Blockchain Technology

Dr. Preeti Chandrakar
Assistant Professor

Department of Computer Science and Engineering
National Institute of Technology, Raipur
September 2021

Frauds:

Home » india news » Uttar Pradesh: Beware of frauds selling insurance policy online, fake call centre busted, 14 women involved

Uttar Pradesh: Beware of frauds selling insurance policy online, fake call centre busted, 14 women involved

SPEED NEWS DESK | Updated on: 26 July 2021, 7:47 IST

"The accused used to collect the data of insurance policy holders whose policies were on the verge of maturity. The gang then used to convince the gullible policyholders not to encash the money and extent the policy for which they would get more incentives and loans," Superintendent of Police Amit Pathak said.

INDIA NEWS

In Gurugram, fake insurance claim unravels racket

The insurance fraud was discovered by chance, after possibly a few hundred claims, because of an insurance policy that was linked to three others.

By Leena Dhankhar, Gurugram
UPDATED ON JUL 03, 2021 01:08 AM IST

The Gurugram Police said a gang of six is behind the fraud, built around stolen insurance data, forged death certificates, hundreds of bank accounts, and fake claims.(Virendra Singh Gosain/HT File Photo)

PARTNERS IN CRIME

A gang of six may have claimed at least 150 insurance policies in Gurugram through an elaborate fraud, police say

MODUS OPERANDI

DATA STOLEN
Through connections at hospitals, banks and govt depts., the gang got insurance policy details, Aadhaar numbers and other details.

FAKE DEATH CERTIFICATES
The accused created around 300 bank accounts in the name of a patient's nominee and forged death certificates to claim insurance

SAFETY NET
The gang targeted people with policies up to Rs 30 lakh as insurance companies don't carry out physical verification for such claims.

Four of the six accused have been arrested and search is on for the remaining two.

Business News » India News

Fraud by husband-wife in United India Insurance Company: Amount reaches whopping Rs 170 crores- Check details

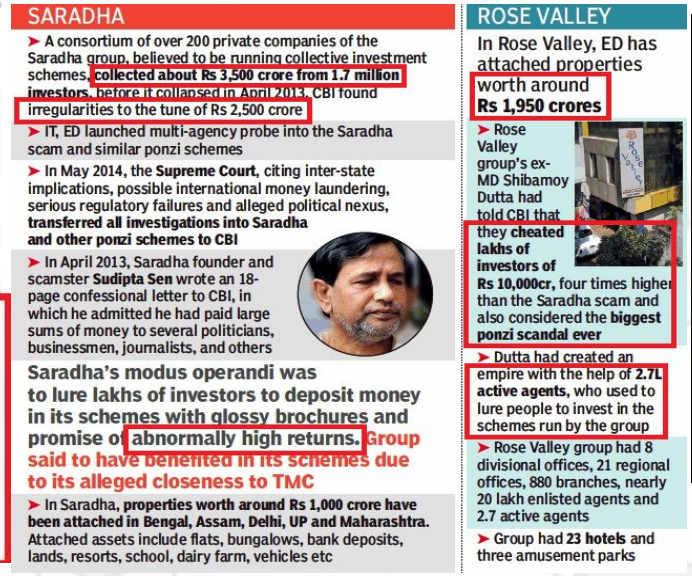
Earlier this month, a couple working in the United India Insurance Company which is a government general insurance company were arrested for a cheating case. Now there has been an update on the matter. The fraud amount by the couple has now reached Rs 170 Crores.

Earlier this month, a couple working in the United India Insurance Company which is a government general insurance company were arrested for a cheating case. Now there has been an update on the matter. The fraud amount by the couple has now reached Rs 170 Crores.

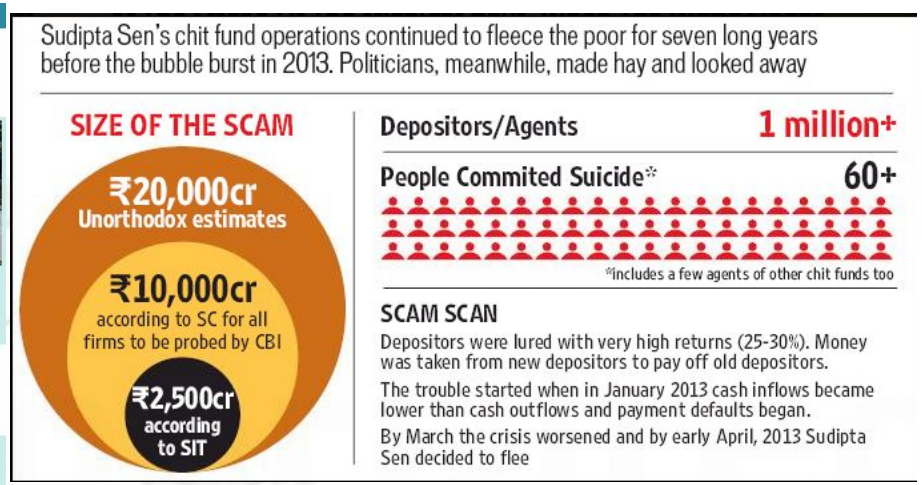
During the investigation conducted by the economic offences wing (EOW) it has been found that in 70 accounts, Rs 170 crores have been transferred. The reason behind noticing the scam so late is that the husband was working in the accounts department and the wife in the IT department, and she used to change the entry in the records.

Scams

http://indpaedia.com/ind/index.php/Saradha_Scam



http://indpaedia.com/ind/index.php/Saradha_Scam



http://www.twenty22.in/2014/05/cbi-to-probe-saradha-scam.html

Crown Ponzi scheme: Jagjit faced 400 FIRs

- Jagjit Singh's firm began operations in 2011-12, promising to double investors' money in three years. It shut shop in early 2014
- Thousands of investors from North were duped not once but several times as accused floated 7 firms one after another. Two investors had died by suicide
- The Punjab Police had formed an SIT in 2016 on the orders of the Punjab and Haryana High Court
- Following protests, nearly 400 FIRs were clubbed together for probe by the Crime Branch. The ED was holding a separate inquiry

https://www.tribuneindia.com/news/punjab/fugitive-md-held-for-10k-cr-chit-fund-scam-399889

Bhubaneswar: Chit fund fraud held in Vrindavan for Rs 1.5 crore scam

Debabrata Mohapatra / TNN / Updated: May 21, 2022, 08:35 IST

https://timesofindia.indiatimes.com/city/bhubaneswar/chit-fund-fraud-held-for-1-5-crore-scam/articleshow/91697953.cms

Woman held in Rs 7 crore chit fund scam

The accused persons being the directors of the Bhubaneswar-based company had lured gullible people to invest money in their company for higher interests by investing the amount in share market for lucrative profit.

https://www.thestatesman.com/cities/bhubaneshwar/woman-held-rs-7-crore-chit-fund-scam-1503068856.html

Odisha: Firm dupes over 500 investors of Rs. 10crore in chit fund scam

Debabrata Mohapatra / TNN / Updated: Feb 2, 2022, 13:24 IST

https://timesofindia.indiatimes.com/city/bhubaneswar/chit-fund-scam-firm-dupes-over-500-investors-of-10cr/articleshow/89286024.cms

Scams

West Bengal: ED attaches assets worth Rs 5 crore of journalist Suman Chattopadhyay in 'chit fund scam'

Journalist Suman Chattopadhyay allegedly received funds from the I-Core group under the guise of business investment.

https://www.newslaundry.com/2022/04/01/west-bengal-ed-attaches-assets-worth-rs-5-crore-of-journalist-suman-chattopadhyay-in-chit-fund-scam

Fugitive in ₹500-crore chit fund scam arrested in Odisha

Satyasundar Barik

BHUBANESWAR MARCH 31, 2022 14:54 IST
UPDATED: MARCH 31, 2022 14:54 IST

https://www.thehindu.com/news/national/other-states/fugitive-in-500-crore-chit-fund-scam-arrested-in-odisha/article65277291.ece

CBI files chargesheet against 13 in Guwahati chit fund scam of Rs 238 crore

It is alleged that the accused collected a huge amount of money from people with an assurance to pay back with lucrative interest without any guarantor and permission of RBI/SEBI.

https://www.indiatoday.in/india/story/chit-fund-scam-guwahati-chit-fund-case-cbi-files-chargesheet-private-companies-1910339-2022-02-08

CBI arrests TMC leader Pranab Chatterjee in Rs 3.74 crore chit fund scam

The TMC leader was held for allegedly siphoning off money from a trust running the scheme

https://www.business-standard.com/article/current-affairs/cbi-arrests-tmc-leader-pranab-chatterjee-in-rs-3-74-crore-chit-fund-scam-121121001302_1.html

ED attaches assets worth Rs 300 cr of Icore Group in chit fund scam case

The Enforcement Directorate on Tuesday provisionally attached assets worth Rs 300 Crore under PMLA, 2002 in its ongoing investigation against Icore Group of companies in a chit fund scam case

https://www.business-standard.com/article/current-affairs/ed-attaches-assets-worth-rs-300-cr-of-icore-group-in-chit-fund-scam-case-121092900097_1.html

Scams

Rose Valley regional manager arrested over Rs 2.82 crore chit fund scam in Odisha

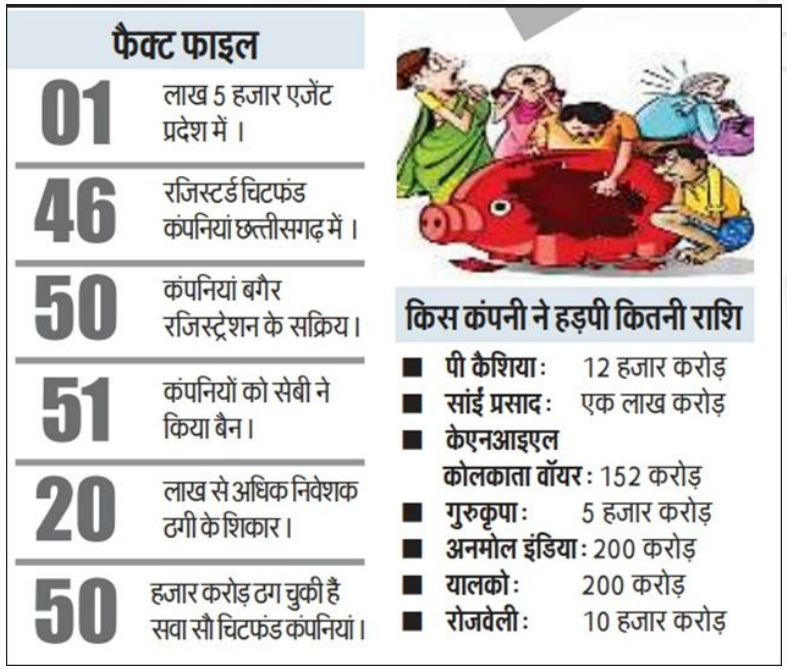
Investigations revealed Rose Valley Group of Companies, registered with Registrar of Companies at Kolkata, had collected crores of rupees from unsuspecting depositors across Odisha

https://www.newindianexpress.com/states/odisha/2021/aug/03/rose-valley-regional-manager-arrested-over-rs-282-crore-chit-fund-scam-in-odisha-2339590.html

Kolkata Police unearth Rs 2k crore chit fund scam

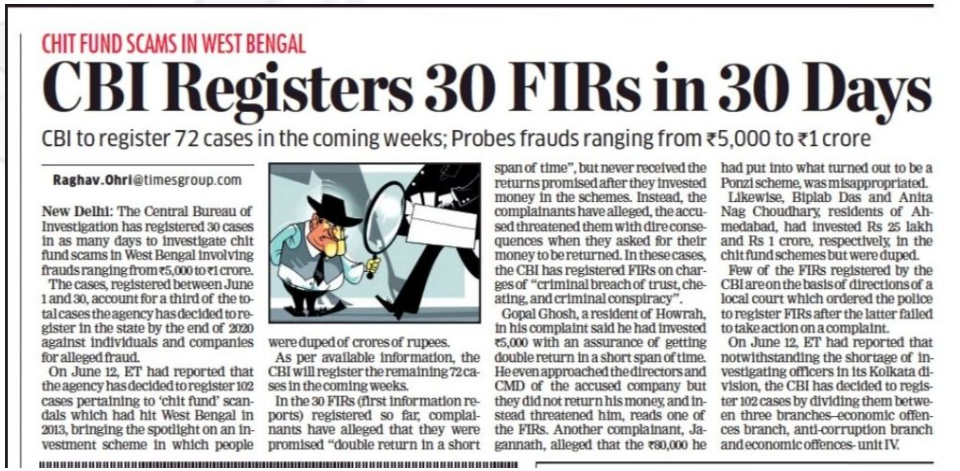
Saturday, 23 April 2022 | Pioneer News Service | Kolkata

https://www.dailypioneer.com/2022/india/kolkata-police-unearth-rs-2k-crore-chit-fund-scam.html



https://www.naidunia.com/chhattisgarh/raipur-125-chit-fund-companies-fraud-of-rs-50000-crore-in-chhattisgarh-2734411

https://www.facebook.com/BhupeshBaghelCG/photos/a.479052125536672/1601529449955595/?_rdr



https://twitter.com/raghavohri0/status/1279987726134030337

Course Objectives

1. The students are expected to understand the architectural components of a blockchain system like Consensus algorithms, Permissioned & Permission less blockchain, Ethereum, Hyperledger, Design a Distributed Application etc.

2. The students are expected to understand smart contracts, their technical capabilities, practical applications, limitations and security constraints they operate within

3. The students are expected to understand forking and the way the Bitcoin network evolves

Applications Of Blockchain

Digital IDs

Bitcoin

Real estate

Voting

Payment and Transfers

Heath Care

Internet of Things

Online music

Banking

Law Enforcement

Block Chain Technology

[7th Semester, Fourth Year]

Course Description Offered by Department	Credits	Status	Code
Block Chain Technology [Pre-requisites: Programming]	3-0-0, (3)	EPR	CS107204CS

Course Objectives

1. The students are expected to understand the architectural components of a blockchain system
2. The students are expected to understand smart contracts, their technical capabilities, practical applications, limitations and security constraints they operate within
3. The students are expected to understand forking and the way the Bitcoin network evolves

Course Content

Unit-1 Introduction to Blockchain:

Basic Cryptographic primitives used in Blockchain , Understand the differences between centralised, decentralised and distributed peer to peer networks, Consensus algorithms and their scalability problems, Definition of Blockchain, History of blockchain, Blockchain 2.0, Types of Blockchain, Public Ledgers, Blockchain as public ledgers, Blockchain Architecture, Markle Root Tree, working of blockchain, , Permissioned Model of Blockchain.

Unit-2 Cryptocurrency and Consensus:

Bitcoin, Bitcoin Transactions, The Chain and the Longest Chain, Cryptocurrency to Blockchain 2.0. Creation of coins, Payments and double spending, Fork, Bitcoin Scripts, Bitcoin P2P Network, Transaction in Bitcoin Network, Block Mining, Distributed Consensus Importance, Distributed consensus in open environments, Consensus in Bitcoin- Bitcoin Consensus, Proof of Work (PoW), Hashcash PoW, Bitcoin PoW, Proof of Stake, Proof of Burn and Proof of Elapsed Time, The life of a Bitcoin Miner, Mining Difficulty, Mining Pool. Byzantine fault tolerant system, Hybrid Consensus, blockchain and future world of Web 3.0.

Unit-3 Platforms and Smart Contracts:

Different Blockchain Platforms: Ethereum, Hyperledger, EOS, IBM Blockchain, CORDA, Ethereum basics: Ethereum Virtual Machine (EVM), Wallets for Ethereum, Ethereum and Smart Contracts, The Turing Completeness of Smart Contract Languages and verification challenges, Using smart contracts to enforce legal contracts, Writing smart contracts using Solidity , Hyperledger fabric, the plug and play platform and mechanisms in permissioned blockchain. Chaincode, Design a Distributed Application (DAPP)

Unit-4 Security and Applications:

Attacks on Blockchains: Sybil attacks, selfish mining, 51% attacks advent of algorand; Sharding based consensus algorithms to prevent these attacks, Attacks on different consensus, Attacks on Smart Contracts. Applications of blockchain in cyber security, integrity information, Applications of blockchain in Healthcare, Financial system, Supply chain management, E-governance, Property records, Micropayments, Notary, Sidechains, Agriculture, Domain Name Service and future of Blockchain,

Course Materials

Course Materials

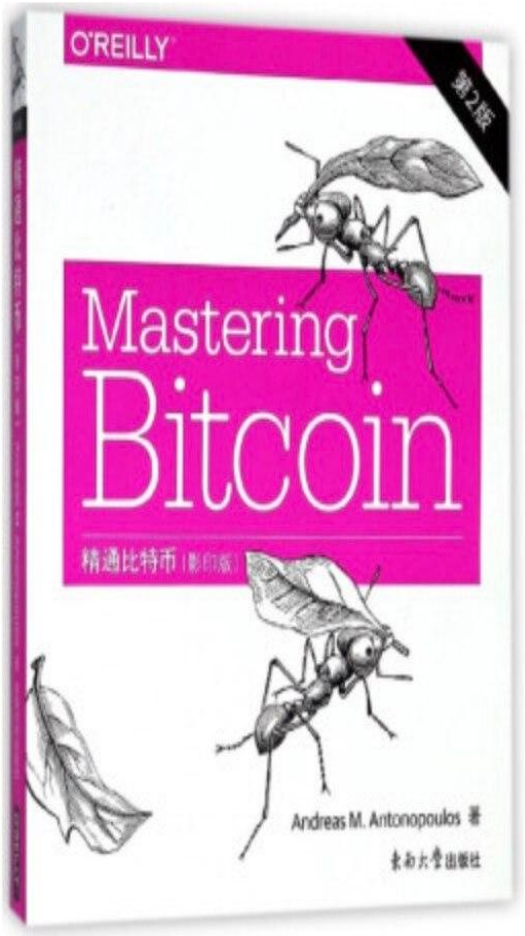
Required Text: Text books

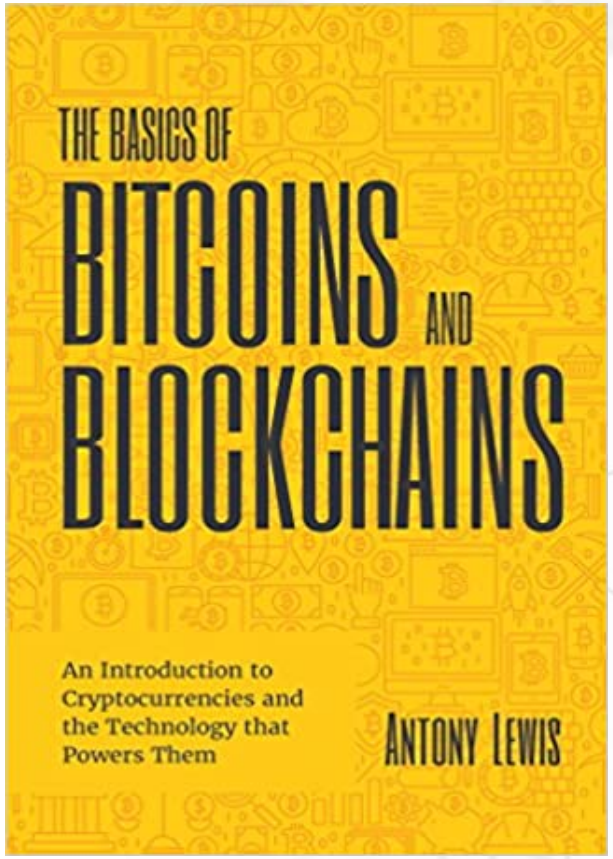
1. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press (July 19, 2016).
2. Blockchain Technology: Cryptocurrency and Applications S. Shukla, M. Dhawan, S. Sharma, S. Venkatesan
3. Oxford University Press 2019
4. Mastering Bitcoin: Unlocking Digital Cryptocurrencies, Antonopoulos

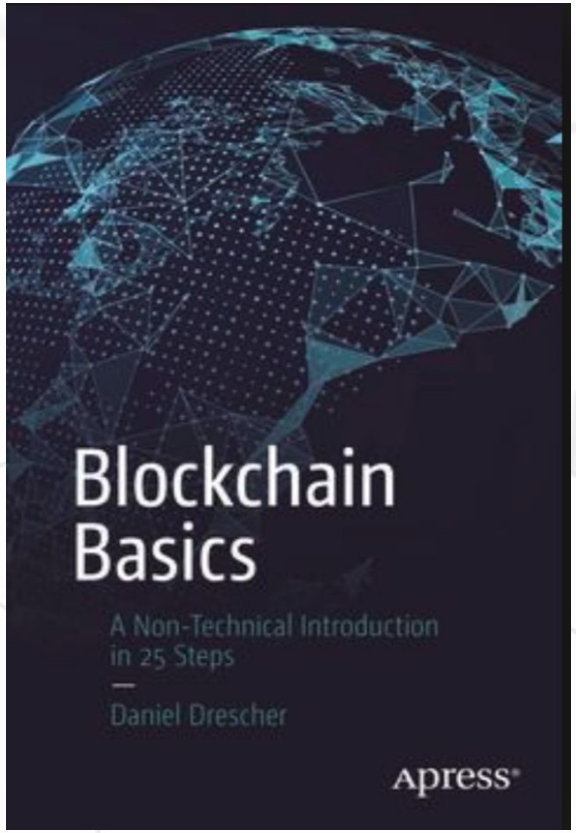
Optional Materials: Reference Books

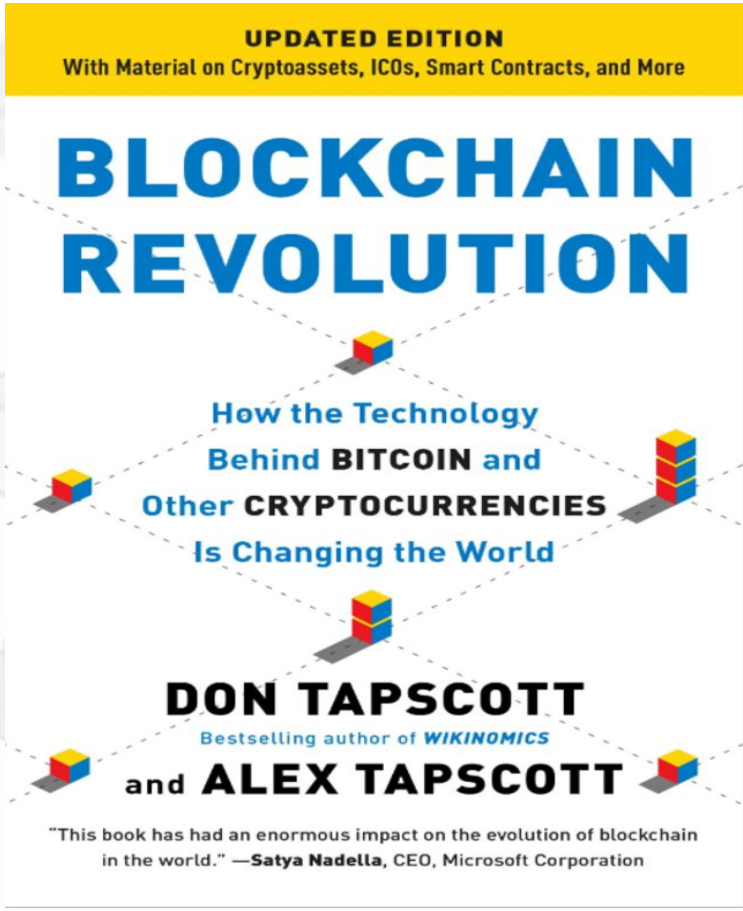
1. Josh Thompson, 'Blockchain: The Blockchain for Beginnings, Guild to Blockchain Technology and Blockchain Programming', Create Space Independent Publishing Platform, 2017.3. Imran Bashir, "Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained", Packt Publishing.

Block chain books



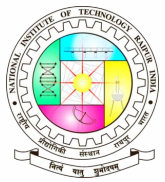






Objective of class

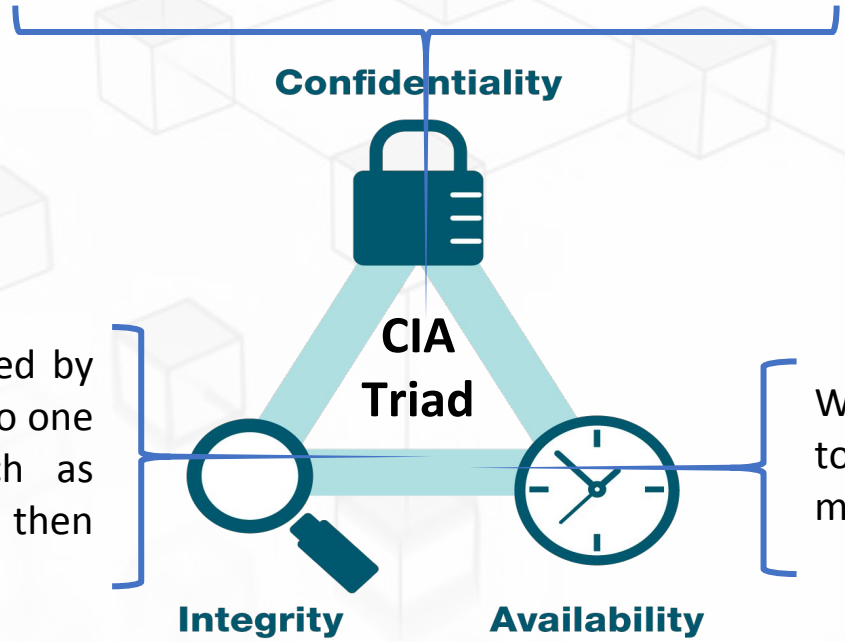
- Fundamentals of Cryptography that are in blockchain
- Hash Function and their properties
- Public Key Cryptosystem
- Digital Signature
- Hash Puzzle
- Hash Pointers
- Markel Data Structure



Fundamentals of Cryptography

- **Why we need cryptography ?**
  - To provide **Confidentiality, Integrity and Availability (CIA triad)** to the message or data that is transmitting from source to destination over the internet.

The message/data is only readable to the receiver or the authenticate person only. No third party or any attacker can read the message.

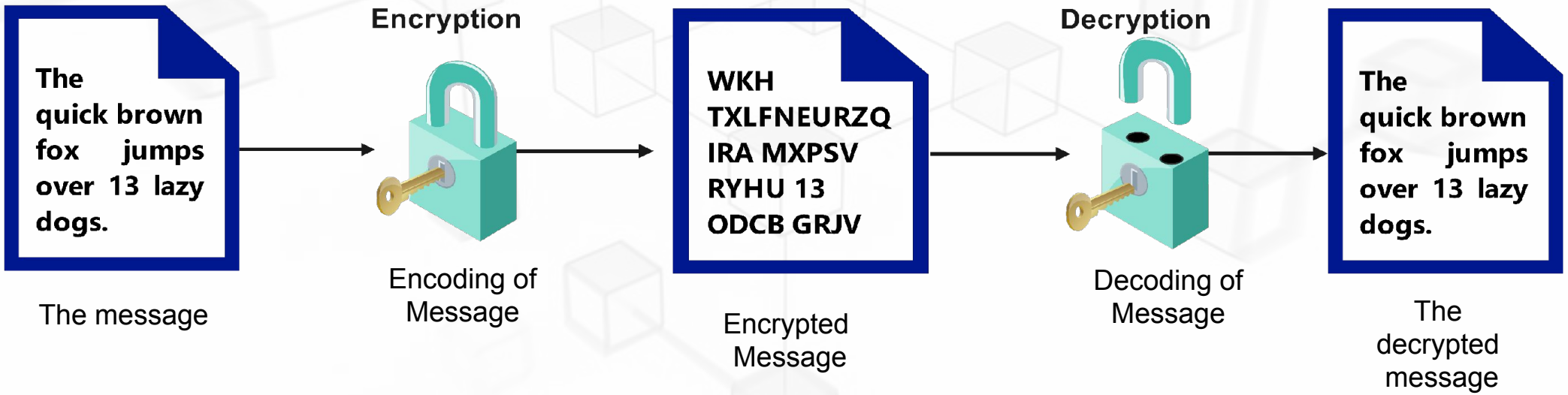


The message/data can be modified by the authenticated user only and no one else, if unauthorized user such as attacker will modify the message then it will be detectable.

When an authorised users wants to access the message or data it must be available to them.

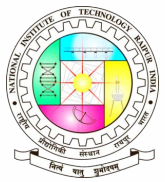
Fundamentals of Cryptography

- **In cryptography normally two related function are there:**
  - Encryption
  - Decryption



Fundamentals of Cryptography

- **Simple text/ Message**
  - The message that can be readable by human without any difficulty.
- **Encryption**
  - The process of encoding the input message with the help of desirable encryption algorithm.
- **Encrypted Message**
  - The message that can not be readable to human without applying the required decryption algorithm.
- **Decryption**
  - The revers process of encoding in which encrypted message is processed required decryption algorithm to get original form of the input message.
- **Cipher**
  - The process of Encryption and Decryption is known as **Cipher**.



Fundamentals of Cryptography

- For a valid encryption and decryption process, following condition must be true

If E(M)==C && D(C)==M

then M=D(E(M))

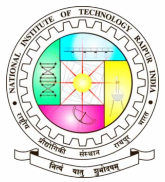
Where:

M = Message

E = Encryption process

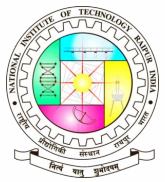
C = Cipher text/ Encrypted text

D = Decryption process



Fundamentals of Cryptography

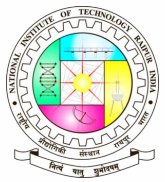
- **Key based encryption and decryption algorithms**
  - All modern Cryptographic algorithms are using key to control encryption and decryption process.
  - The cryptographic algorithms are recognized in two different types based on the symmetry or asymmetry of encryption and decryption key.
  - The keys are using for encryption and decryption are must be secret and only known by the sender and receiver
- **Types of key based cryptosystem**
  1. Symmetric key cryptosystem
  2. Asymmetric key cryptosystem



Fundamentals of Cryptography

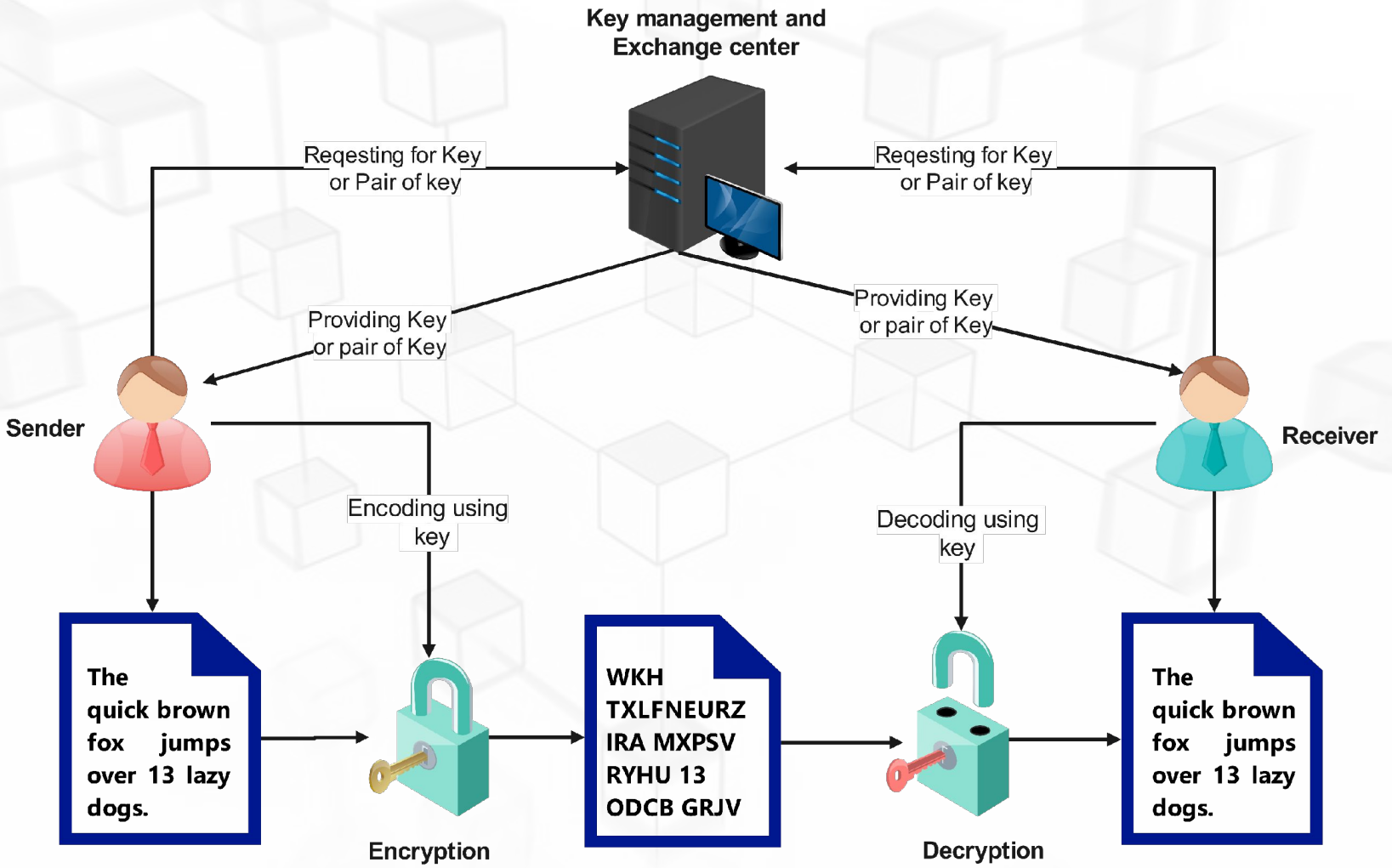
- **Key based cryptosystems involve following steps**

1. **Key generation**
   - In this process a key generation algorithm is used to generate single key(in case of Symmetric key cryptosystem) or a pair of key(Asymmetric key cryptosystem).
   - The keys are generated and handled by key management and exchange authority, present in the network.
2. **Key sharing**
   - After the successfully key generation key exchange authority share the key with the authorized/requested user in network.
3. **Encryption and decryption**
   - Then the provided key or pair of key will used for encryption and decryption by authorized users of the network.



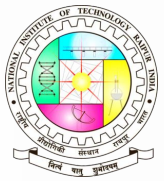
Fundamentals of Cryptography

- **Key based cryptosystems**



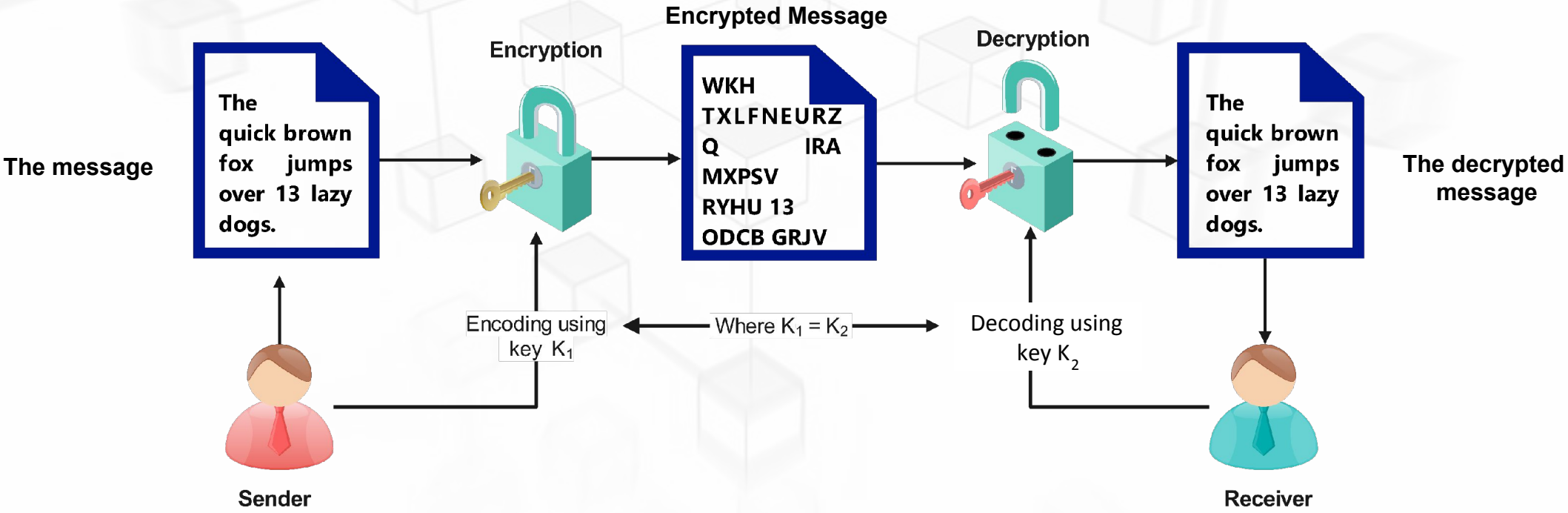
Fundamentals of Cryptography

- **Types of key based cryptosystem**
  1. Symmetric key cryptosystem
  2. Asymmetric key cryptosystem



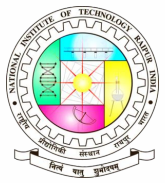
Fundamentals of Cryptography

- **Symmetric key cryptosystem**
  - Also known as single-key cryptography
  - Both the keys are same and can be derived from each other, such that $k_1 = k_2$
  - Both sender and receiver used same key for encrypting and decrypting the message.



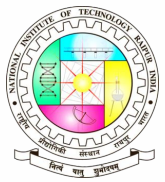
Fundamentals of Cryptography

- Symmetric key cryptography is based on a combination of the substitution and permutation.
- Symmetric key cryptography can apply on stream of bits or block of bits, both process is known as stream ciphers and block ciphers.
- **Stream Ciphers**
  - Operates on the stream of bits.
- **Block ciphers**
  - Operates on the block of bits. (such blocks having ..64/128/256…bits).
- **Examples**
  - AES, DES, IDEA, RC4, Blowfish…..



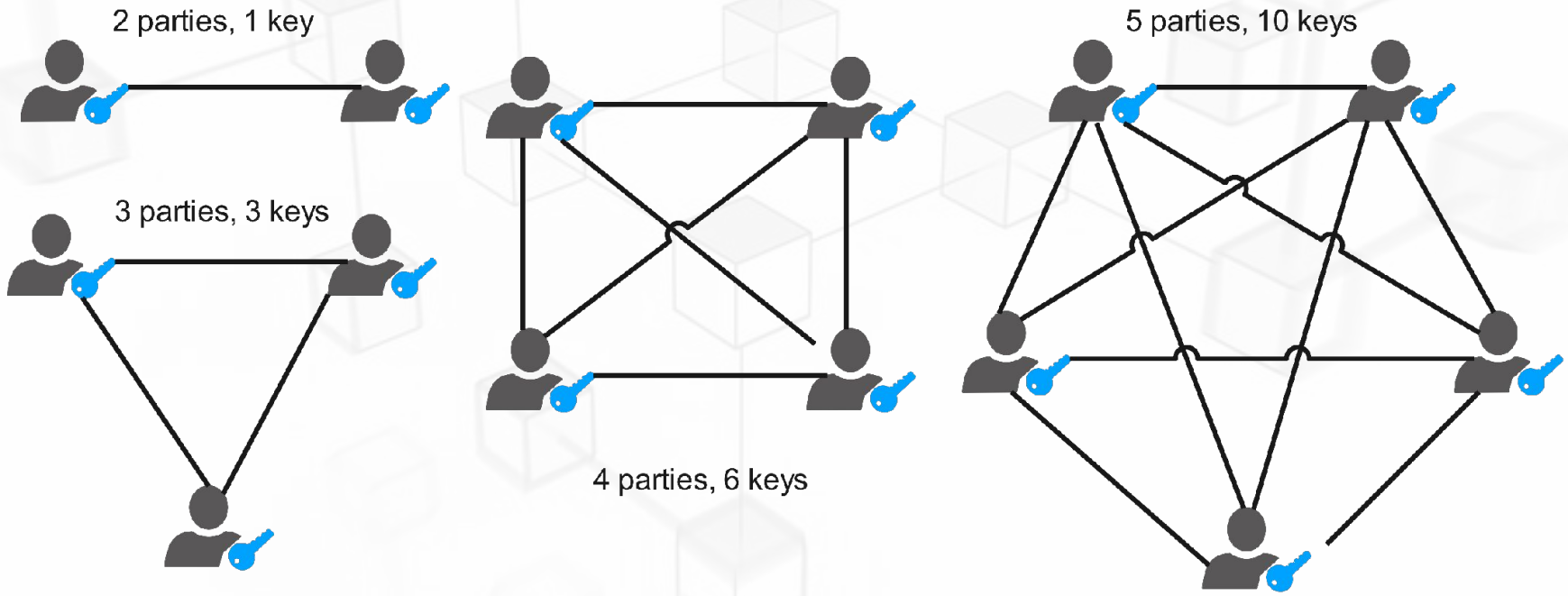
Fundamentals of Cryptography

- **Advantages of Symmetric key cryptosystem**
  - Simple: no need of complex mathematical equations to generate key , encryption and decryption process for a message.
  - Fast: generating only one key which is used in both encryption and decryption process.
  - Assurance from non repudiation: If the message is encrypted by sender then it can not deny that file is not send by him/her.
- **Disadvantages of Symmetric key cryptosystem**
  - Key exchange: The process of exchanging secret key is unreliable, suppose we want to share key over telephone or by mail and if someone monitoring the communicating line then it have the key that will used to decrypt the message and also alter that.
  - Kye management: keys required **K**=(k*(k-1))/2, means number of keys are increasing proportionally to increasing number of percipients.



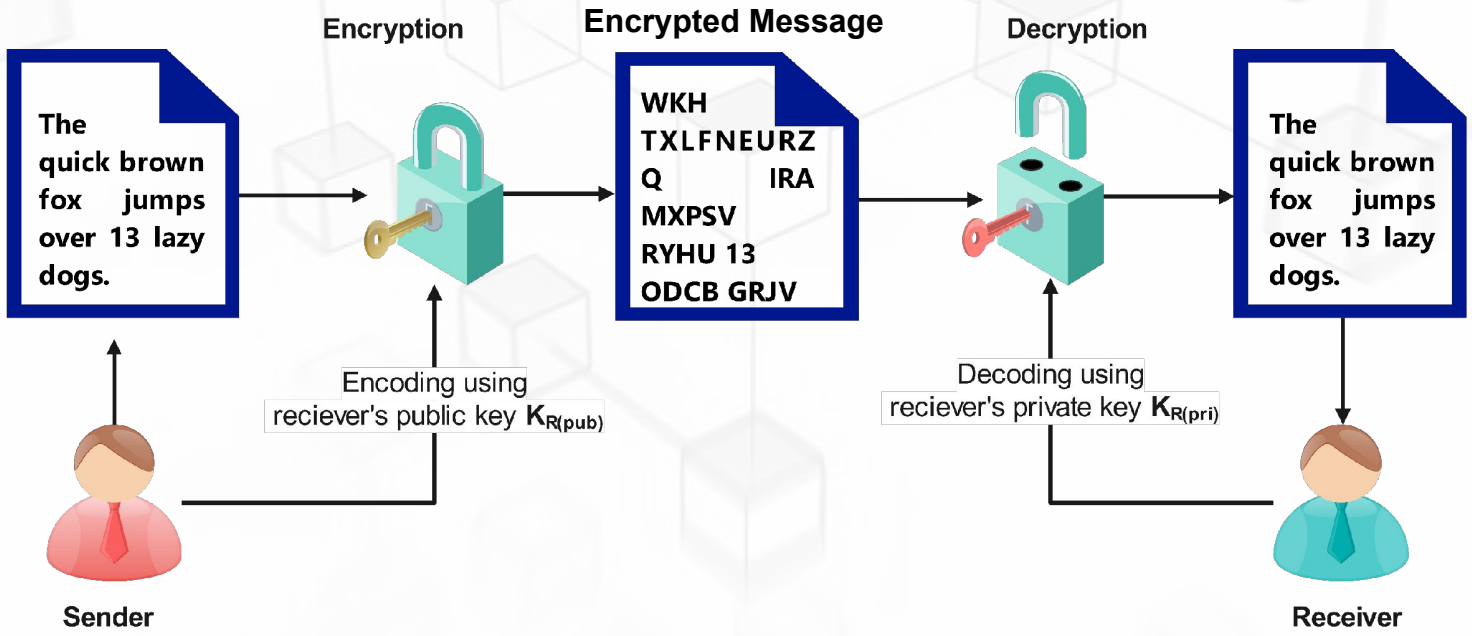
Fundamentals of Cryptography

- **Disadvantages of Symmetric key cryptosystem**
  - Kye management: keys required **K**=(k*(k-1))/2, means number of keys are increasing proportionally to increasing number of percipients.



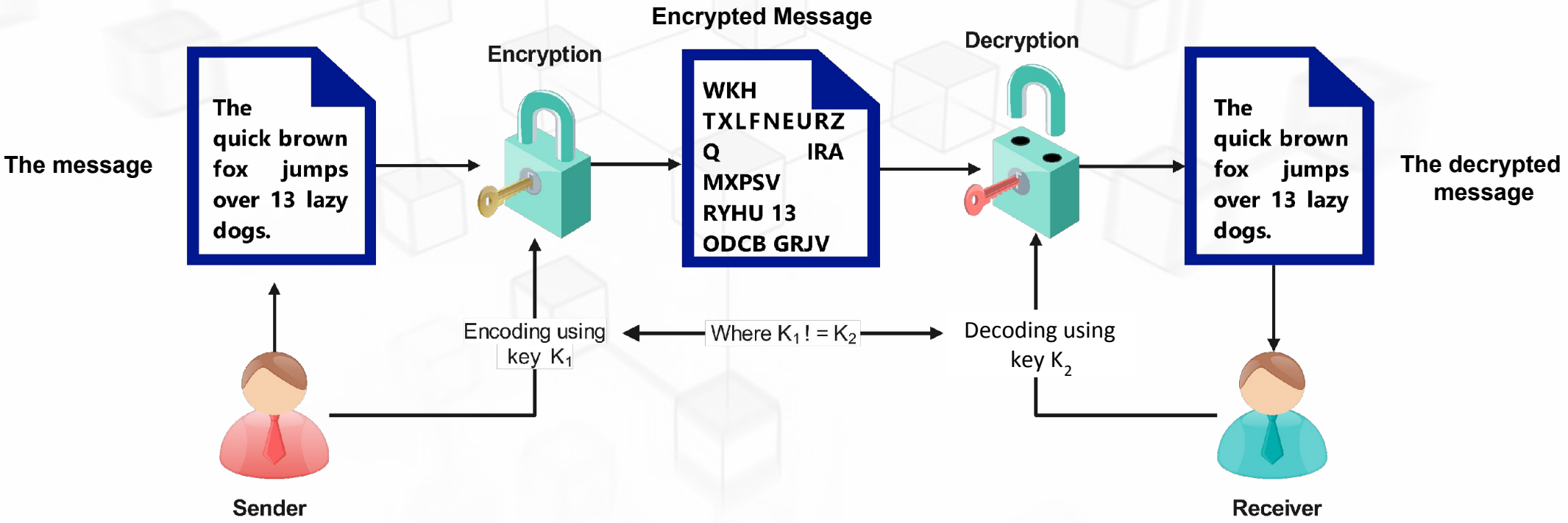
Asymmetric Key Cryptosystem

- **Asymmetric key cryptosystem**
  - It is also known as **Public-Key Cryptography(PKC).**
  - Let suppose receiver's public key = $K_{R(pub)}$ And private key = $K_{R(pri)}$



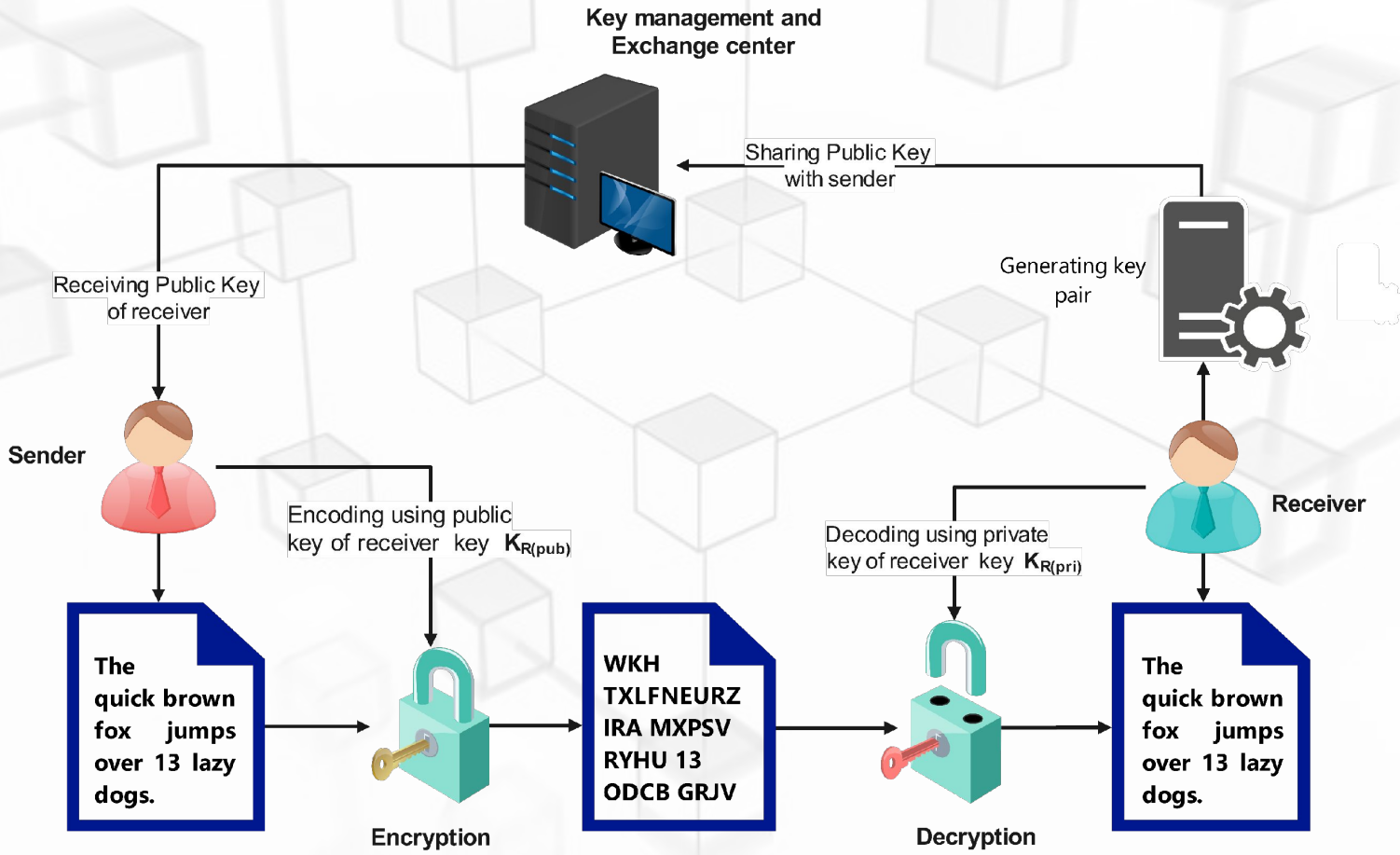
Asymmetric Key Cryptosystem

- **Asymmetric key cryptosystem**
  - Key are Different and can not be derived from each other, such that $k_1 ! = k_2$
  - Both sender and receiver used Different keys for encrypting and decrypting the message.



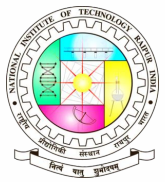
Fundamentals of Cryptography

- Process of key sharing and encryption and decryption of Public key Cryptosystem



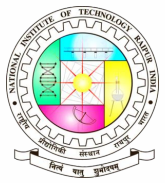
Fundamentals of Cryptography

- **Advantages of public key cryptosystem**
  - Batter key management : unlike symmetric key cryptosystem there is no need to share decryption key by the sender.
  - More secure then symmetric key cryptosystem as it having different keys for ciphering and developed with more complex mathematical algorithms.
- **Disadvantages of public key cryptosystem**
  - Slower: As it uses complex mathematical formulas that takes longer time.
  - More complex: Due to its security and key generation system the algorithms are more complex.
- **Examples**
  - Rivest–Shamir–Adleman(RSA), Elliptic Curve Cryptography(ECC), Diffie-Hellman, El-Gamal…….



RSA Cryptosystem

- **RSA algorithm**
  - It is a public key cryptosystem developed in 1976 by
  - MIT mathematician- Ronald Rivest, Adi Shamir and Leonard Adleman
  - RSA can be used for digital Signatures
  - Security of RSA depends on the difficulty of factoring the large integer n
  - Involves three steps
    - Key Generation
    - Encryption
    - Decryption



RSA Algorithm history

- Invented in 1977 at MIT
- Named for Ron Rivest, Adi Shamir, and Len Adleman
- Based on 2 keys, 1 public and 1 private

- **Key Generation**

Select two large primes p and q, such that $p \neq q$.

$n = p * q$.

$\varphi(n) = (p-1)*(q-1)$, where φ is Euler's totient function.

Select an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n))=1$ (coprime).

$d = e^{-1} \bmod \varphi(n)$

Public key $\leftarrow (e,n)$

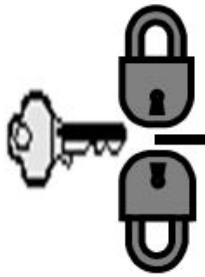
Private key $\leftarrow d$

- **Encryption**

$c = m^{e} \bmod n$

- **Decryption**

$m = c^{d} \bmod n$



Examples on RSA

- **RSA Algorithm Example**
- Choose p = 3 and q = 11
- Compute n = p * q = 3 * 11 = 33
- Compute $\phi(n) = (p - 1) * (q - 1) = 2 * 10 = 20$
- Choose e such that $1 < e < \phi(n)$ and e and n are coprime. Let e = 7
- Compute a value for d such that $(d * e) \% \phi(n) = 1$. One solution is d = 3 [(3 * 7) % 20 = 1]
- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)
- The encryption of $m = 2$ is $c = 2^7 \% 33 = 29$
- The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$

RSA Algorithm Example

1) Choose $p = 3$ and $q = 11$
2) Compute $n = p * q = 3 * 11 = 33$
3) Compute $\varphi(n) = (p - 1) * (q - 1) = 2 * 10 = 20$
4) Choose e such that $1 < e < \varphi(n)$ and e and n are co-prime. Let $e = 7$
5) Compute a value for d such that $(d * e) \% \varphi(n) = 1$. One solution is $d = 3$ $((3 * 7) \% 20 = 1)$

Public key KU = $\{e, n\} => \{7, 33\}$
Private key KR = $\{d, n\} => \{3, 33\}$

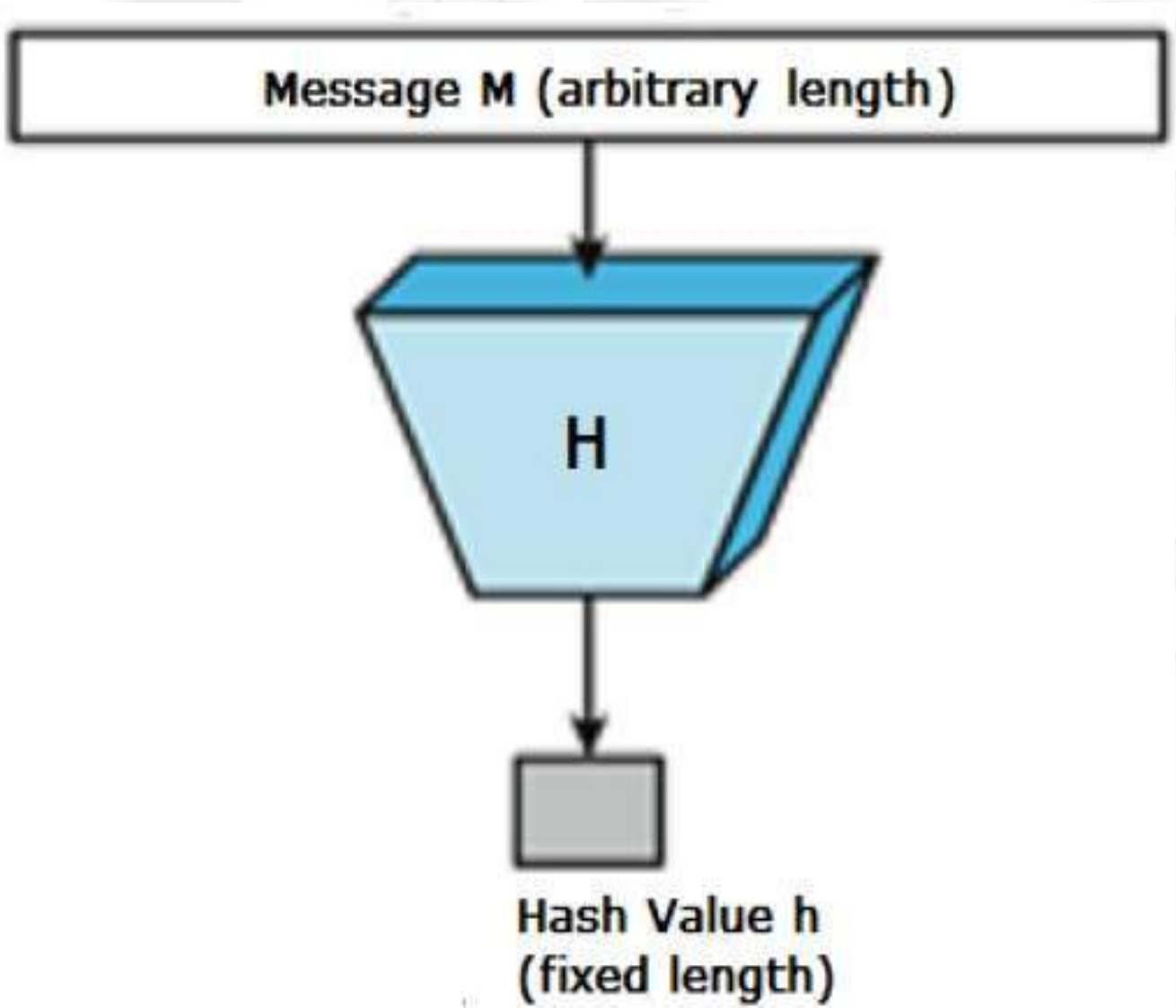
Plaintext $M = 2$,
The process of encryption:
The cipher text $C = M^e \pmod n = 2^7 \% 33 = 29$
The process of decryption:
$C^d \pmod n = 29^3 \% 33 = 2 ====\rightarrow M$

Exercise:

1) Choose $p = 7$ and $q = 11$
2) Compute $n = p * q = 7 * 11 = 77$
3) Compute $\varphi(n) = (p - 1) * (q - 1) = 6 * 10 = 60$
4) Choose e such that $1 < e < \varphi(n)$ and e and n are co-prime. Let $e = 49$
5) Compute a value for d such that $(d * e) \% \varphi(n) = 1$. One solution is $d =$ _____
You choose the value of d, such $(d * 49) \% 60 = 1$.

The plaintext $M = 7$
The process of encryption:
The cipher text $C = M^e \pmod n =$ _____

Hash Functions



Hash Functions

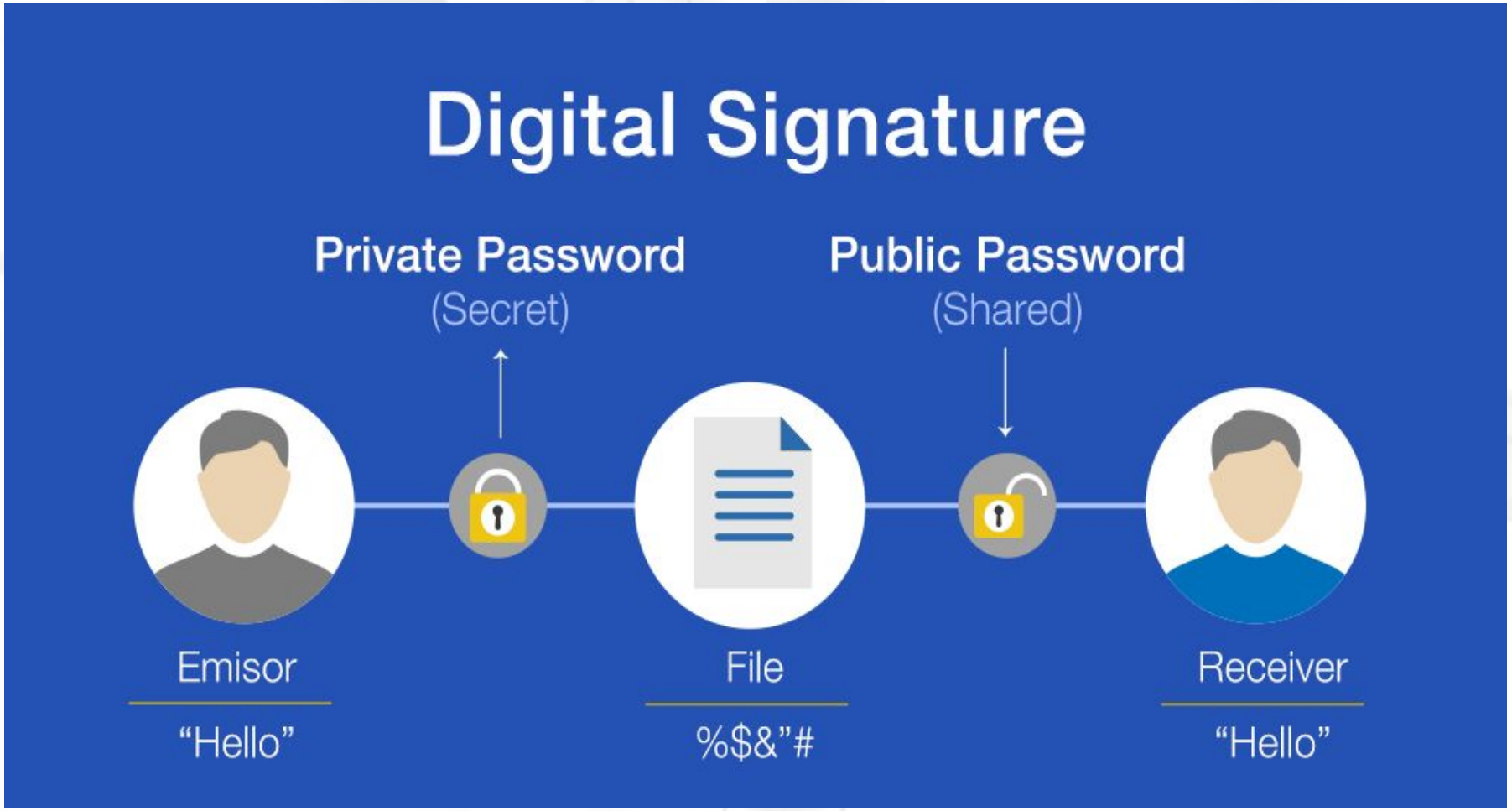
- A *hash function h* is generated by a *function H* of the form:

$$h = H(M)$$

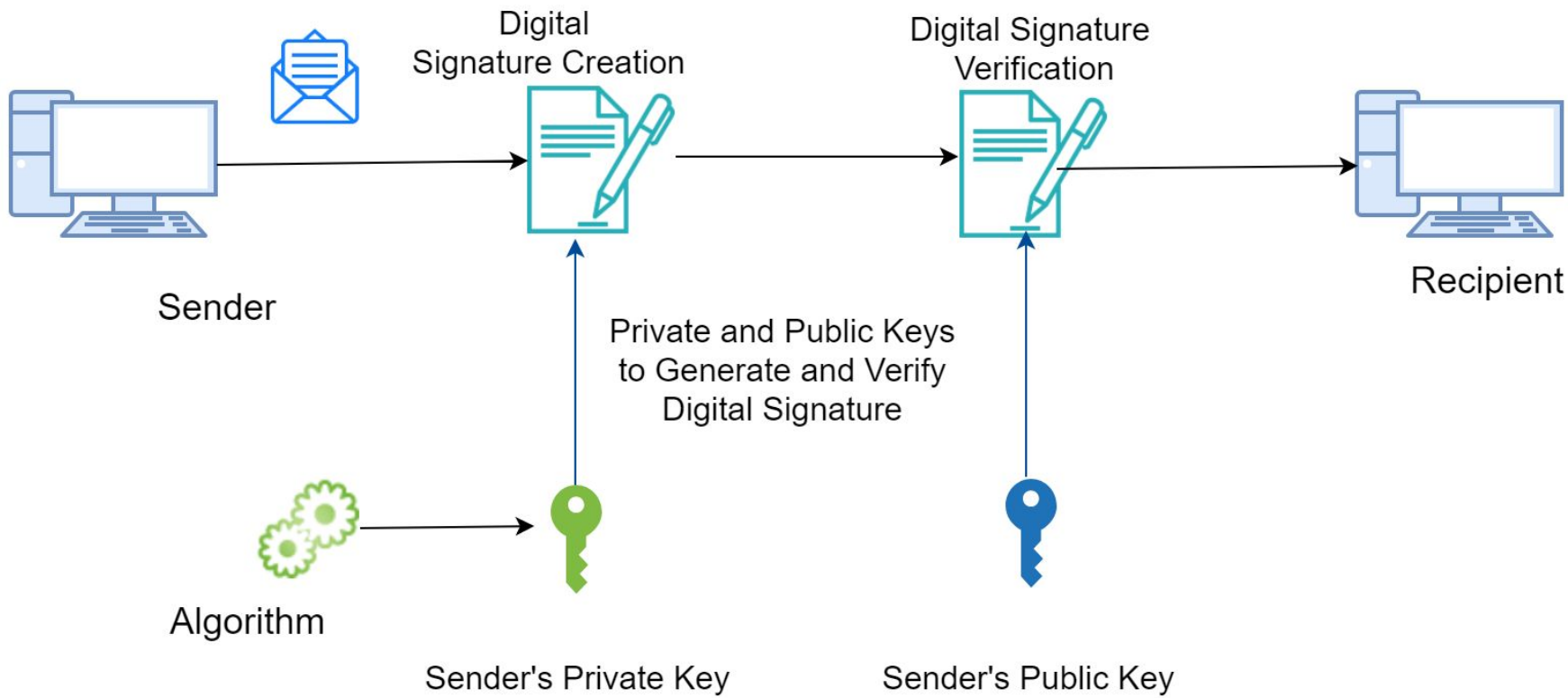
- Condenses arbitrary message to *fixed size*; usually assume that the *hash function* is *public* and *not keyed* as compared to *MAC* which is *keyed*.
- *Hash* used to *detect changes to message*.
- Can use in various ways with message.
- Most often to *create a digital signature*.

Properties of Hash Functions

1. Can be applied to any *sized message M*.
2. Produces *fixed-length output h*.
3. It is *easy to compute h=H(M)* for any *message M*.
4. Given *h* is *infeasible* to find *x* (*H(x)=h*)
   - *One-way property*
5. Given *x* is *infeasible* to find *y* (*H(y)=H(x)*)
   - *Weak collision resistance*
6. It is *infeasible* to find any *x, y* (*H(y)=H(x)*)
   - *Strong collision resistance*


Digital Signature
Private Password
(Secret)
Public Password
(Shared)
Emisor
"Hello"
File
%$&"#
Receiver
"Hello"

Digital Signatures



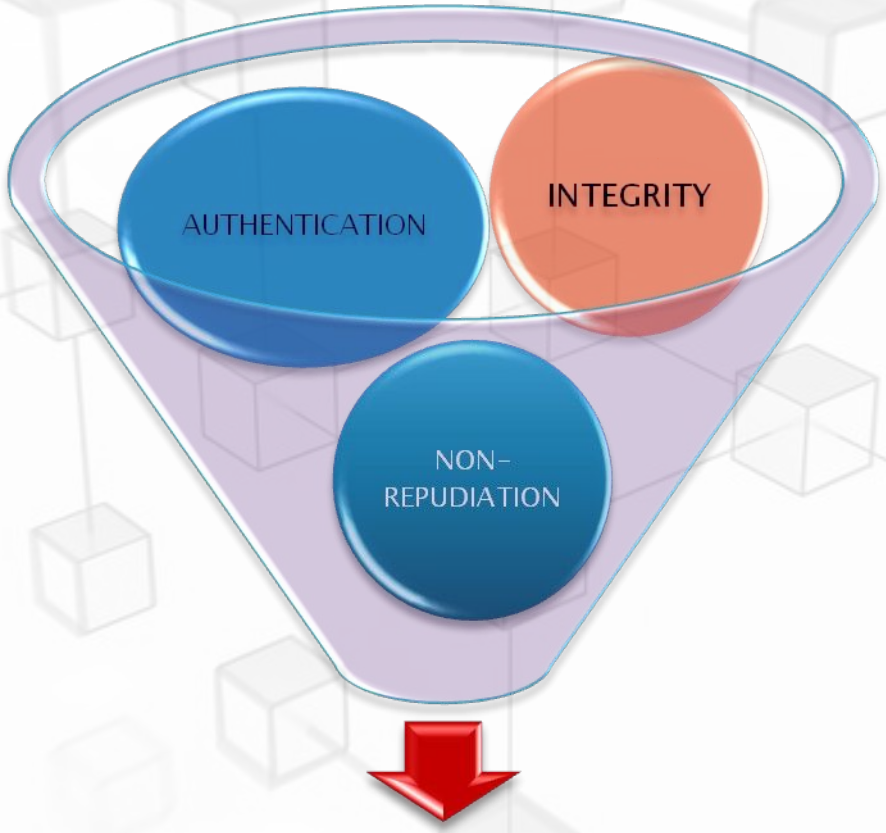
- A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged

- Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender can not easily repudiate it later.

- The originator of a message uses a signing key (Private Key) to sign the message and send the message and its digital signature to a recipient

- The recipient uses a verification key (Public Key) to verify the origin of the message and that it has not been tampered with while in transit

WHY DIGITAL SIGNATURE



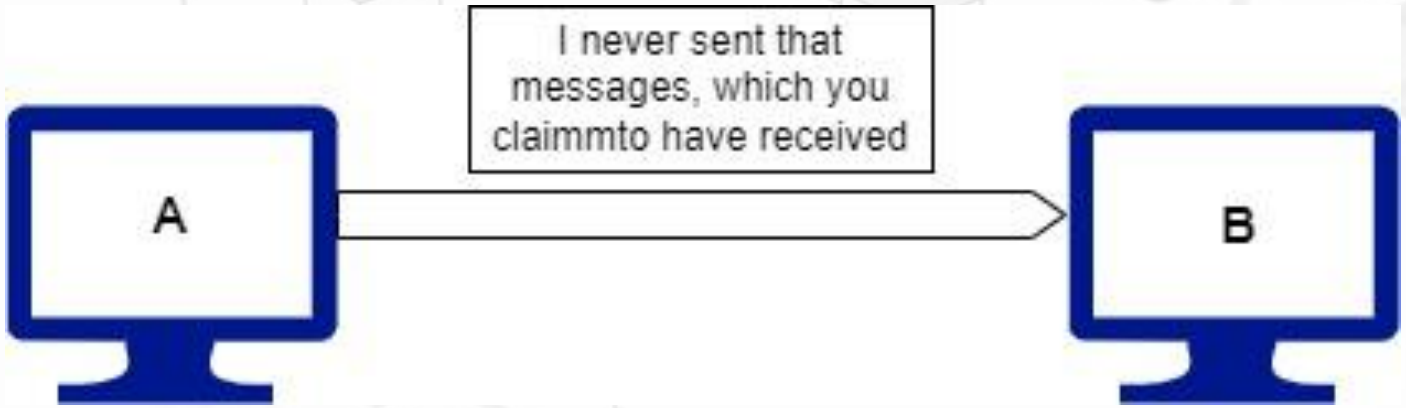
DIGITAL SIGNATURE

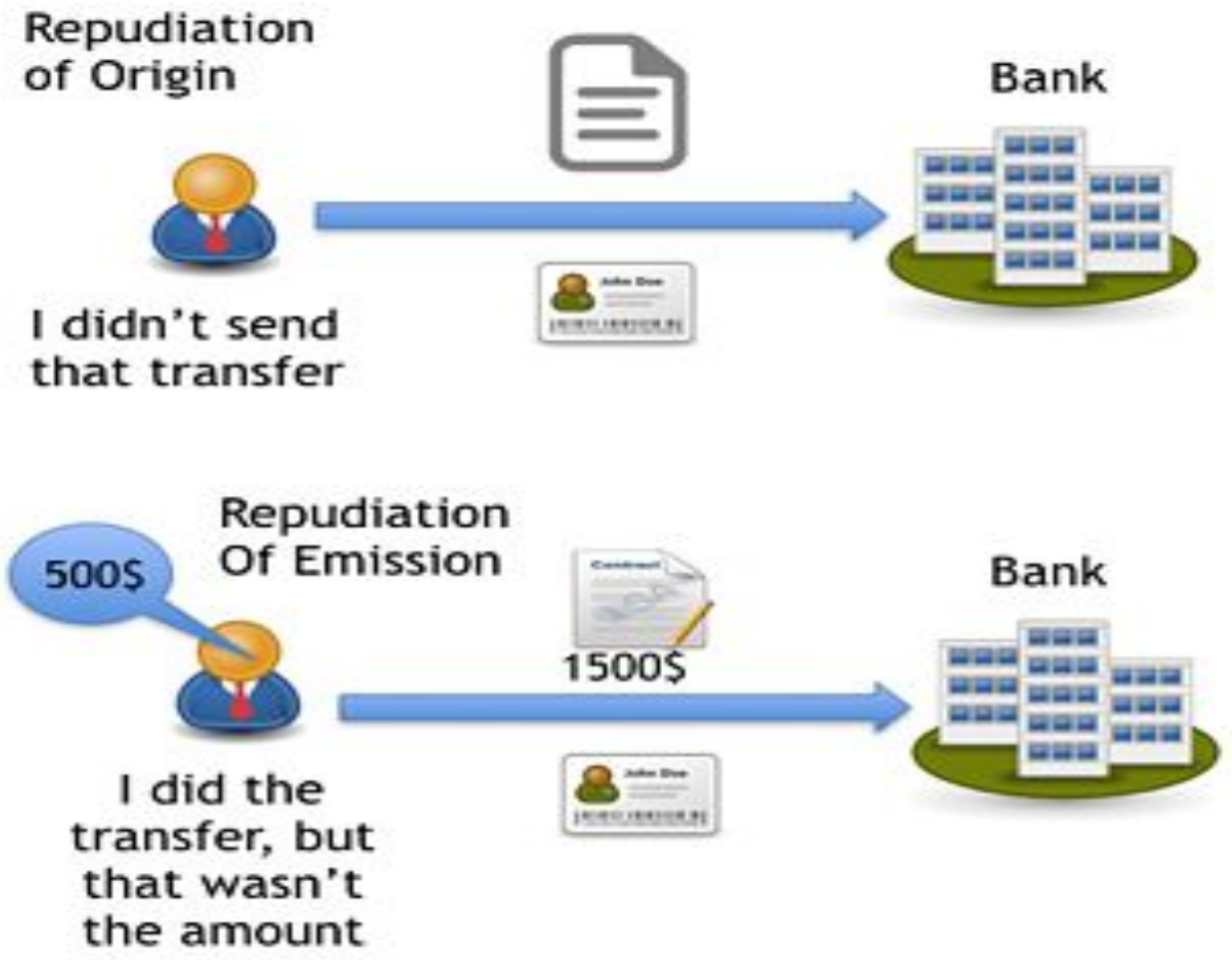
Nonrepudiation

- Nonrepudiation service protects against repudiation by either the sender or the receiver of the data
- It ensures that entity cannot deny a previous commitment or action
- In nonrepudiation with proof of the origin, the receiver of the data can later prove the identity of the sender if denied
- In nonrepudiation with proof of delivery, the sender of data can later prove the data were delivered to the intended recipient.

Non-repudiation

- It does not allow the sender of a message to refute the claim of not sending that message




Repudiation
of Origin
Bank
I didn't send
that transfer
Repudiation
Of Emission
500$
1500$
Bank
I did the
transfer, but
that wasn't
the amount

Authentication

- Establish proof of identities
- It ensures that the origin of a message or document is correctly identified