfer, offering global interoperability

.....

- **ENERGY CONSUMPTION**
- The technology works on the Proof-of-Work mechanism to validate transactions and to ensure trust to add them to the network. This mechanism requires a lot of computational power to solve complex mathematical puzzles to process, verify, and, most importantly, to secure the entire network.
- To overcome this issue, the Co-Founder of Ethereum is come up with the solution to switch Proof-of-Work to Proof-of-Stake. With this mechanism in practice, participants need not solve complex puzzles, thus reducing a lot of energy consumption.
- **LACK OF TALENT**
- The demand for blockchain professionals is increasing without a pause, but high-quality talents can be seen as a major challenging factor in the adoption of this technology. As of 2019, the global demand for blockchain engineers is above 517% over the last year.

LACK OF STANDARDIZATION

- What standardization does Blockchain follow is a question that is still unanswered? Despite a wide variety of networks that exist, there is no universal standard yet. The lack of standardization arises issues such as interoperability, increased costs, and difficult mechanisms, making mass adoption an impossible task. As blockchain technology follows no standard version, it is acting as a barrier for the entry of new developers and investors as well.
- Apart from the challenges mentioned above, cost, security, and privacy are the other challenging factors for large scale implementations.

FUTURE SCOPE

- Though financial services are the early adopters, other sectors will definitely adopt this fantastic technology.
- The integration of Blockchain with AI will make Blockchain more secure and its platform user-friendly.
- Career opportunities in this domain are growing to increase at an alarming rate.
- Integration with new-age technology like IoT will help in building secure infrastructure.
- Enterprise Blockchain will continue to mature and develop, leading to high job prospects and good pay.

ISSUES

- The current architecture of the blockchain is high on energy consumption and also has problems with scaling .
- The root problem is that all transaction in the blockchain have to be processed by basically everyone and everyone must have a copy the global ledger.
- Blockchains are sometimes inefficient.
- Users are Their Own Bank: Private Key.
- Blockchain cannot go back: Data is immutable.

What is Digital Signature?

- Hash value of a message when encrypted with the private key of a person is his digital signature on that e-Document
  - Digital Signature of a person therefore varies from document to document thus ensuring authenticity of each word of that document.
  - As the public key of the signer is known, anybody can verify the message and the digital signature

Digital Signatures

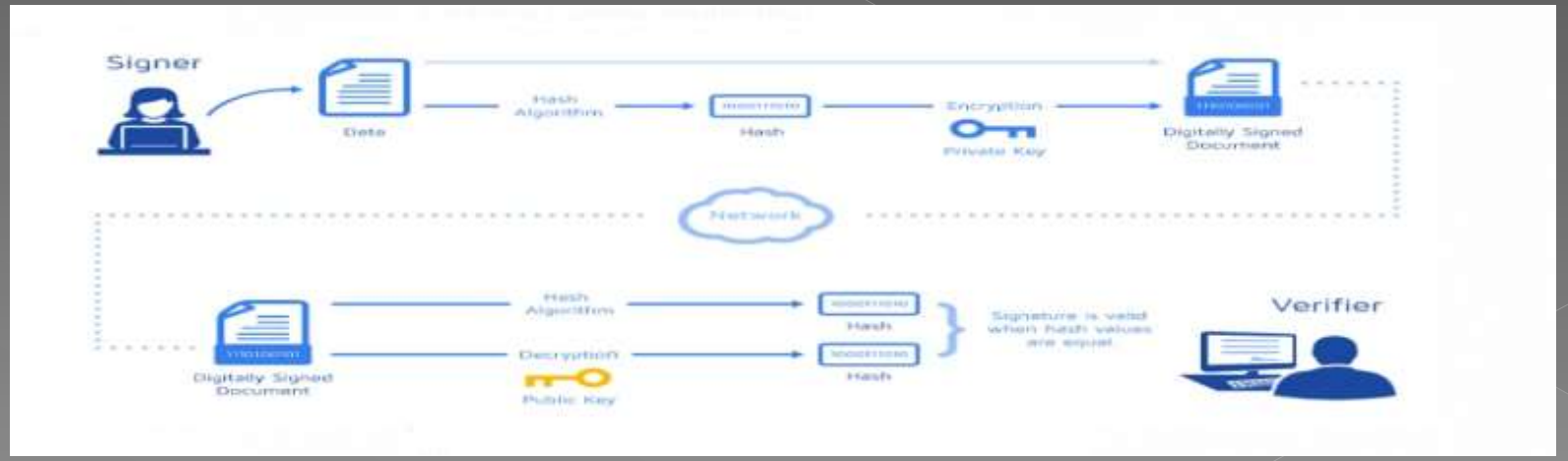
Each individual generates his own key pair
[Public key known to everyone & Private key only to the owner]

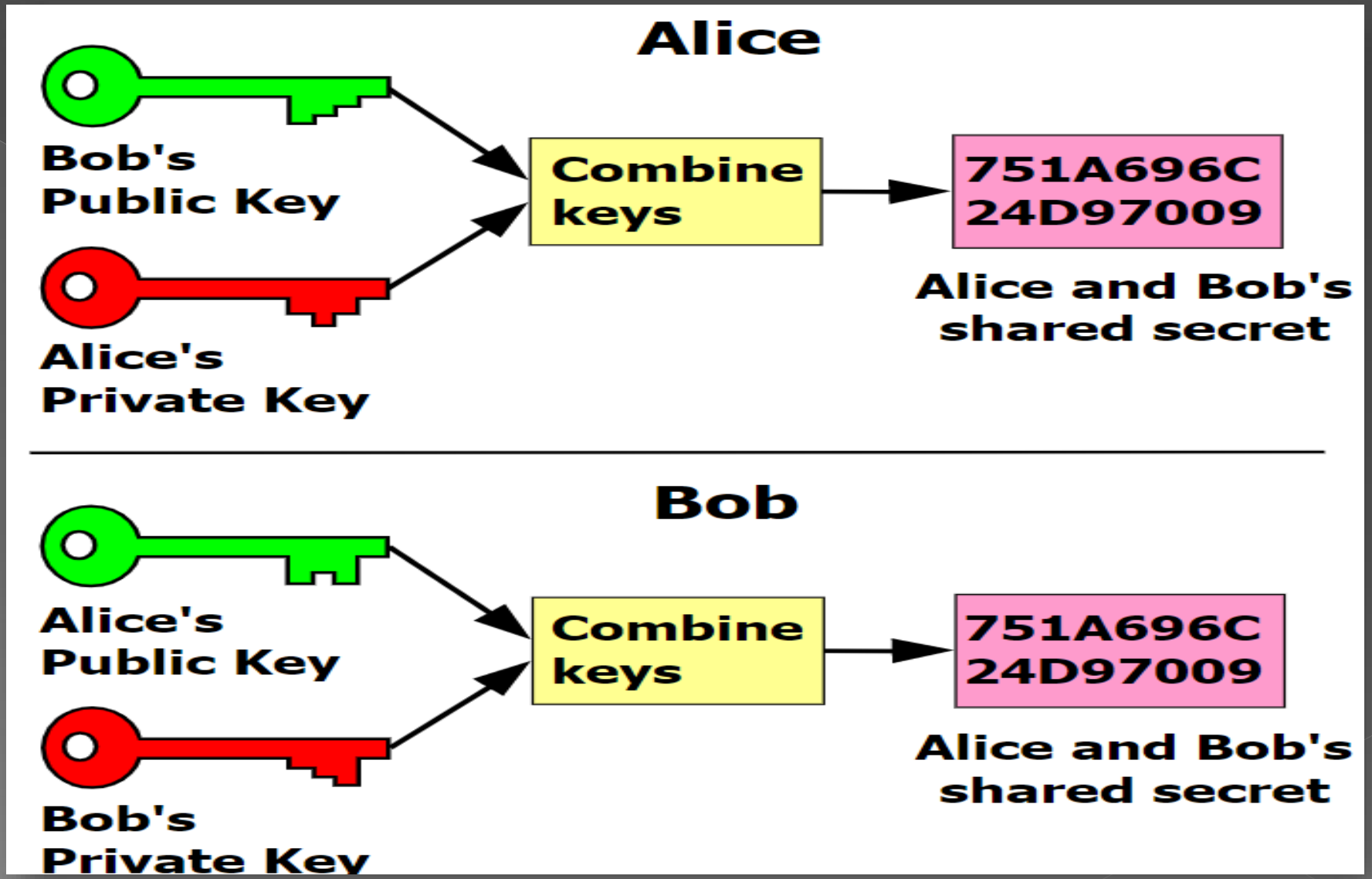
Private Key – Used for making digital signature

Public Key – Used to verify the digital signature

DIGITAL SIGNATURES

- **Digital signatures are messages that identify and authenticate a particular person as the source of the electronic message; and indicate such person's approval of the information contained in the electronic message (Policy and Communications Staff, 2000).**
- **They help users to achieve basic security building blocks such as identification, authentication, and integrity.**




Alice
Bob's
Public Key
Alice's
Private Key
Combine
keys
751A696C
24D97009
Alice and Bob's
shared secret
Bob
Alice's
Public Key
Bob's
Private Key
Combine
keys
751A696C
24D97009
Alice and Bob's
shared secret

Signed Messages

Message

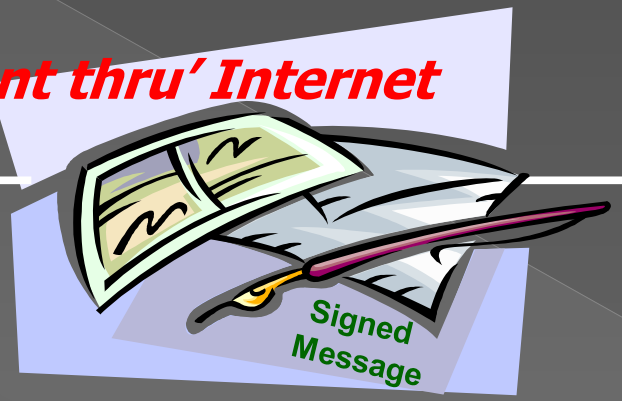
Message + signature

Hash

SIGN hash With *Sender's Private key*

Sender

Sent thru' Internet



Message + Signature

Calculated Hash

COMPARE

if OK Signatures verified

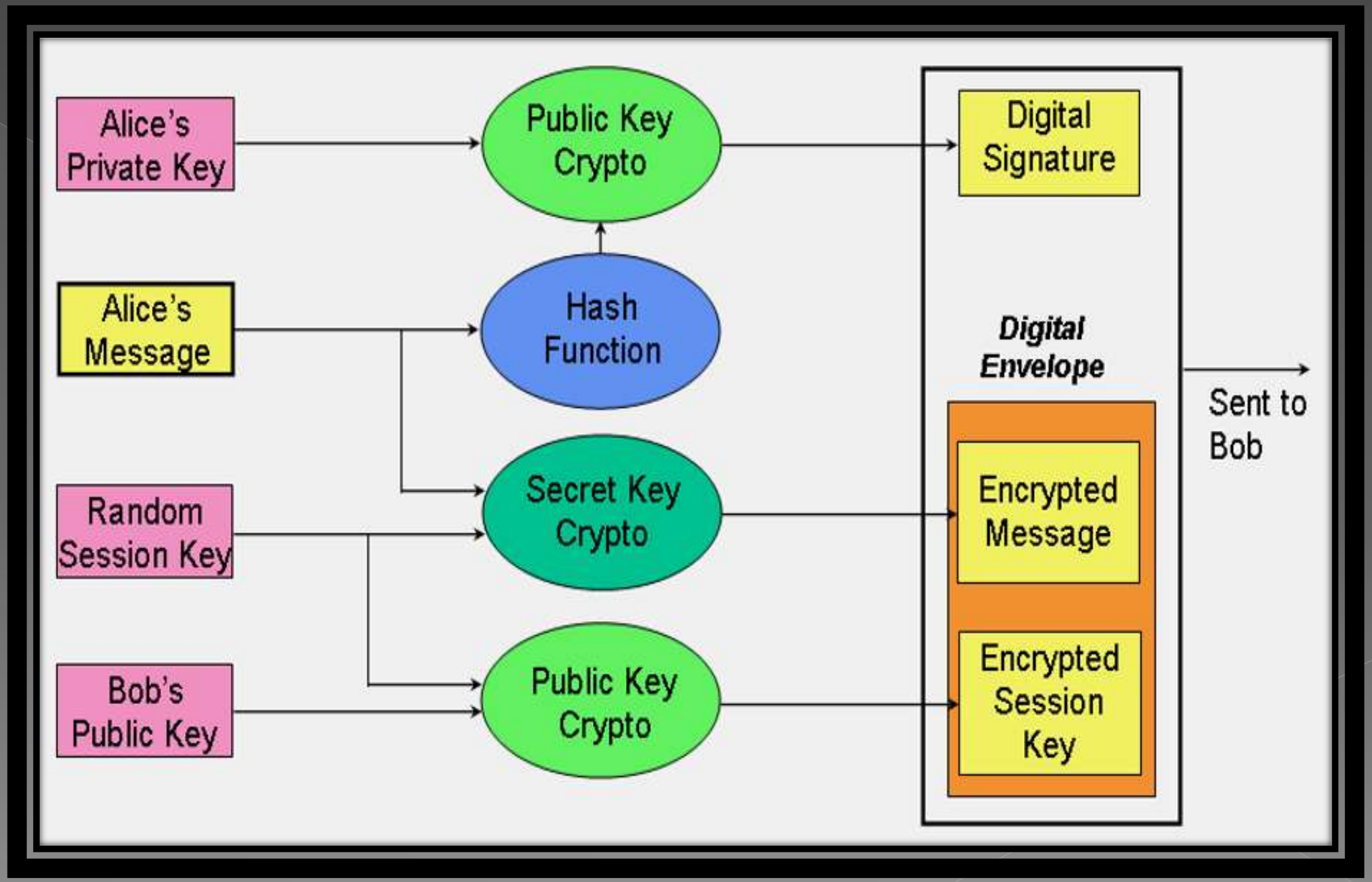
Hash

Decrypt Signature With *Sender's Public Key*

Receiver

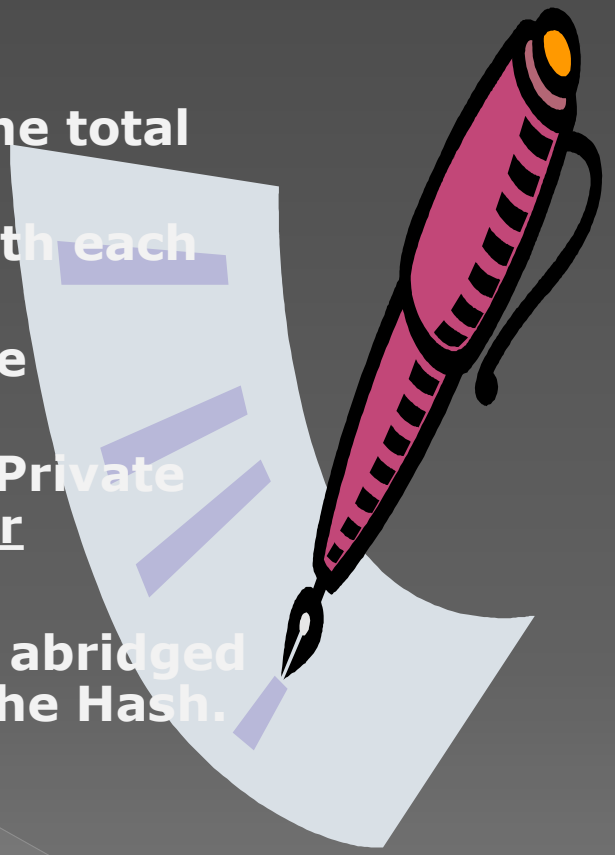
. . .

- Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.
- Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.
- In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high.


Alice's Private Key
Public Key Crypto
Digital Signature
Alice's Message
Hash Function
Digital Envelope
Sent to Bob
Random Session Key
Secret Key Crypto
Encrypted Message
Bob's Public Key
Public Key Crypto
Encrypted Session Key

Concepts

- A 1024 bits number is a very big number much bigger than the total number of electrons in whole world.
- Trillions of Trillions of pairs of numbers exist in this range with each pair having following property
  - A message encrypted with one element of the pair can be decrypted ONLY by the other element of the same pair
- Two numbers of a pair are called keys, the Public Key & the Private Key. User himself generates his own key pair on his computer



- Any message irrespective of its length can be compressed or abridged uniquely into a smaller length message called the Digest or the Hash.
- Smallest change in the message will change the Hash value

Click for Hash Generation

IMPORTANCE OF DIGITAL SIGNATURE

- Out of all cryptographic primitives, the digital signature using public key cryptography is considered as very important and useful tool to achieve information security.
- Apart from ability to provide non-repudiation of message, the digital signature also provides message authentication and data integrity−
- Message authentication − When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.
- Data Integrity − In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.
- Non-repudiation − Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.
- By adding public-key encryption to digital signature scheme, we can create a cryptosystem that can provide the four essential elements of security namely − Privacy, Authentication, Integrity, and Non-repudiation.

HOW DIGITAL SIGNATURE WORKS ?

- *Digital signatures are created and verified by using public key cryptography, also known as asymmetric cryptography. By the use of a public key algorithm, such as RSA, one can generate two keys that are mathematically linked- one is a private key, and another is a public key.*
- *The user who is creating the digital signature uses their own private key to encrypt the signature-related document. There is only one way to decrypt that document is with the use of signer's public key.*
- *This technology requires all the parties to trust that the individual who creates the signature has been able to keep their private key secret. If someone has access the signer's private key, there is a possibility that they could create fraudulent signatures in the name of the private key holder.*

THE STEPS WHICH ARE FOLLOWED IN CREATING A DIGITAL SIGNATURE ARE:

- Select a file to be digitally signed.
- The hash value of the message or file content is calculated. This message or file content is encrypted by using a private key of a sender to form the digital signature.
- Now, the original message or file content along with the digital signature is transmitted.
- The receiver decrypts the digital signature by using a public key of a sender.
- The receiver now has the message or file content and can compute it.
- Comparing these computed message or file content with the original computed message. The comparison needs to be the same for ensuring

MERITS

- Time management
- Cost management
- Increased contract speed
- Enhanced document security
- Enhance customer relationships
- Long term retention and access
- Global acceptance and legal compliance
- Track the status of your document in real time digital signature

DEMERITS

- A digital signature will be highly dependent on the technology used to create it.
- To use digital signatures, you have to purchase digital certificates that can be quite pricey.
- Once the user sends the message there is no undo for them. So user must be specific to whom the are sending.
- The private key must be kept in a secure manner.
- Signature requires considerable amount of time.
- Sender and receiver have to use same network and has to secure their private and public key.

APPLICATIONS OF DIGITAL SIGNATURE

- To send and receive encrypted emails, that are digitally signed and secured
- To carry out secure online transactions
- To identify participants of an online transaction
- To apply for tenders, efiling with Registrar of Companies (MCA), efiling of income tax returns and other relevant applications
- To sign and validate Word, Excel and PDF document formats

FUTURE SCOPE OF PROJECT

- In the Future, Digital Signatures Will Play an Integral Role in Helping **to Secure Electronic Commerce**. **E-commerce** is the act of selling, buying, and exchanging goods and services over an electronic network; for instance, the internet.
-
- There has been a constant need for data security during the transmission of sensitive information. Due to the e-commerce and online banking boom, companies needed to secure their networks to gain confidence in customers. This has led to greater and faster rate of adoption rates of digital signatures, which act as the sender's personal seal of authenticity over any electronic document.
- With the evolution of technology, the way of executing documents has also evolved. With the increasing demand for modern, convenient methods for entering binding transactions, electronic agreements and digital signatures have gained a lot of momentum in recent years. Such developments have significantly changed how these transactions are entered and the execution processes.

- Younger consumers have also been a driving force behind the rise in digital signatures in the financial services industry. Various Gen Z and Millennials across the world have signed financial documents, such as **opening a bank account, loan agreement, investment, wealth management, mortgage agreements during the pandemic, which has resulted in a burgeoning of digital signature demand**. Also, government agencies, like the DMV and immigration, have also provided more e-signature support for the critical documents.
- With the outbreak of COVID-19, the digital signature market is anticipated to exhibit a positive growth rate due to the rise in remote working that has shifted the focus from relying on paper-based documentation and increasing digitalization of the transaction process. Enterprises are seeking business methods that are seamless and efficient and can be done from anywhere. Enterprises are also considering taking document processes online.


Thank
you!