Fast Track Webinar Series

VISA *for* DISA

Day 1

ICAI Information Systems Audit Course (Old & New Syllabus)

15th Batch

INFORMATION SYSTEMS AUDIT COURSE

Module - 6

Emerging Technologies

Monday ◊ 26th JAN 2023 ◊ 08:30 AM to 09:30 AM ◊ www.3spro.blogspot.com

CA Dr GOPAL KRISHNA RAJU

Chartered Accountant, Insolvency Professional, Registered Valuer & Arbitrator

Visiting Faculty, Indian Institute of Management

Pointers

- ISA 3.0 (new syllabus) is an enriched version of ISA 2.0 (old syllabus). Not to be distinguished
- Read the ICAI Study Material minimum 2 - 3 times for getting clarity and confidence
- **Exam Preparation Tip: Practice eliminating the three choices by reasoning**
- All references made in this material is based on the following BGM of ICAI – Module 6 – Emerging Technologies

https://resource.cdn.icai.org/60976daab49637bgmisa-mod6.pdf

https://isaat.icaiexam.icai.org/ISA_July22v1/

Reference Material for ICAI ISA PQC

Basic

- ISA Background Material 3.0
- DISA AT Mock Test Papers

Additional

- ICAI Publication on "Guide to Cloud Computing for Accountants"
- ICAI "E- learning on Robotics Process Automation"
- ICAI Concept Paper on "Blockchain Technology - Adoption Trends and Implications for Accountancy Profession"
- ICAI Concept Paper on "Embracing Robotic Process Automation - Opportunities and Challenges for Accountancy Profession"
- Webinars organized by Digital Accounting and Assurance Board of ICAI
- ICAI Journals
- ISACA Publications / T ech Briefs on Emerging T echnologies
- ISACA Audit Programs on Emerging Technologies

VISA for DISA – 8 Steps

- **Step 1:** First Member have to sign up on ww.pqc.icai.org
- **Step 2:** Now Member can apply for DISA course by sign in on pqc.icai.org . Member have to pay Rs.10000 for registration.
- **Step 3:** For selecting the virtual batch, first the member have to complete E-Learning (ISA PQC 3.0) which is available on Digital Learning Hub which contain 8 Chapters.
- **Step 4:** After Completion, E Learning Assessment have to pass which contain Maximum marks 30 with 60 minute time. Minimum marks required for E Learning Assessment is only 10 marks and there are 5 attempt available to member for clear the E-learning Assessment.
- **Step 5:** After Clear this assessment, member can select virtual batch for ISA Professional Training
- **Step 6:** Professional Training for 18 days are available on Digital Learning Hub for 4 hrs. daily (With Minimum Attendance 90%)
- **Step 7:** After Completion of Professional Training, member need to clear Eligibility Test which is conducted by ICAI (60% Marks required for clear Eligibility Test)
- **Step 8:** After Clearing Eligibility test, Member are now required to clear Assessment Test conducted by ICAI **(60% Marks required to clear Assessment Test)**

ISA 2.0 (with weightage) and ISA 3.0

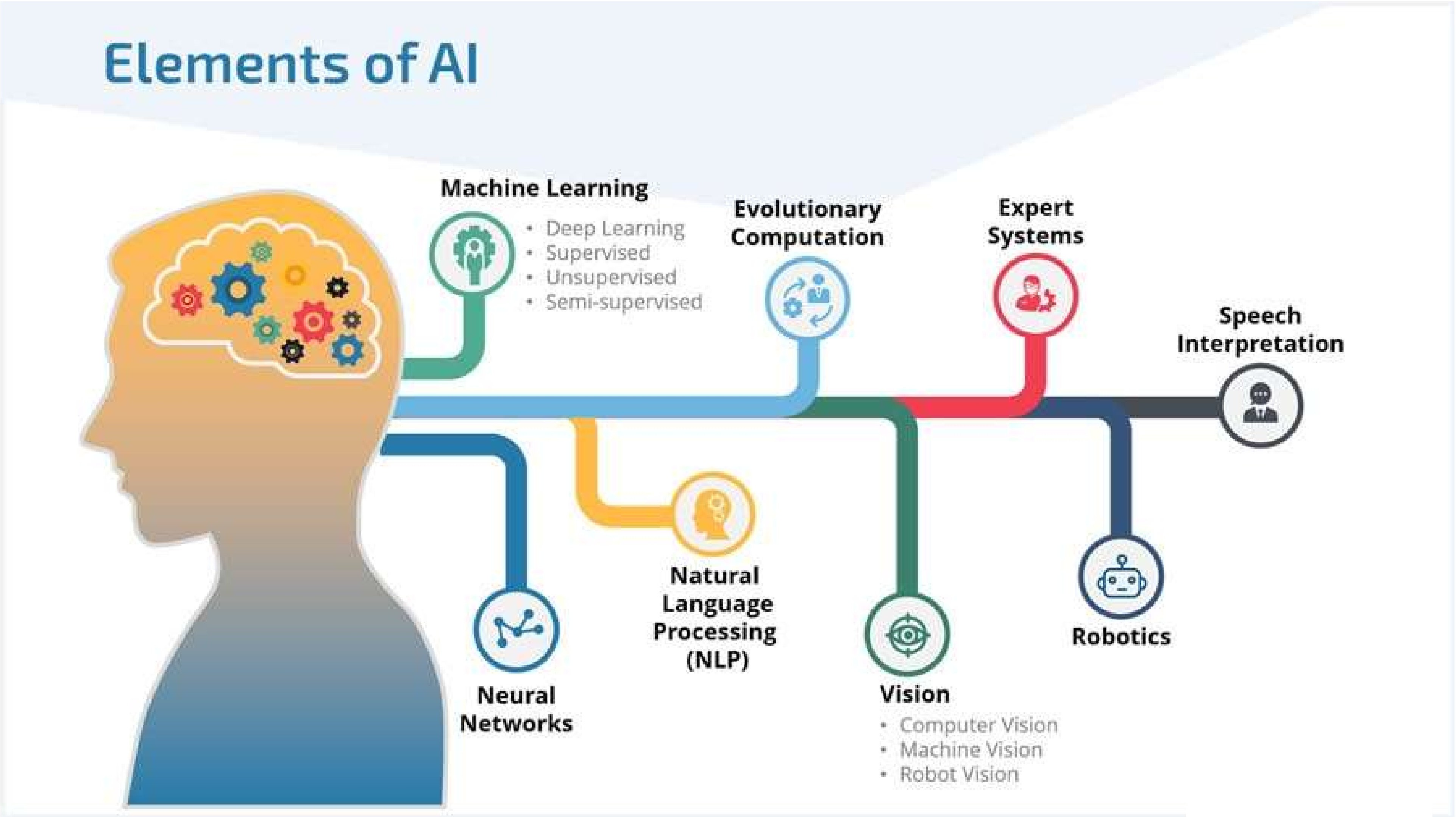
Weightage	ISA 2.0	ISA 3.0
18%	Primer on Information Technology, IS Infrastructure and Emerging Technology	Information Systems Process Audit
12%	Information Systems Assurance Services	Governance and Management of Enterprise Information Technology, Risk Management, Compliance and Business Continuity Management
12%	Governance and Management of Enterprise Information Technology, Risk Management and Compliance Reviews	System Development, Acquisition, Implementation and Maintenance Application System Audit
18%	Protection of Information Systems Infrastructure and Information Assets	Information Systems Operations and Management
12%	Systems Development: Acquisition, Maintenance and Implementation	Protection of Information Assets
6%	Business Continuity Management	Emerging Technologies
12%	Business Applications Software audit	
10%	Project Report	

Module 6
Emerging Technologies

Artificial Intelligence	6.1
Blockchain	6.2
Cloud Computing	6.3
Data Analytics	6.4
Internet of Things	6.5
Robotic Process Automation	6.6

Artificial Intelligence (AI), Blockchain (B), Cloud Computing (C) and Data Analytics (D) are considered to be the **ABCD**s of emerging **technologies** that are transforming businesses globally

6.1 Artificial Intelligence



1. Who is known as the "Father of AI"?

a) Fisher Ada

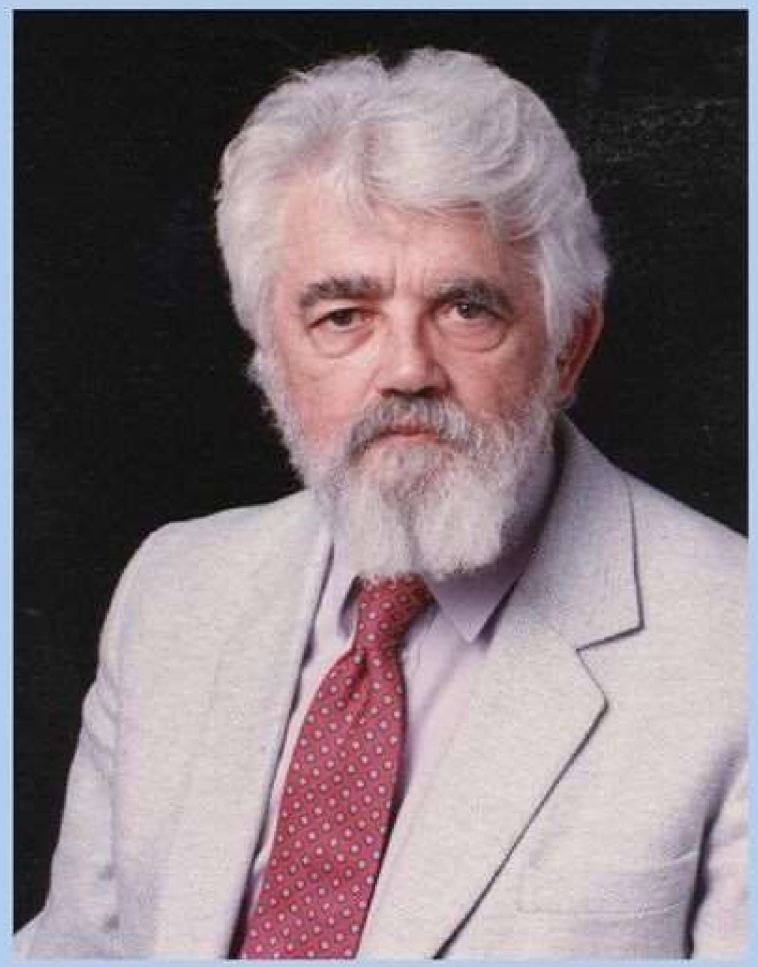
b) Alan Turing

c) John McCarthy

d) Allen Newell

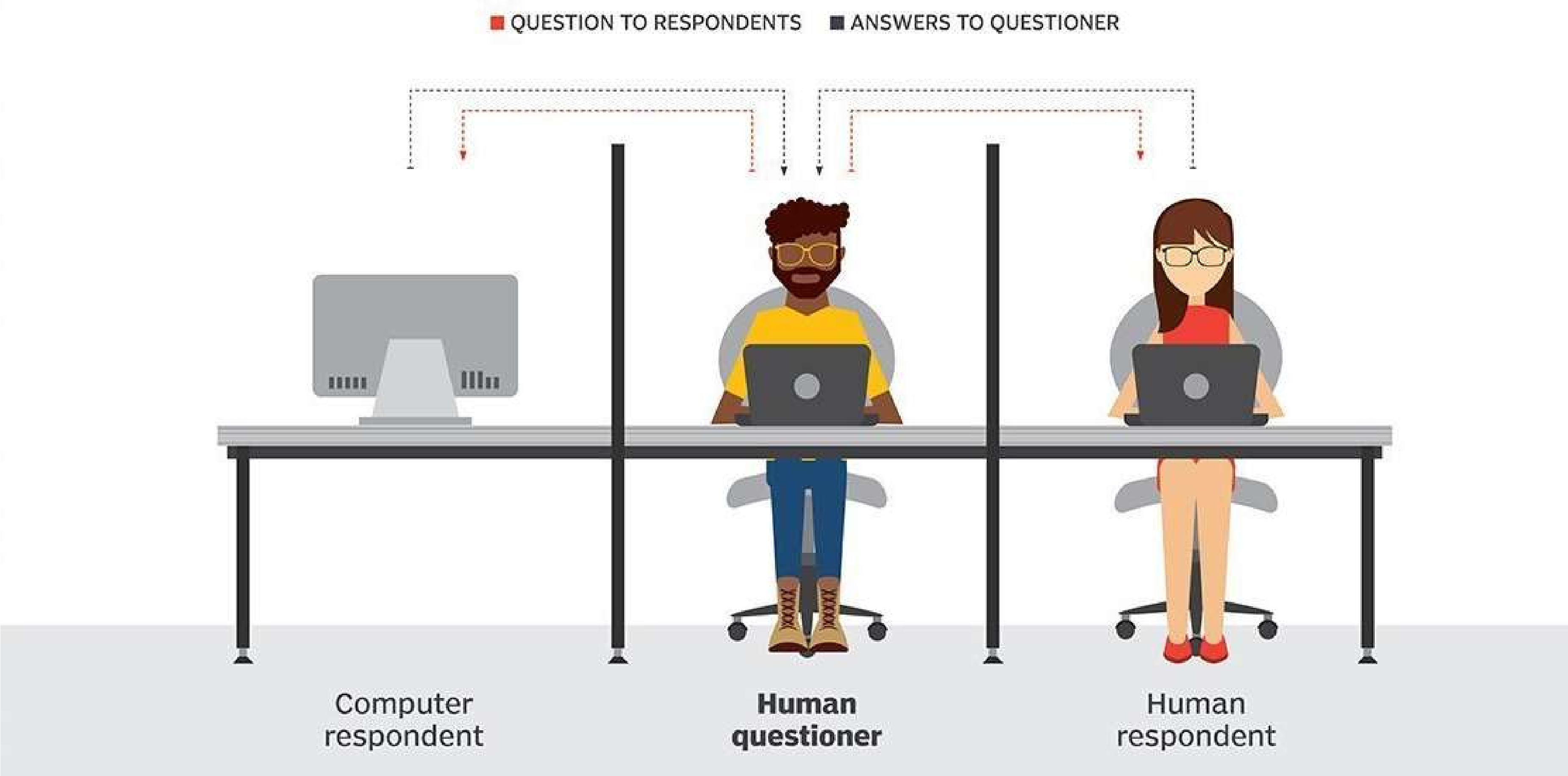
JOHN McCARTHY

In 1956 John McCarthy regarded as the father of AI, organized a conference to draw the talent and expertise of others interested in machine intelligence for a month of brainstorming. He invited them to Vermont for "The Dartmouth summer research project on artificial intelligence." From that point on, because of McCarthy, the field would be known as Artificial intelligence. Although not a huge success, the Dartmouth conference did bring together the founders in AI, and served to lay the groundwork for the future of AI research.



Turing test

During the Turing test, the human questioner asks a series of questions to both respondents. After the specified time, the questioner tries to decide which terminal is operated by the human respondent and which terminal is operated by the computer.



2. A technique that was developed to determine whether a machine could or could not demonstrate the artificial intelligence known as the ……

a) Boolean Algebra

b) Turing Test

c) Logarithm

d) Algorithm

Knowledge Representation

Knowledge representation is the part of Artificial Intelligence that deals with AI agent thinking and how their thinking affects the intelligent behaviour of agents.

A good knowledge representation requires the following properties:

- **Representational Accuracy**
- **Inferential Adequacy**
- **Inferential Efficiency**
- **Acquisitional efficiency**

3. Among the given options, which is not the required property of Knowledge representation?

a) Inferential Efficiency

b) Inferential Adequacy

c) Representational Verification

d) Representational Accuracy

4. Which term describes the common-sense of the judgmental part of problem-solving?

a) **Values-based**

b) **Critical**

c) **Analytical**

d) **Heuristic**

A heuristic technique, or a heuristic, is any approach to **problem solving** or **self-discovery** that employs a **practical method** that is not guaranteed to be optimal, perfect, or rational, but is nevertheless sufficient for reaching an immediate, short-term goal or approximation

5. Which AI technique enables the computers to understand the associations and relationships between objects and events?

a) **Heuristic Processing**

b) **Cognitive Science**

c) **Relative Symbolism**

d) **Pattern Matching**

In computer science, pattern matching is the act of **checking a given sequence** of tokens for the presence of the constituents of some pattern. In contrast to pattern recognition, the match usually has to be exact: "either it will or will not be a match."

6.2 Blockchain

Four elements characterize Blockchain

Replicated ledger

- History of all transactions
- Append-only with immutable past
- Distributed and replicated

Cryptography

- Integrity of ledger
- Authenticity of transactions
- Privacy of transactions
- Identity of participants

Consensus

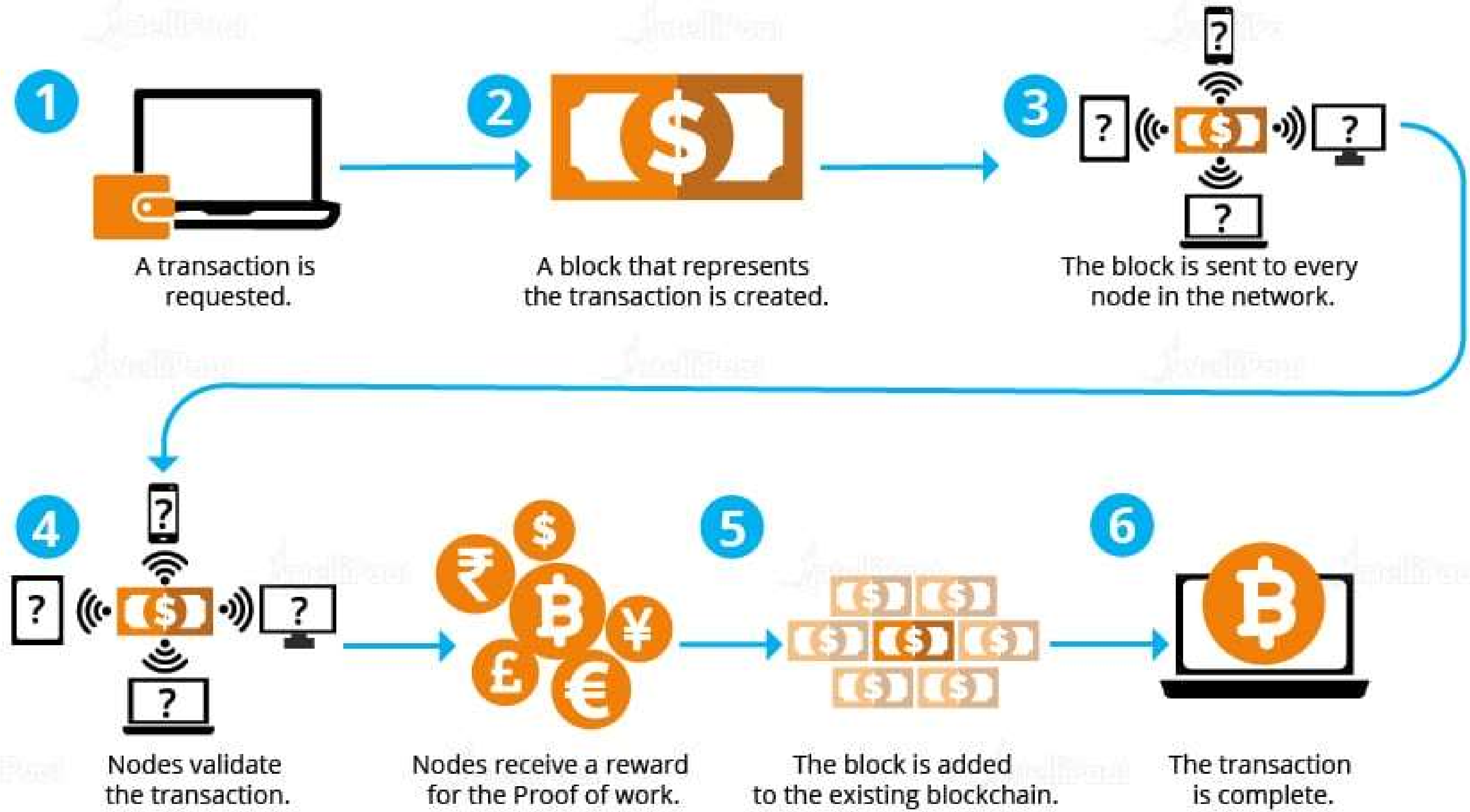
- Decentralized protocol
- Shared control tolerating disruption
- Transactions validated

Business Logic

- Logic embedded in the ledger
- Executed together with transactions
- From simple "coins" to self-enforcing "smart contracts"

Geneva, 21 March, 2017

How Do Blockchains Work?



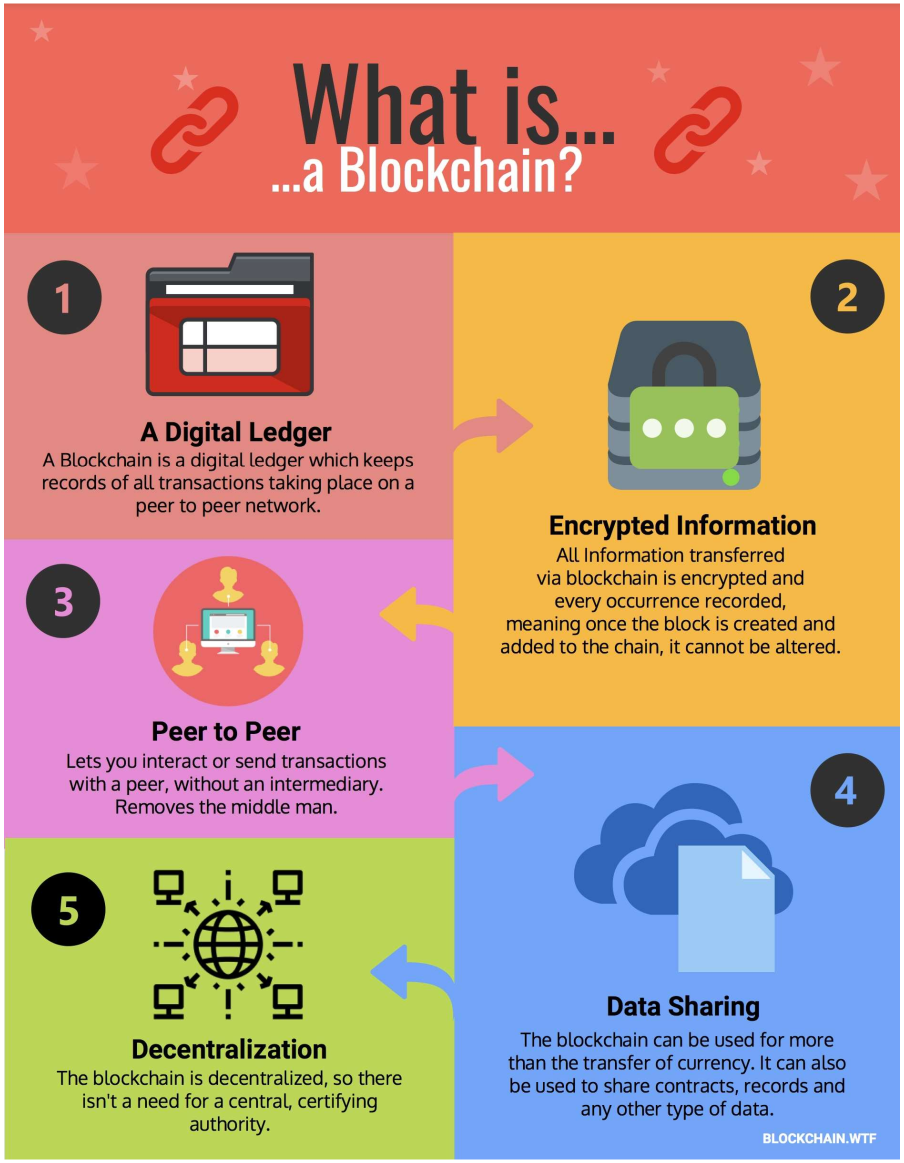
6. A blockchain is a type of?

a) Object

b) Database

c) Table

d) View



7. Blockchains store data in the form of?

a) Line

b) Circle

c) Block

d) Rhombus

Blockchain differs from a typical database in the way it stores information; it store data in blocks that are then chained together.

8. In Bitcoin case, blockchain is used in a …… way

a) Decentralized

b) Centralized

c) Both A and B

d) None of the above

In Bitcoins, blockchain is used in a decentralized way so that no single person or group has control — rather, all users collectively retain control.

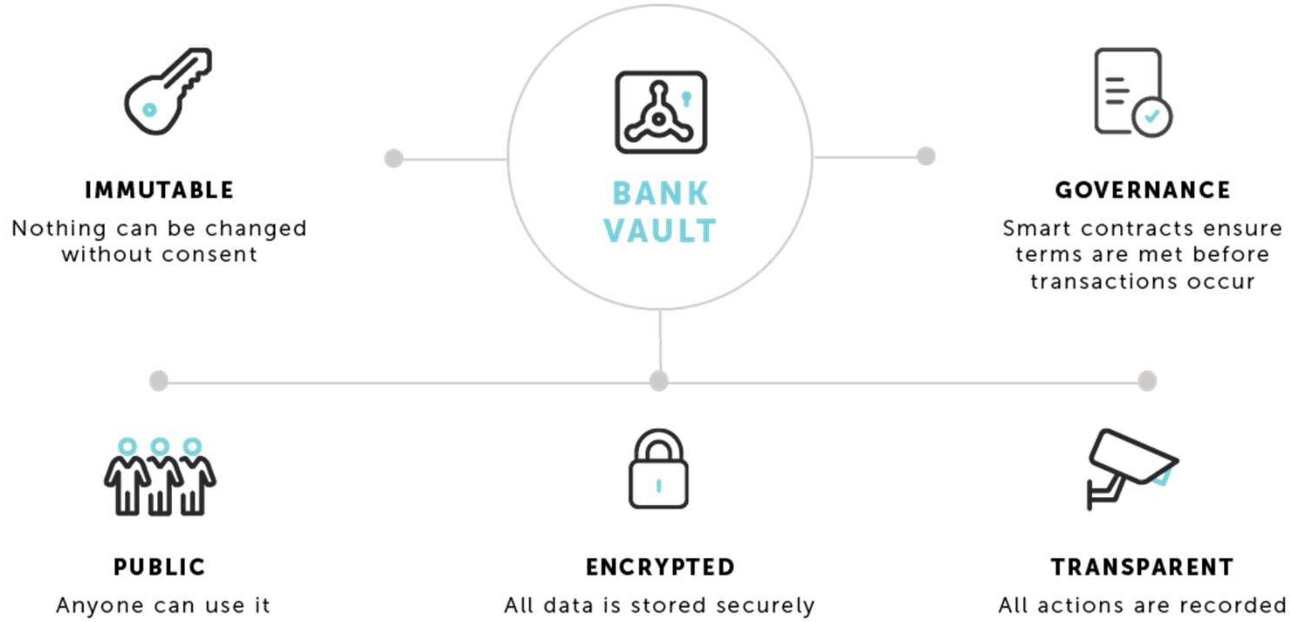
9. Decentralized blockchains are immutable?

a) True

b) False

c) (a) or (b)

d) Can't Say



Immutable: unchanging over time or unable to be changed.

Decentralized blockchains are immutable, which means that the **data entered is irreversible**. For Bitcoin, this means that transactions are permanently recorded and viewable to anyone.


SATOSHI NAKAMOTO
NET WORTH – $ 19 BILLION
A persons who design and developed bitcoin, authored the bitcoin white paper, and created and deployed bitcoin's original reference implementation. As part of the implementation, Nakamoto also devised the first blockchain database

10. The first blockchain was conceptualized by a person (or group of people) known as Satoshi Nakamoto in?

a) 2004

b) 2005

c) 2006

d) 2008

Nakamoto has stated that work on the writing of the code for bitcoin began in 2007. On 18 August 2008, he or a colleague registered the domain name bitcoin.org, and created a web site at that address. On 31 October 2008, Nakamoto published a paper on the cryptography mailing list at metzdowd.com describing a digital cryptocurrency, titled "Bitcoin: A Peer-to-Peer Electronic Cash System"

11. Which of the following statement is true about blockchain?

a) A blockchain is a decentralized, distributed, and oftentimes public, digital ledger consisting of records called blocks

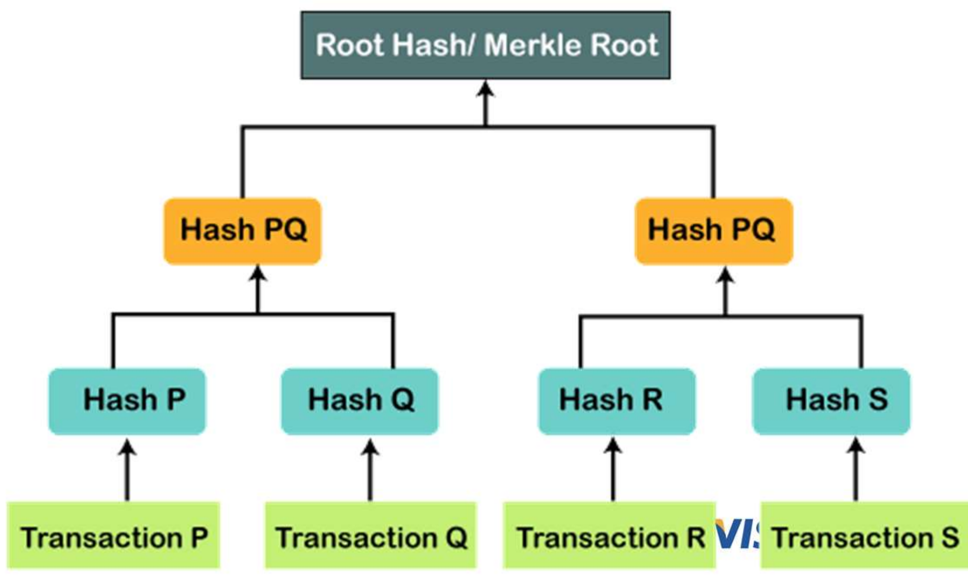
b) A blockchain database is managed autonomously using a peer-to-peer network and a distributed timestamping server

c) A blockchain has been described as a value-exchange protocol.

d) AOTA

Merkle Tree

- A hash **tree**, or the **Merkle tree**, encodes the **blockchain** data in an efficient and secure manner.
- It enables the quick verification of **blockchain** data, as well as quick movement of large amounts of data from one computer node to the other on the peer-to-peer **blockchain** network.



12. Blocks hold batches of valid transactions that are hashed and encoded into a?

a) Merkle Tree

b) Cryptographic Hash

c) Genesis Block

d) Temporary Fork

13. Which of the following is popularly used for storing bitcoins?

a) Pocket

b) E-Wallet

c) Box

d) Stack

A digital wallet also known as "e-Wallet" is an electronic device, online service, or software program that allows one party to make electronic transactions with another party bartering digital currency units for goods and services.

- Bitcoin, unlike most traditional currencies, is a digital currency.
- Thus, the approach to this kind of currency is completely different, particularly when it comes to acquiring and storing it.
- As Bitcoins don't exist in any physical shape or form, they can't technically be stored anywhere. Instead, it's the private keys used to access your public Bitcoin address and sign for transactions that need to be securely stored. A combination of the recipient's public key and your private key is what makes a Bitcoin transaction possible.
- There are several different forms of **Bitcoin wallet**, catering for different requirements and varying in terms of safety and security, convenience, accessibility and so on.

https://rbidocs.rbi.org.in/rdocs/Speeches/PDFs/CRYPTOCURRENCIESFBEA27DE561D427DB9DD5F25BE2CB8BB.PDF

Virtual Currency in India

- **RBI cautions users of Virtual Currencies against Risks – Dated 24th Dec 2013**

  https://www.rbi.org.in/commonperson/English/Scripts/PressReleases.aspx?Id=2522

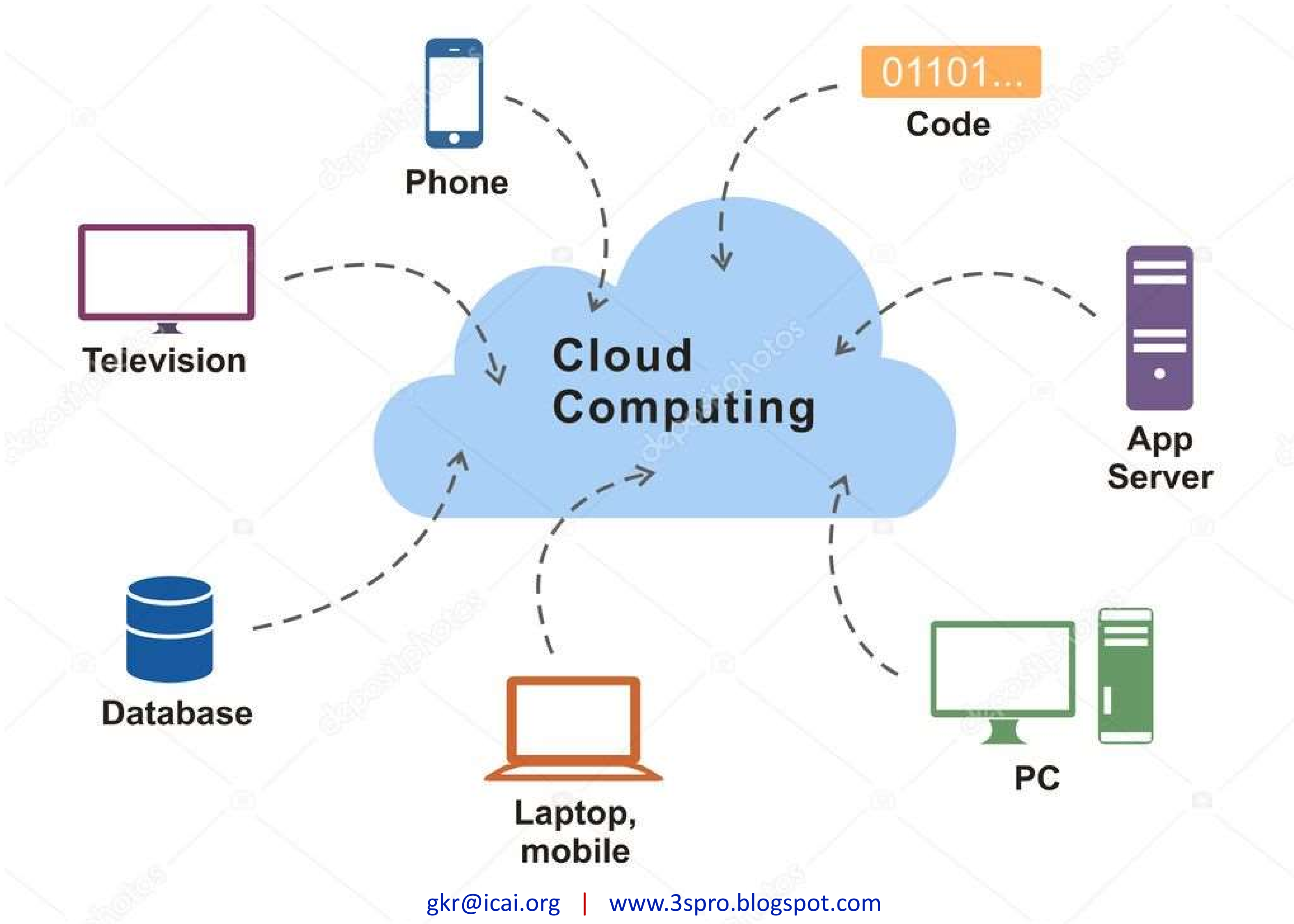
- **Prohibition on dealing in Virtual Currencies (VCs) – Dated 6th April 2018**

  https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTI15465B741A10B0E45E896C62A9C83AB938F.PDF

News: Cryptocurrency ban: RBI's proposed digital currency project; Central Bank Digital currency (CBDC)

https://m.rbi.org.in/Scripts/BS_ViewBulletin.aspx?Id=18766

6.3 Cloud Computing

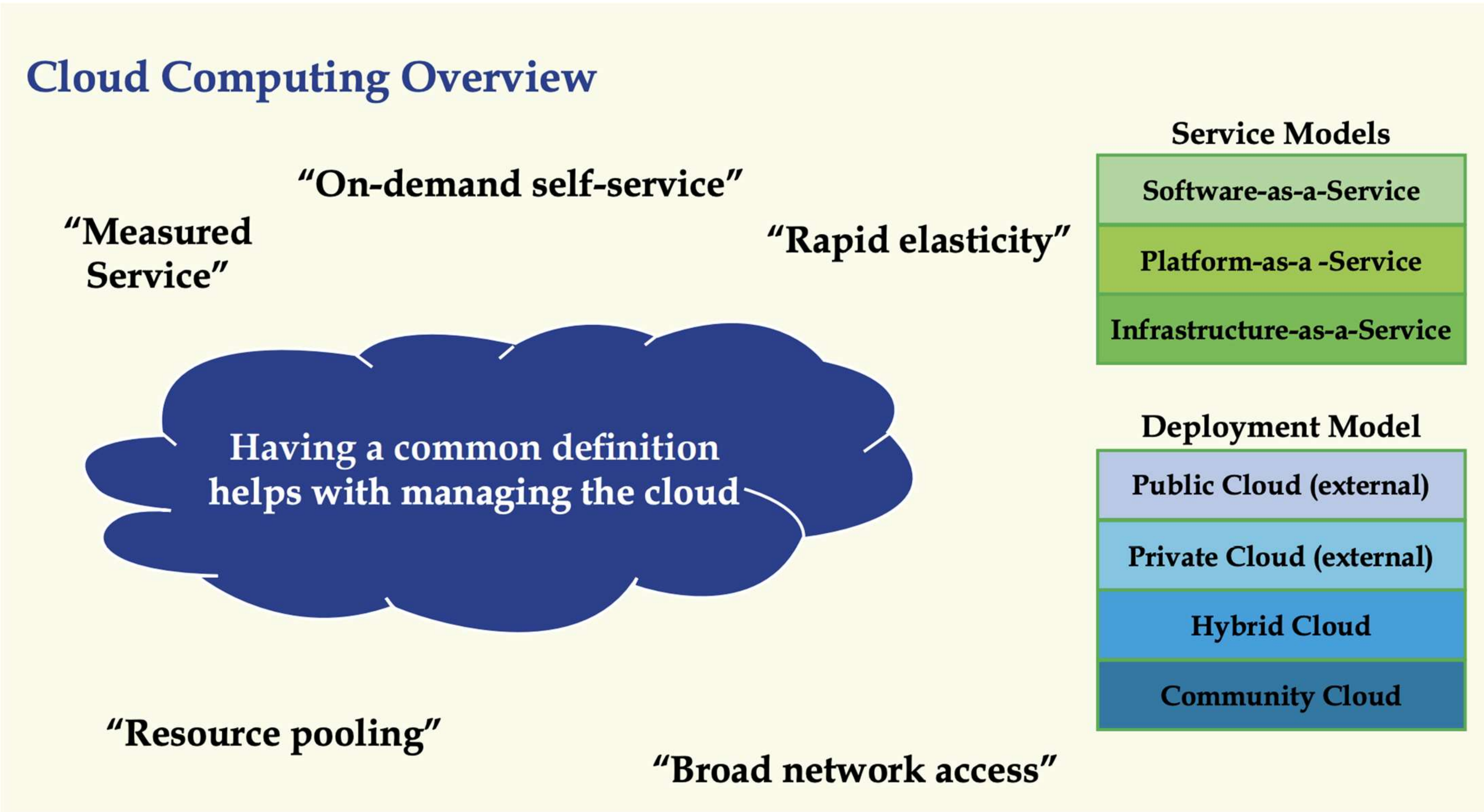


Cloud Computing

- National Institute of Standards and Technology (NIST) defines cloud computing as: **"Cloud computing is a model for enabling ubiquitous, convenient, on-demand, network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management efforts or service provider interaction."**

Top cloud providers in 2021: **AWS**, **Microsoft Azure**, and **Google Cloud**

Cloud Computing



Cloud Computing Overview - Service Delivery

Responsibility Chart-Your Organizations vs Cloud Vendor

14. What type of computing technology refers to services and applications that typically run on a distributed network through virtualized resources?

a) **Distributed Computing**

b) **Cloud Computing**

c) **Soft Computing**

d) **Parallel Computing**

Virtualization is the fundamental technology that powers cloud computing. This software separates compute environments from physical infrastructures, so you can run multiple operating systems and applications simultaneously on the same machine.

15. Cloud computing is a kind of abstraction which is based on the notion of combining physical resources and represents them as …….. resources to users.

a) Real

b) Cloud

c) Virtual

d) Artificial

16. Which one of the following cloud concepts is related to sharing and pooling the resources?

a) **Polymorphism**

b) **Virtualisation**

c) **Abstraction**

d) **Encapsulation**

The application runs on physical systems that are not specified in real.
The information stored in the locations that are also not specified or unknown, administration of the systems are outsourced to others and can be accessed by the user.

Polymorphism

- The word **polymorphism** means having many forms. Real life **example** of **polymorphism**: A person at the same time can have different characteristic. Like a man at the same time is a father, a husband, an employee. So the same person posses different behaviour in different situations. This is called **polymorphism**.
- In programming languages, polymorphism is the provision of a single interface to entities of different types or the use of a single symbol to represent multiple different types.

Encapsulation

- **Encapsulation** is a process by which a lower-layer protocol receives data from a higher-layer protocol and then places the data into the data portion of its frame.
- Thus, **encapsulation** is the process of enclosing one type of packet using another type of packet.

17. Which one of the following is Cloud Platform by Amazon?

a) Azure

b) AWS

c) Cloudera

d) AOTA

Cloudera, Inc. is a US-based software company that provides a software platform for data engineering, data warehousing, machine learning and analytics that runs in the cloud or on premises.

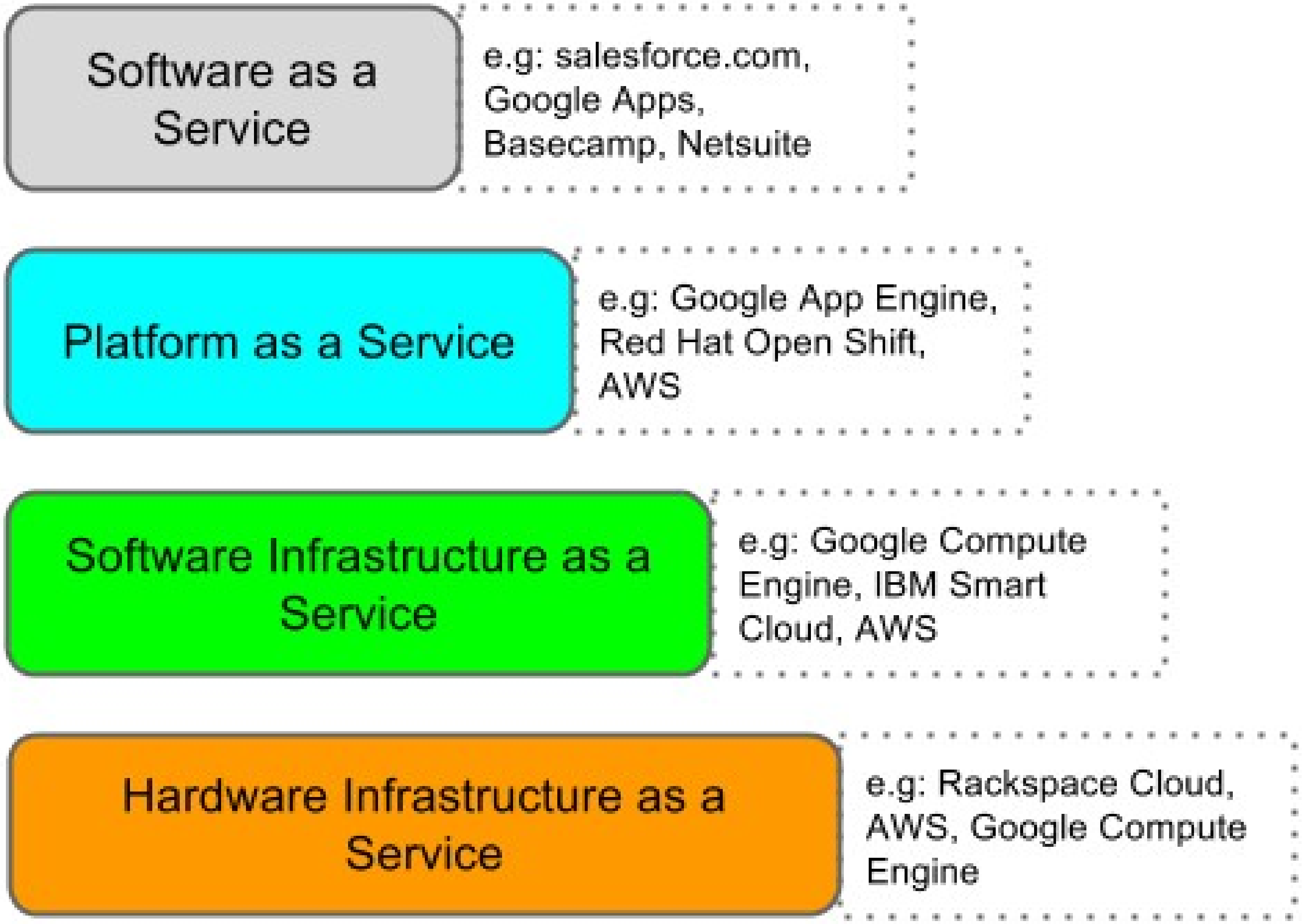
18. Which of the following is a type of Cloud Computing Service Models?

a) Public-as-a-Service

b) Platform-as-a-Service

c) Community-as-a-Service

d) Private-as-a-Service


Software as a Service
e.g: salesforce.com, Google Apps, Basecamp, Netsuite
Platform as a Service
e.g: Google App Engine, Red Hat Open Shift, AWS
Software Infrastructure as a Service
e.g: Google Compute Engine, IBM Smart Cloud, AWS
Hardware Infrastructure as a Service
e.g: Rackspace Cloud, AWS, Google Compute Engine

19. What does P2P technology stand for?

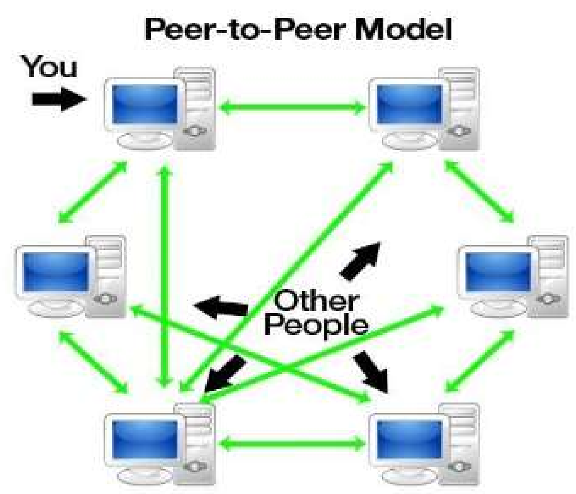
a) Password to Password

b) Peer to Peer

c) Product to Product

d) Private Key to Public Key

UNSTRUCTTURED PEER TO PEER



20. What is Blockchain?

a) A distributed ledger on a peer to peer network

b) A type of cryptocurrency

c) An exchange

d) A centralized ledger

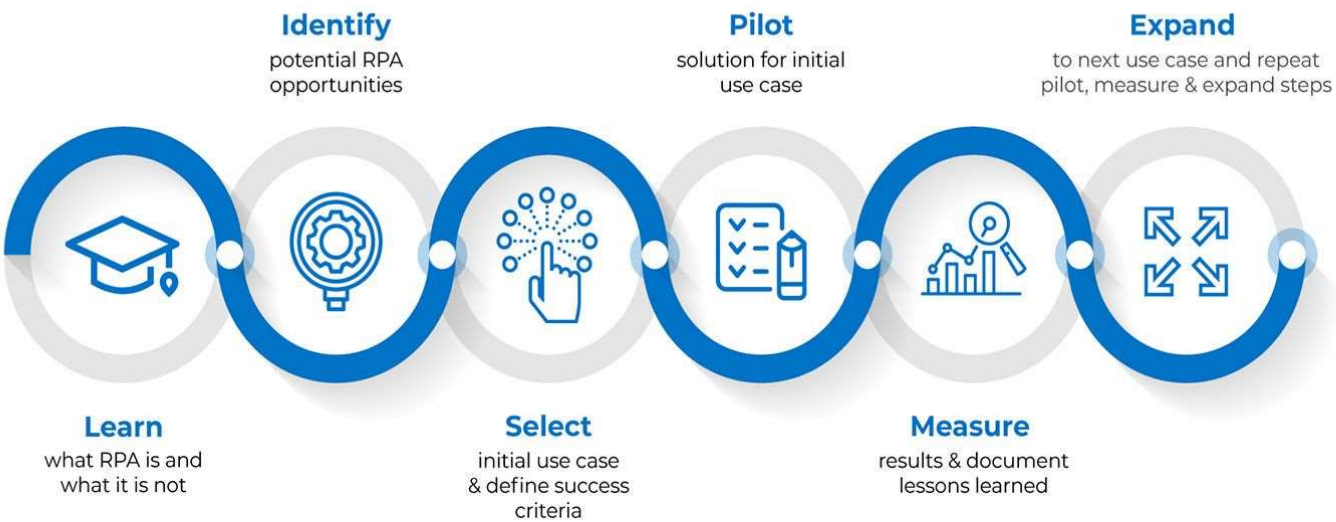
21. Which of the following is not a step involved in RPA?

a) Preparation of project

b) Development of business cases

c) Implementation of RPA

d) Data Cleaning



22. Which of the following statements about RPA is false?

a) It is walking and talking robot

b) It is a computer coded software

c) These are programs that replace human repetitive tasks

d) These perform in cross functional platforms

RPA in Finance: Banks use RPA to perform repetitive tasks like data entry and to automate customer service and back-office workflows.

6.5 Internet of Things

- ✓ The term "Internet of things" was coined by Kevin Ashton of Procter & Gamble, later MIT's Auto-ID Center, in 1999, though he prefers the phrase "Internet *for* things".
- ✓ At that point, he viewed radio-frequency identification (RFID) as essential to the Internet of things, which would allow computers to manage all individual things.
- ✓ The main theme of the Internet of Things is to embed short-range mobile transceivers in various gadgets and daily necessities to enable new forms of communication between people and things, and between things themselves.

Less than 40% of companies are deploying IoT devices within their infrastructures today.

- ✓ By **2021**, 35 billion IoT **devices** will be installed around the world. The number of **connected devices** in **2021** will be 46 billion.
- ✓ The installed base of active **Internet of Things** connected devices is forecast to reach 30.9 billion units by 2025.

23. Which of the following is a system of inter-connected and inter-related computing devices which have ability to transfer the data over network:

a) **Blockchain**

b) **Internet of Things**

c) **Robotic Process Automation**

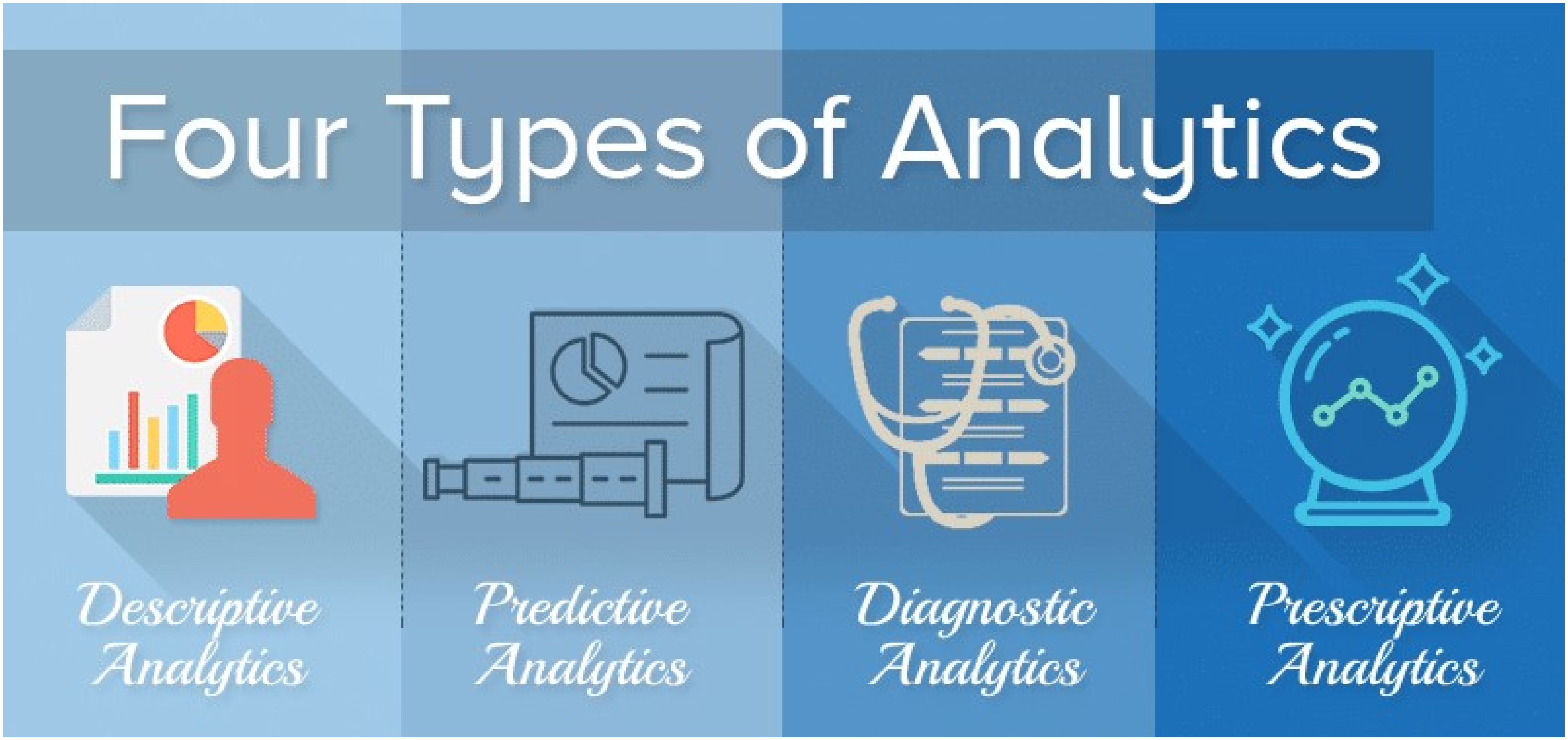
d) **Artificial Intelligence**

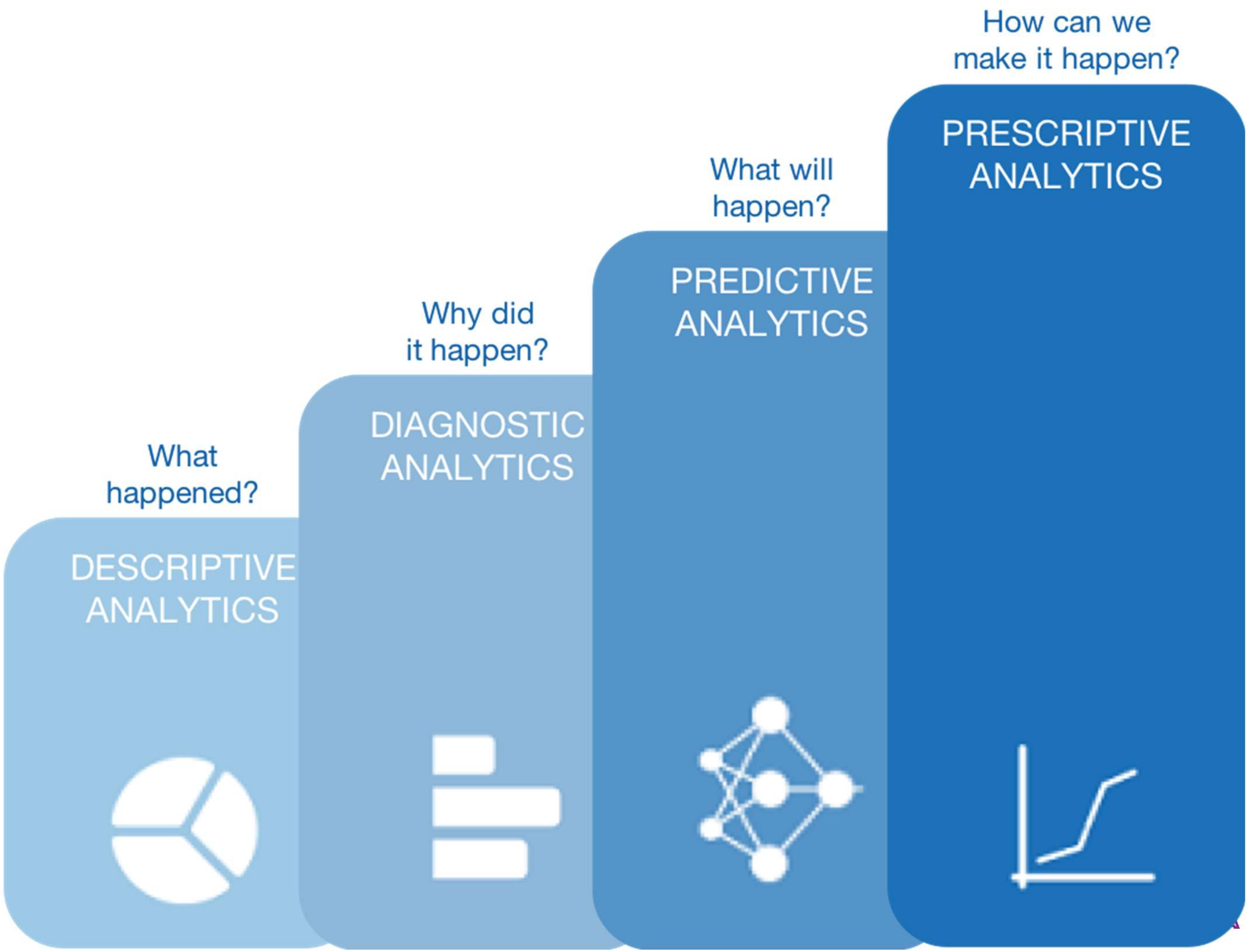
The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

Internet of Medical Things

- IoT devices can be used to enable **remote health monitoring** and **emergency notification systems**.
- These health monitoring devices can range from blood pressure and heart rate monitors to advanced devices capable of monitoring specialized implants, such as pacemakers, Fitbit electronic wristbands, or advanced hearing aids.
- Some hospitals have begun implementing **"smart beds"** that can detect when they are occupied and when a patient is attempting to get up. It can also adjust itself to ensure appropriate pressure and support is applied to the patient without the manual interaction of nurses.

6.4 Data Analytics




What happened?
DESCRIPTIVE ANALYTICS
Why did it happen?
DIAGNOSTIC ANALYTICS
What will happen?
PREDICTIVE ANALYTICS
How can we make it happen?
PRESCRIPTIVE ANALYTICS

24. Which one is simplest form of Data Analytics?

a) Predictive

b) Descriptive

c) All of the mentioned

d) Prescriptive

Descriptive analytics is a preliminary stage of data processing that creates a summary of historical data to yield useful information and possibly prepare the data for further analysis

25. The method by which companies analyse customer data or other types of information in an effort to identify patterns and discover relationships between different data elements is often referred to as:

a) Customer data management

b) Data mining

c) Data digging

d) NOTA

- A **data lake** is a storage repository that holds a vast amount of raw data in its native format until it is needed.
- While a hierarchical **data warehouse** stores data in files or folders, a data lake uses a flat architecture to store data.

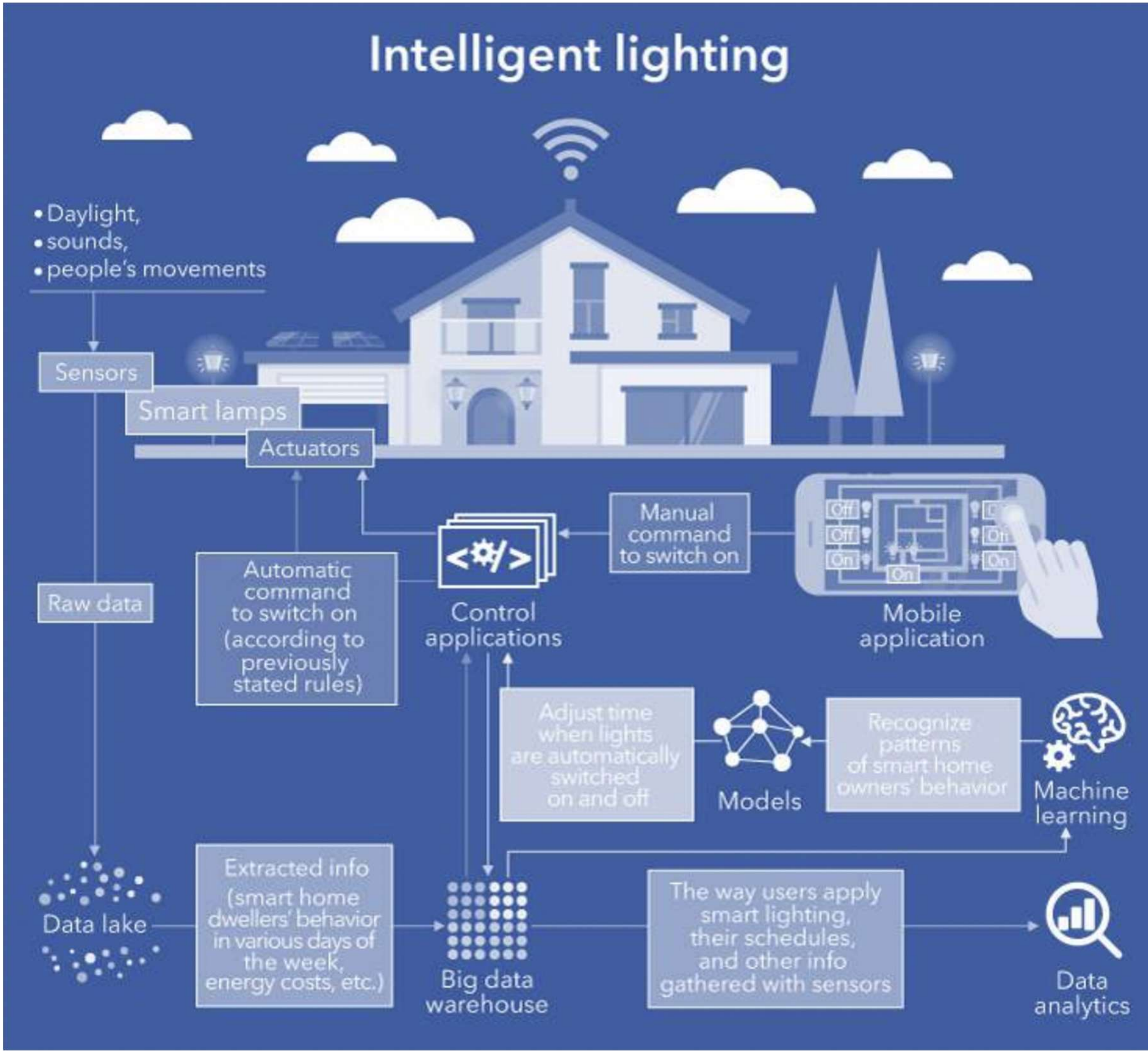
26. Which of the following is a central storage for all kinds of structured, semi structured or unstructured raw data collected from multiple sources even outside of company's operational systems?

a) Data Warehouse

b) Data Lake

c) Database

d) Data marts


Intelligent lighting
• Daylight,
• sounds,
• people's movements
Sensors
Smart lamps
Actuators
Manual command to switch on
Automatic command to switch on (according to previously stated rules)
Control applications
Mobile application
Off
On
Raw data
Adjust time when lights are automatically switched on and off
Models
Recognize patterns of smart home owners' behavior
Machine learning
Extracted info (smart home dwellers' behavior in various days of the week, energy costs, etc.)
Data lake
Big data warehouse
The way users apply smart lighting, their schedules, and other info gathered with sensors
Data analytics

27. Which of the following tools best describe Predictive Analytics?

a) Simulation

b) Statistical Analysis

c) Machine Learning

d) Graphical reports

Predictive Analytics analyses the past behaviour and makes predictions about the future to identify the new trends. Simulation is one such technique used in **predictive analytics**. Graphical reports and statistical analysis are more commonly associated with **historical / descriptive analytics**. Machine Learning is used in **Cognitive analytics**.

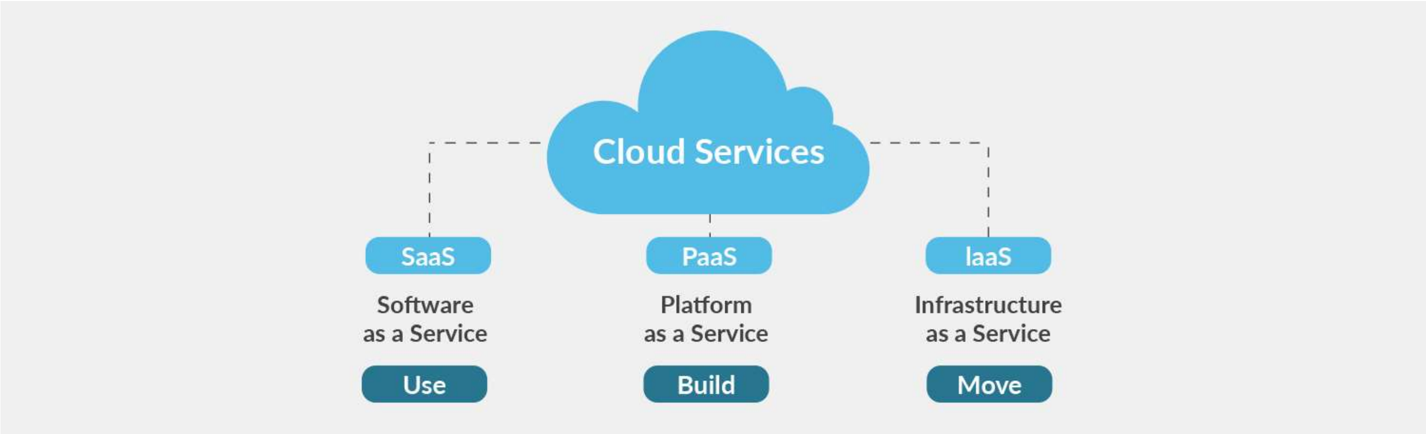
28. Which of the following is not a cloud deployment model?

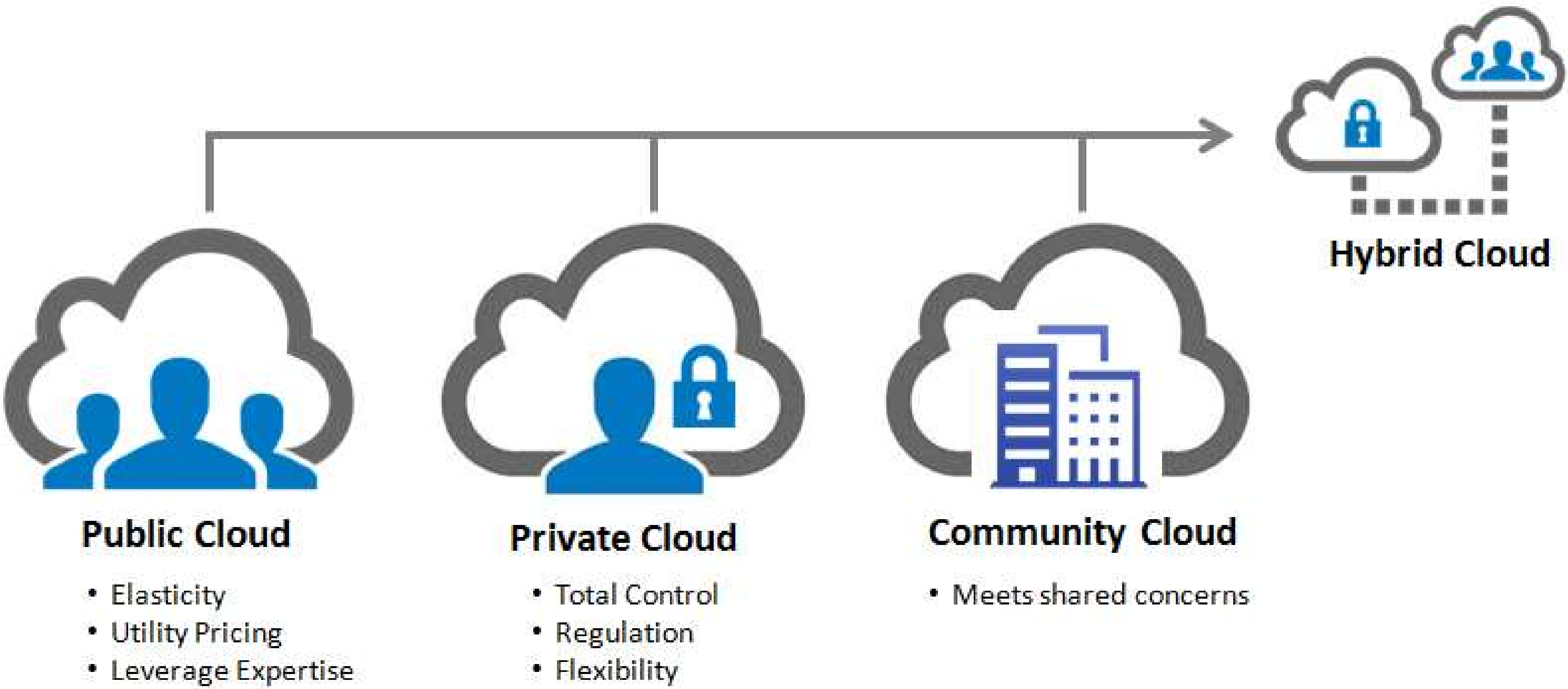
a) Private

b) Public

c) IaaS

d) Hybrid




Hybrid Cloud
Public Cloud
• Elasticity
• Utility Pricing
• Leverage Expertise
Private Cloud
• Total Control
• Regulation
• Flexibility
Community Cloud
• Meets shared concerns

29. Which of the following is not a stream of AI?

a) Machine Learning

b) Big Data

c) Speech Recognition

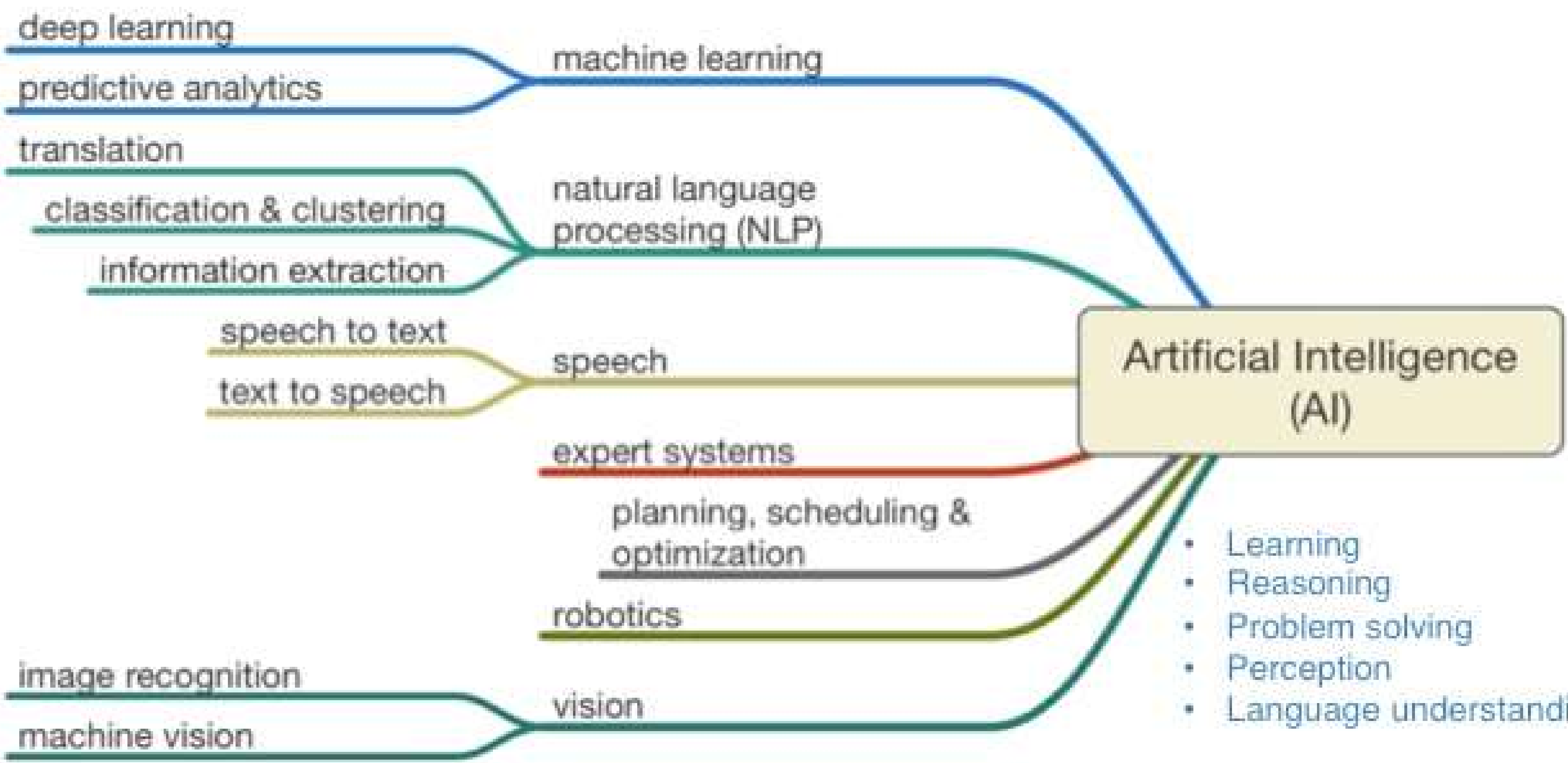
d) Natural language processing (NLP)

The growing maturity of the concept more starkly delineates the difference between "big data" and "business intelligence":

- **Business intelligence** uses applied mathematics tools and descriptive statistics with data with **high information density** to measure things, detect trends, etc.
- **Big data** uses mathematical analysis, optimization, inductive statistics, and concepts from nonlinear system identification to infer laws (regressions, nonlinear relationships, and causal effects) from large sets of data with **low information density** to reveal relationships and dependencies, or to perform predictions of outcomes and behaviours

What is AI?

the science of making computers do things that require intelligence when done by humans



- Learning
- Reasoning
- Problem solving
- Perception
- Language understanding

30. Which of the following is **not** an example for AI Platform?

a) IBM Watson Studio

b) Tensor Flow

c) AWS AI

d) Microsoft Power BI

Microsoft Power BI is predominantly a Data Analytics Platform.

Top 10 AI Softwares

01 IBM Watson Studio

02 Microsoft Azure ML

03 TensorFlow

04 Google Cloud AI Platform

05 Salesforce Einstein

06 Infosys Nia

07 H20 AI

08 PyTorch

09 Apache MXNet

10 Wipro Holmes

Evolution of Automation

Automation continuum range from enabling strategies that improve parts of business processes to sophisticated technologies with cognitive elements.

Robotic Process Automation

- Screen scraping data collection
- Rules based business process management
- Tactical toolset to automate repetitive tasks
- Cheaper and faster step towards process efficiency

Intelligent Automation

- Data input and output in any format
- Pattern recognition within unstructured data
- Replication of judgment based tasks
- Basic learning capabilities for continuous improvement to quality and speed

Artificial Intelligence

- Natural language recognition and processing
- Dealing with unstructured super data sets
- Hypothesis based predictive analysis
- Self-learning rules continuously rewritten to improve performance

6.6 Robotic Process Automation

What is RPA

- **RPA is…**
  - Computer-coded software
  - Programs that replace humans performing repetitive rules-based tasks
  - Cross-functional and cross-application macros

- **RPA is not…**
  - Walking, talking auto-bots
  - Physically existing machines processing paper
  - Artificial intelligence or voice recognition and reply software

KEY CONCEPTS OF IOT

Hardware

The heart of IoT is billions of interconnected devices with attached sensors and actuators that sense and control the physical world.

Networking and cloud integration

Network design and management are essential within IoT, due to the sheer volume of connected devices and due to the impact that network design decisions can have at scale.

Embedded programming

IoT devices are embedded devices, and may be prototyped using commoditized micro-controller platforms, such as Arduino, with custom printed circuit boards (PCBs) developed at a later stage.

Data analytics and prediction

Developers will need securely and reliably ingest, store, and query the vast quantities of heterogeneous data originating from these devices.

Security

Security is one of the most critical concerns in IoT, closely related to data ethics, privacy and liability. It must be built-in at every step of the design of the system.

Machine Learning and AI

To be truly intelligent, big data analytics needs to apply cognitive computing techniques drawn from data mining, modeling, statistics, machine learning, and AI.

What are the three types of RPA?

1. **Unattended/Autonomous RPA:** Ideal for reducing work like completing data processing tasks in the background. They don’t require any human intervention. These bots can be launched using:
   - **Specified intervals**
   - **Bot-initiated**
   - **Data input**
2. **Attended RPA:** These bots live on the user’s machine and are triggered by the user. They can be launched:
   - **When embedded on an employee’s device**
   - **Automatically based on predefined conditions**
   - **Leveraging an RPA client tool**
3. **Hybrid RPA:** This is a combination of attended and autonomous bots. These bots address front- and back-office tasks in the enterprise

31. What are the business benefits of RPA?

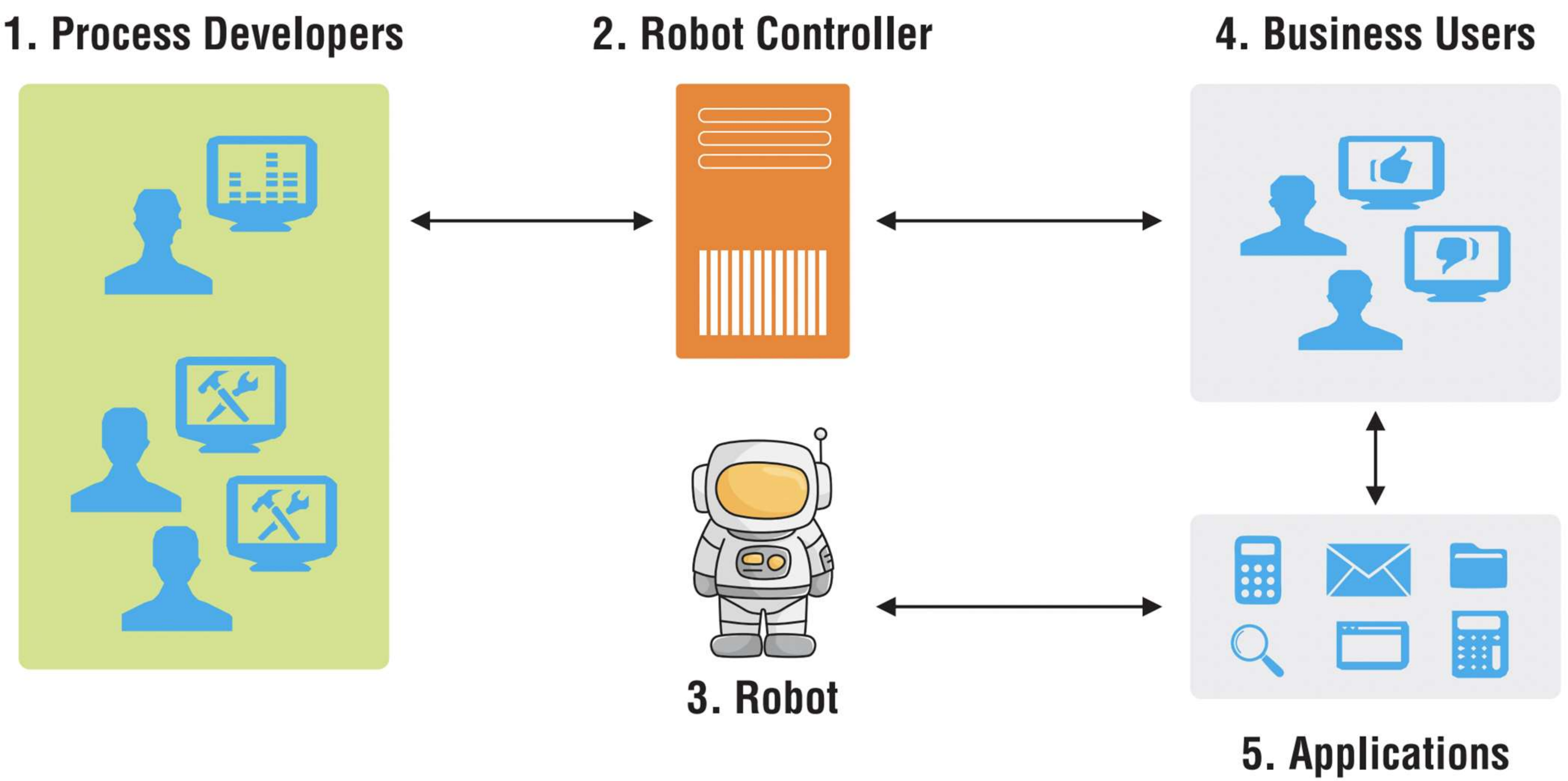
a) Flexibility and scalability

b) Improved accuracy

c) Improved employee morale

d) AOTA

How does RPA work?



32. Following could be the areas for RPA implementation, which when targeted will result in higher and better return on investment; except

a) **Processes requiring High Volume Transactions**

b) **Items Prone to Errors or Re-work**

c) **Significant machine work involved**

d) **High predictability**

33. A single digitally signed instruction was given to a financial institution to credit a customer's account. The financial institution received the instruction three times and credited the account three times. Which of the following would be the MOST appropriate control against such multiple credits?

a) Encrypting the hash of the payment instruction with the public key of the financial institution

b) Affixing a time stamp to the instruction and using it to check for duplicate payments

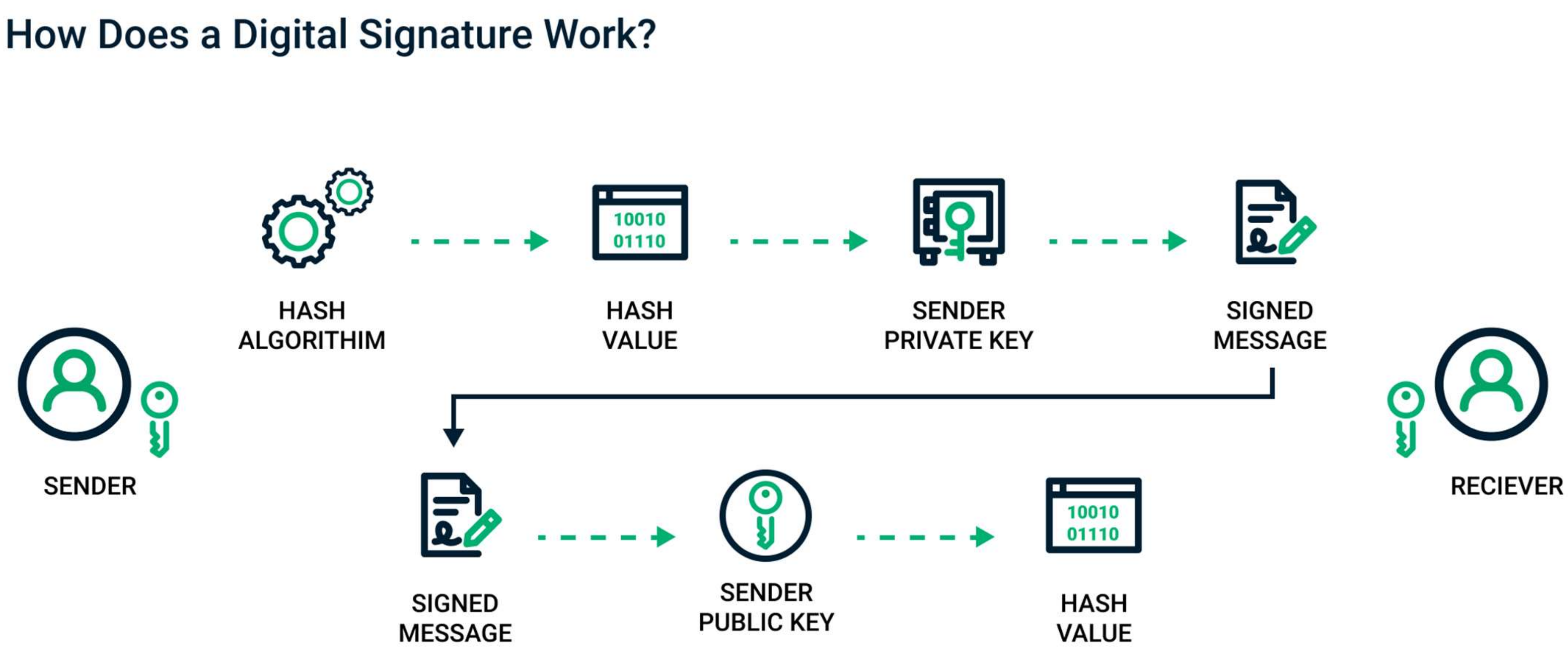
c) Encrypting the hash of the payment instruction with the private key of the instructor

d) Affixing a time stamp to the hash of the instruction before having it digitally signed by the instructor

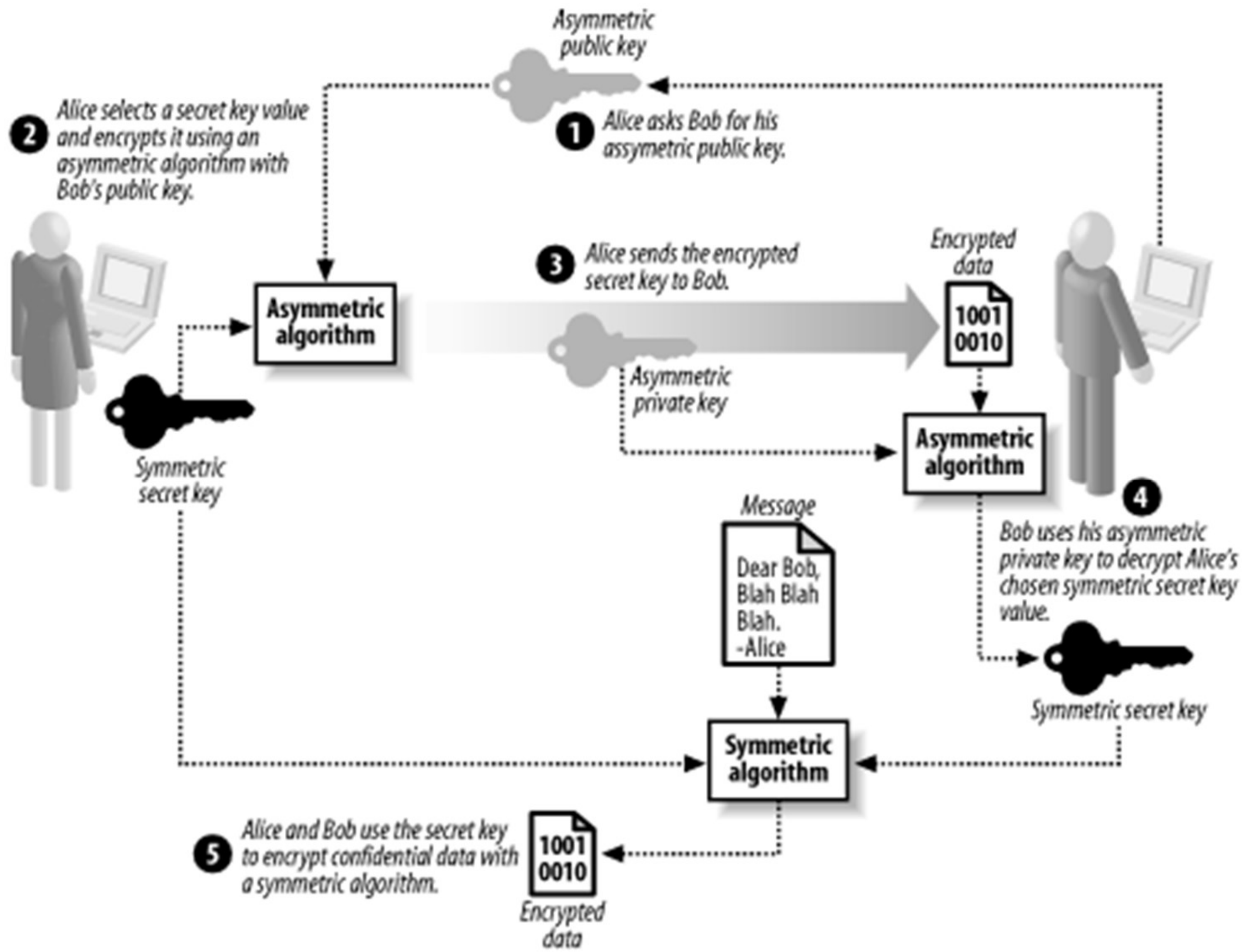
Public Key Infrastructure

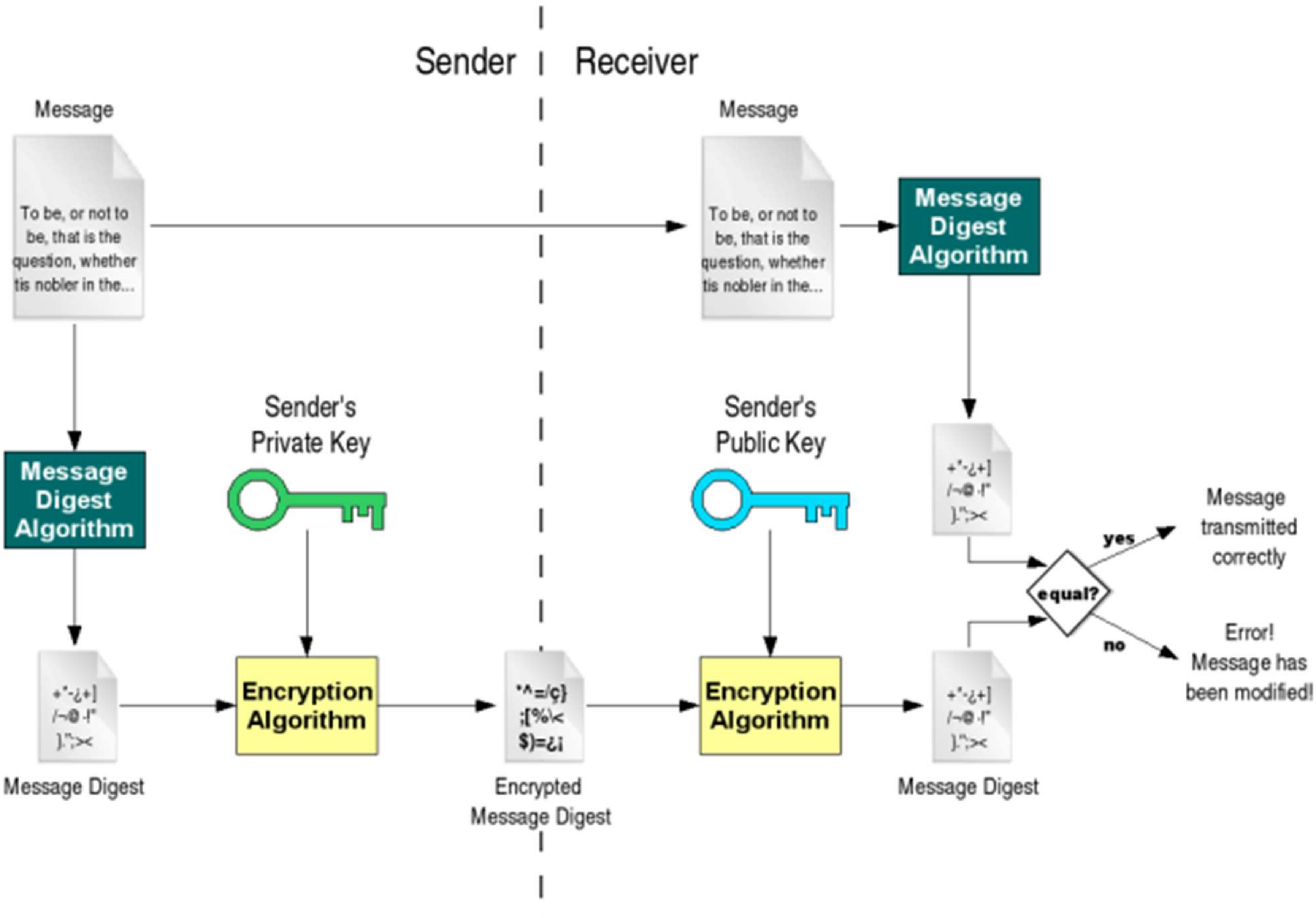
Purpose	Encrypt	Decrypt	Encrypt / Decrypt
Integrity	Sender Private Key	Sender Public Key	Message Digest
Confidentiality	Receiver Public Key	Receiver Private Key	Secret Key

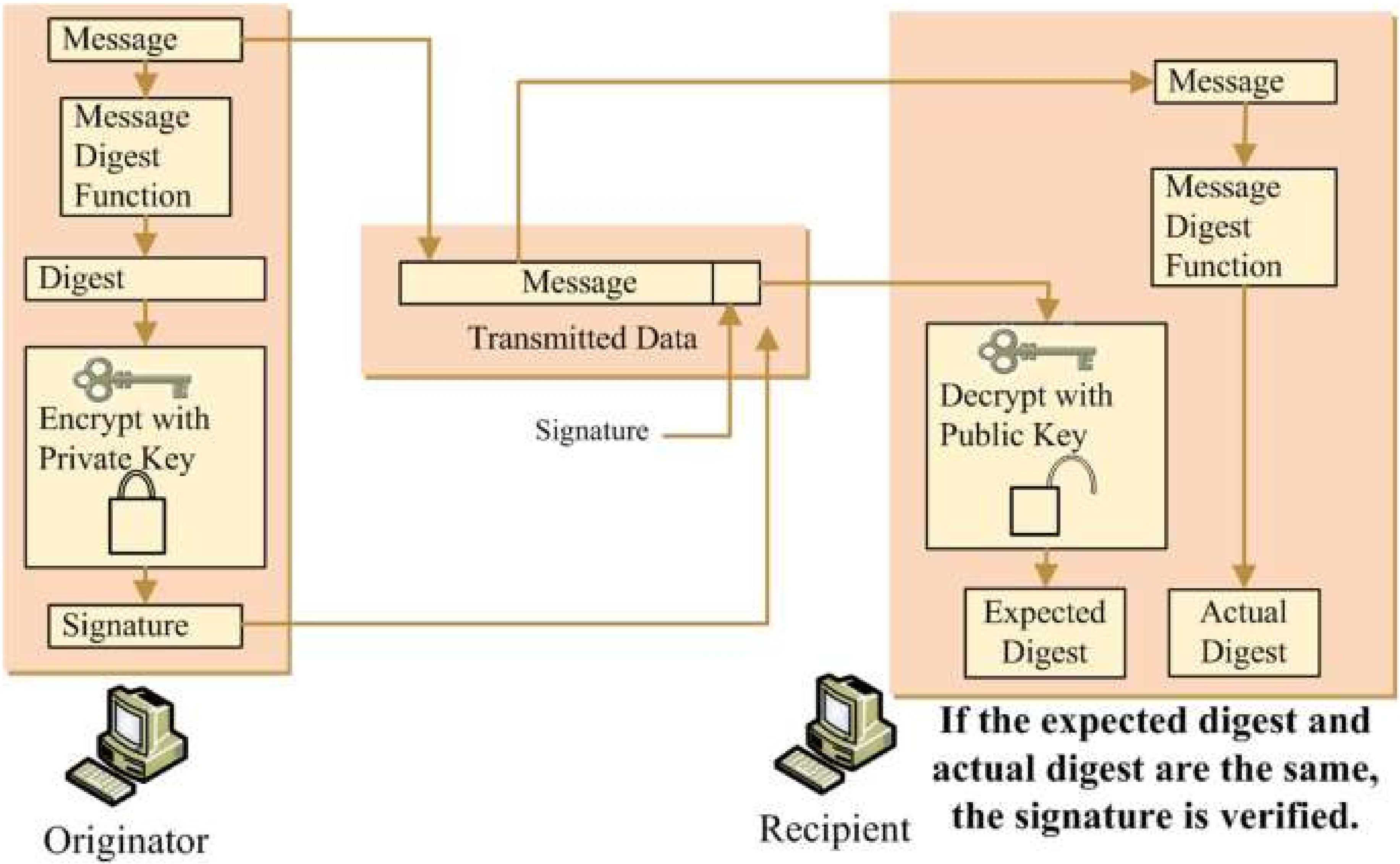
Data Integrity



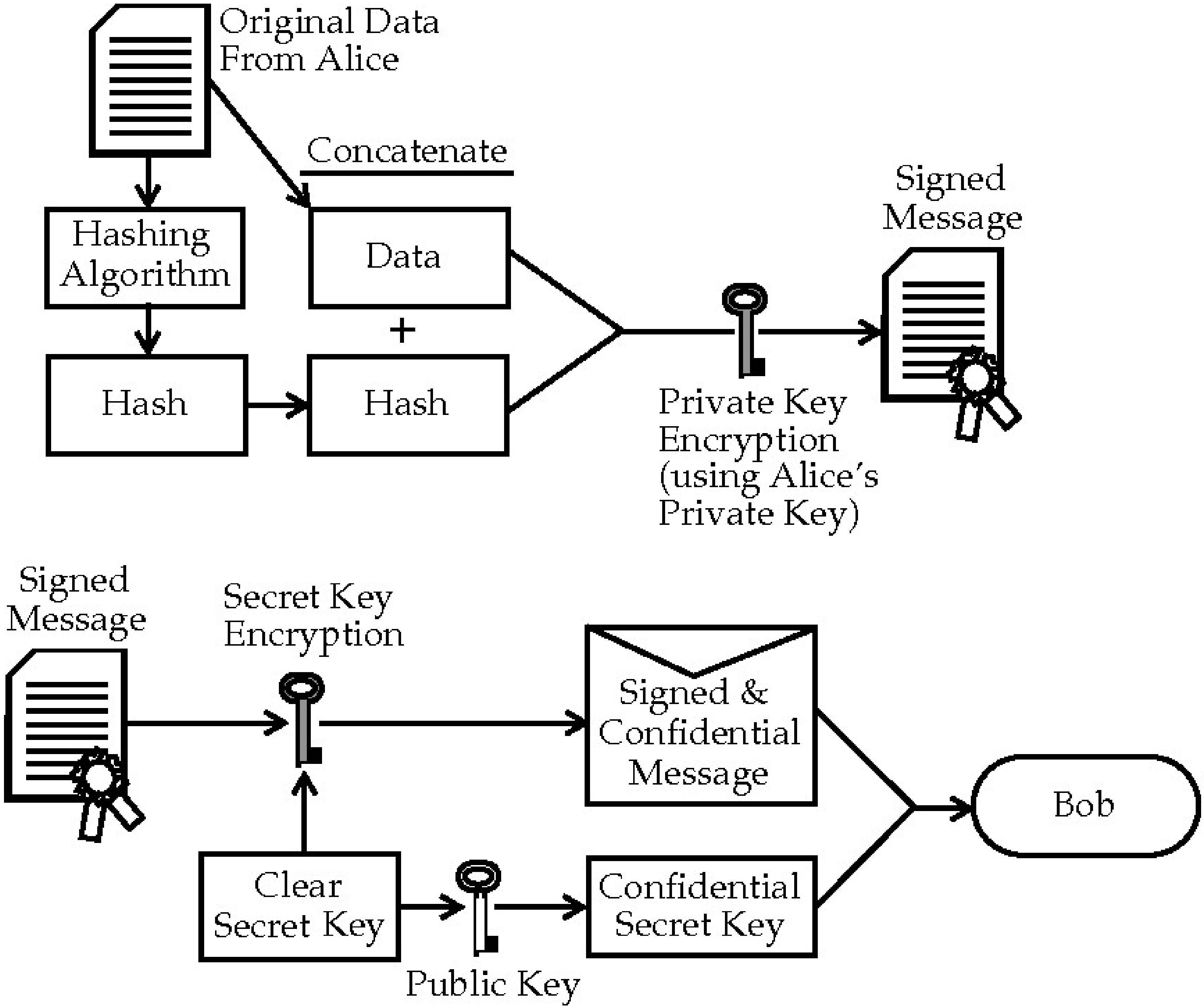
Exchanging symmetric keys using asymmetric encryption



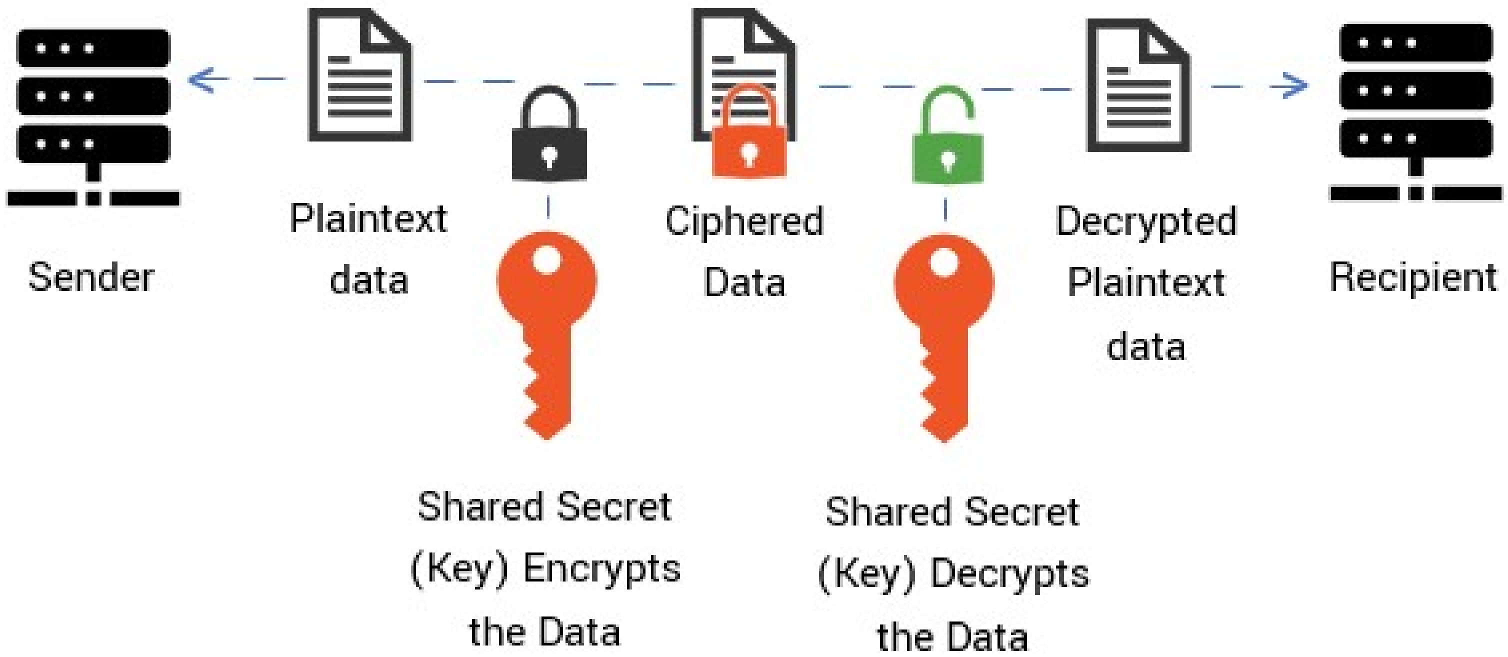

Sender
Receiver
Message
To be, or not to be, that is the question, whether tis nobler in the...
Message
To be, or not to be, that is the question, whether tis nobler in the...
Message Digest Algorithm
Message Digest Algorithm
Sender's Private Key
Sender's Public Key
Encryption Algorithm
Encryption Algorithm
Message Digest
Encrypted Message Digest
Message Digest
equal?
yes
Message transmitted correctly
no
Error! Message has been modified!



If the expected digest and actual digest are the same, the signature is verified.


Original Data
From Alice
Concatenate
Hashing
Algorithm
Data
+
Hash
Hash
Private Key
Encryption
(using Alice's
Private Key)
Signed
Message
Signed
Message
Secret Key
Encryption
Signed &
Confidential
Message
Bob
Clear
Secret Key
Public Key
Confidential
Secret Key

Private Key Encryption (Symmetric)



34. When using public key encryption to secure data being transmitted across a network:

a) both the key used to encrypt and decrypt the data are public.

b) the key used to encrypt is private, but the key used to decrypt the data is public.

c) the key used to encrypt is public, but the key used to decrypt the data is private.

d) both the key used to encrypt and decrypt the data are private.

What is in a Digital Certificate?

- Digital certificates contain specific pieces of information, as determined by the X.509 standard. X.509 is the Authentication framework part of the X.500 series of standards.
- Digital certificates contain at least the following information about the entity being certified:
  - The owner's public key
  - The owner's Distinguished Name
  - The Distinguished Name of the CA that issued the certificate
  - The date from which the certificate is valid
  - The expiry date of the certificate
  - The version number of the certificate data format as defined in X.509. The current version of the X.509 standard is Version 3, and most certificates conform to that version.
  - A serial number. This is a unique identifier assigned by the CA which issued the certificate. The serial number is unique within the CA which issued the certificate: no two certificates signed by the same CA certificate have the same serial number.

What is in a Digital Certificate?......

- An X.509 Version 2 certificate also contains an Issuer Identifier and a Subject Identifier, and an X.509 Version 3 certificate can contain a number of extensions. Some certificate extensions, such as the Basic Constraint extension, are *standard*, but others are implementation-specific. An extension can be *critical*, in which case a system must be able to recognize the field; if it does not recognize the field, it must reject the certificate. If an extension is not critical, the system can ignore it if does not recognize it.
- **The digital signature in a personal certificate is generated using the private key of the CA which signed that certificate. Anyone who needs to verify the personal certificate can use the CA's public key to do so.** The CA's certificate contains its public key.
- **Digital certificates do not contain your private key.** You must keep your private key secret.

35. A Digital Certificate verifies the ……

a) Private key of the subject

b) Public key of the subject

c) Integrity of the subject

d) Strength of the Encryption Algorithm

36. Which of the following cryptography options would increase overhead/cost/time?

a) The encryption is symmetric rather than asymmetric.

b) A long asymmetric encryption key is used.

c) The hash is encrypted rather than the message.

d) A secret key is used.

37. Use of asymmetric encryption in an Internet e-commerce site, where there is one private key for the hosting server and the public key is widely distributed to the customers, is MOST likely to provide comfort to the:

a) customer over the authenticity of the hosting organization.

b) hosting organization over the authenticity of the customer.

c) customer over the confidentiality of messages from the hosting organization.

d) hosting organization over the confidentiality of messages passed to the customer.

38. Private key algorithm is used for …… encryption and public key algorithm is used for ….. encryption.

a) Messages, session key

b) Session key, messages

c) Can be used for both

d) None of the above

39. Which of the following is true about Public Key Infrastructure?

a) PKI is a combination of digital certificates, public-key cryptography, and certificate authorities that provide enterprise wide security.

b) PKI uses two-way symmetric key encryption with digital certificates, and Certificate Authority.

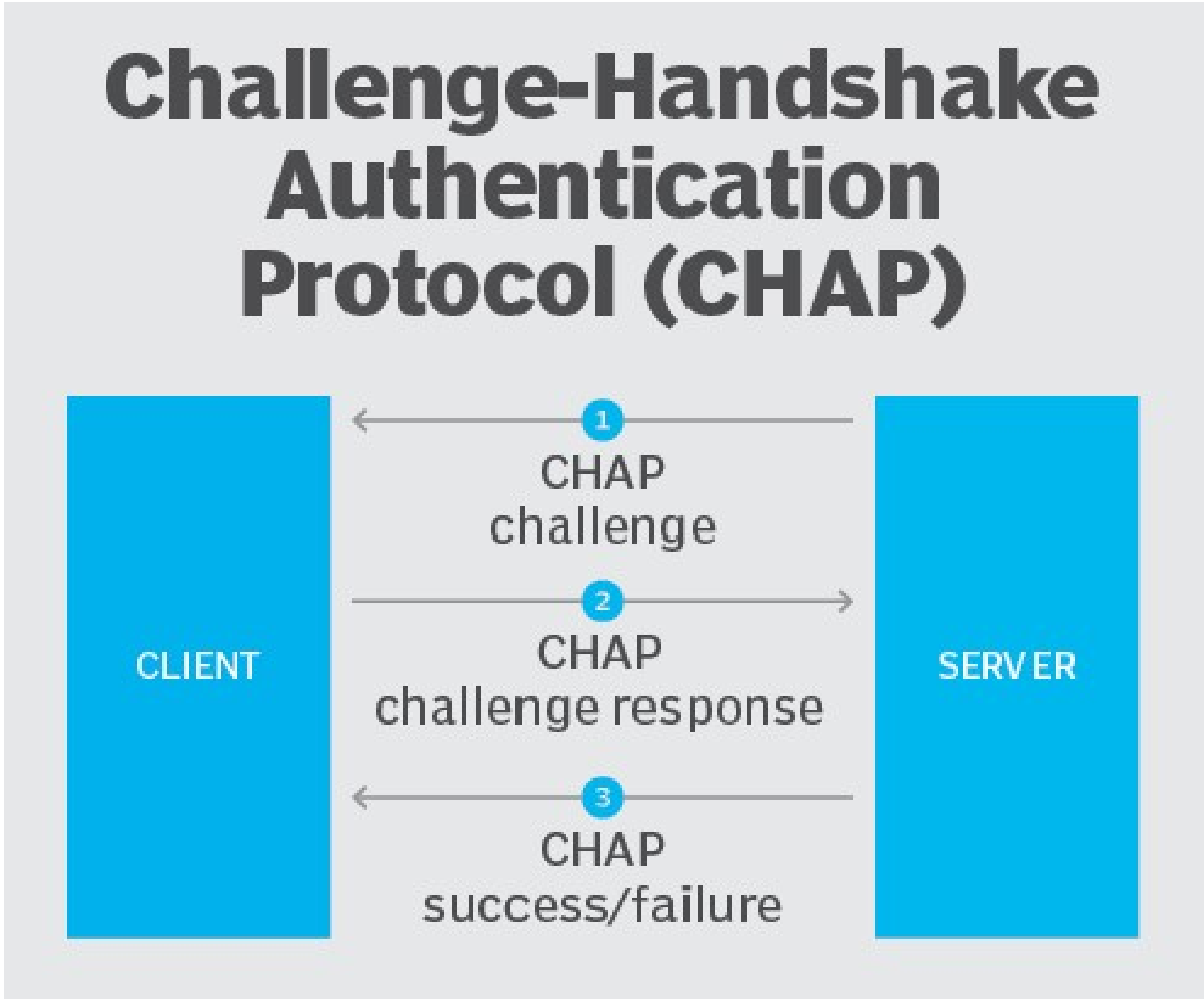
c) PKI uses private and public keys but does not use digital certificates.

d) PKI uses CHAP authentication.

CHAP Authentication

Challenge-Handshake Authentication Protocol (CHAP)

- CHAP is an authentication scheme used by Point-to-Point Protocol (PPP) servers to validate the identity of remote clients.
- CHAP periodically verifies the identity of the client by using a three-way handshake.
- This happens at the time of establishing the initial link (LCP), and may happen again at any time afterwards.
- The verification is based on a shared secret (such as the client's) password
  1. **After the completion of the link establishment phase, the authenticator sends a "challenge" message to the peer.**
  2. **The peer responds with a value calculated using a one-way hash function on the challenge and the secret combined.**
  3. **The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authenticator acknowledges the authentication; otherwise it should terminate the connection.**
  4. **At random intervals the authenticator sends a new challenge to the peer and repeats steps 1 through 3.**


Challenge-Handshake Authentication Protocol (CHAP)
CLIENT
SERVER
1
CHAP challenge
2
CHAP challenge response
3
CHAP success/failure

PAP VERSUS CHAP

PAP	CHAP
A password based authentication protocol used by Point to Point Protocol (PPP) to validate users	A communication protocol that authenticates a user or network host to an authenticating entity
Stands for Password Authentication Protocol	Stands for Challenge Handshake Authentication Protocol
During link establishment, PAP stops working after establishing the authentication, which can lead to attacks on the network	CHAP conducts periodic challenges to make sure that the remote host still has valid password value
Not secure like CHAP	Provide better security than PAP

VISA 4 DISA


SMART CITY
Traffic Management
Education
Air Pollution
Open Data
Internet of Things
Smart Health
Intelligent Shopping
Smart Environment
Electromagnetic Emissions
Smart Buildings
Public Safety
Smart Home
Gas & Water Leak Detection
Smart Street Lights
Smart Energy
Electric Vehicle Charging
Water Quality
Smart Parking
Waste Management

40. ………, one of India's major financial institutions, started its automation journey in 2016. It was one of the first private lenders to adopt software robotics on such a large scale. Using robotic process automation (RPA), the bank's operations department deployed 200 robotics software programs.

a) HDFC Bank

b) Axis Bank

c) HSBC Bank

d) ICICI Bank

Module 6; Page 57; Para 6.6.3

41. Following are applications of RPA in Finance, except

a) Initiating a credit card application

b) Tracking shipments for delivery over GPS

c) KYC authentication

d) Voice recognition and reply

Module 6; Page 57; Para 6.6.2

42. Following are applications of IoT in Finance, except

a) Drone can help gathering evidences to support assertions

b) Cloud-based workplace and process enhancements

c) Tracking shipments for delivery over GPS

d) Reducing time lapse between an event and its recording

Module 6; Page 52; Para 6.5.5

43. The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with ……… and the ability to transfer data over a network without requiring human-to-human or human-to- computer interaction.

a) UIN

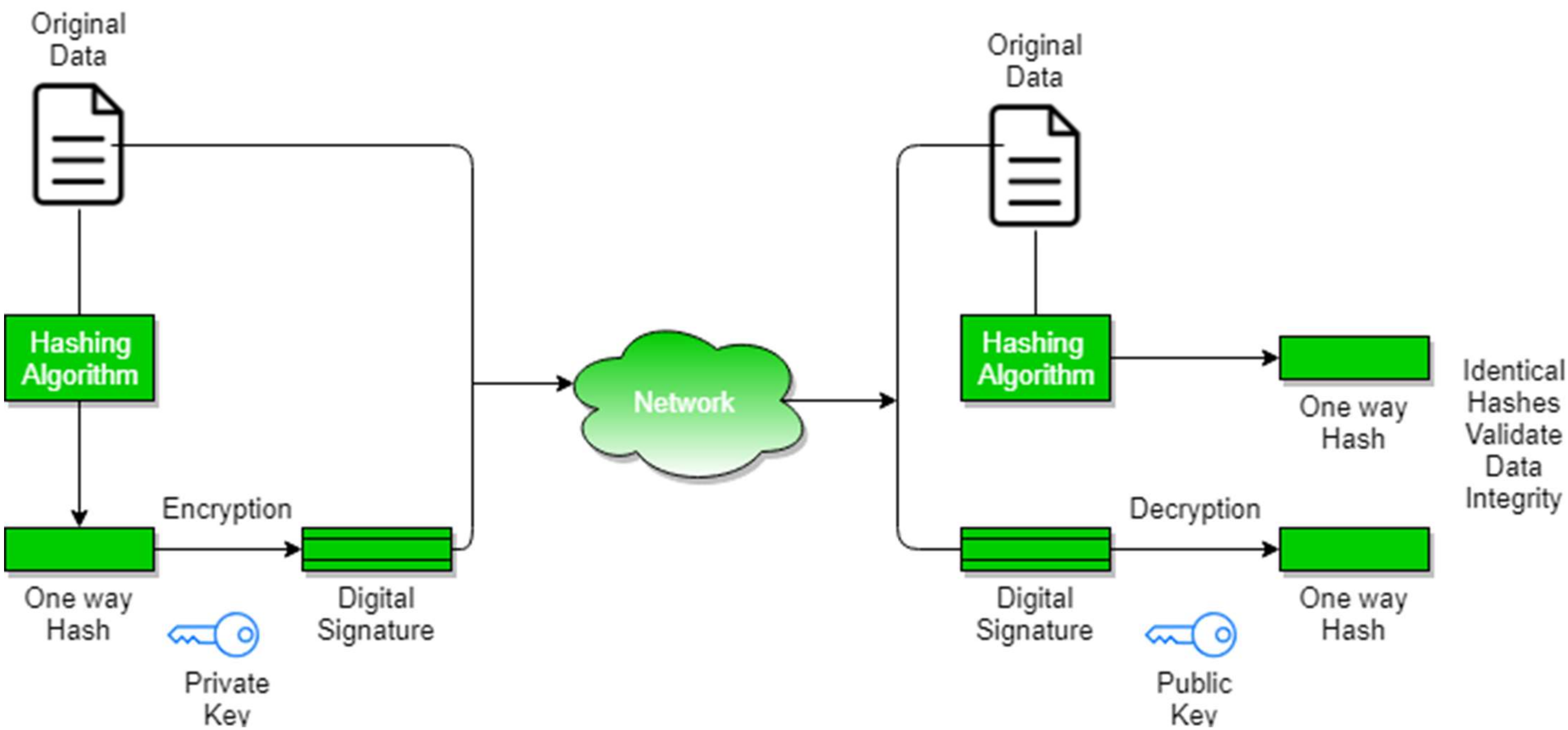
b) UID

c) IMEI

d) MAC

Module 6; Page 47; Para 6.5.1

Data Integrity



44. Digital signatures are designed to provide additional protection for electronic messages in order to determine which of the following?

a) Message read by unauthorized party

b) Message sender verification

c) Message deletion

d) Message modification

Digital Signature

- Digital signatures provide authentication assurance of the email sender.
- A cryptographic process uses the private key of the sender to form a hash value of the message.
- Message hashing provides assurance that the message is from the specified sender and was not modified

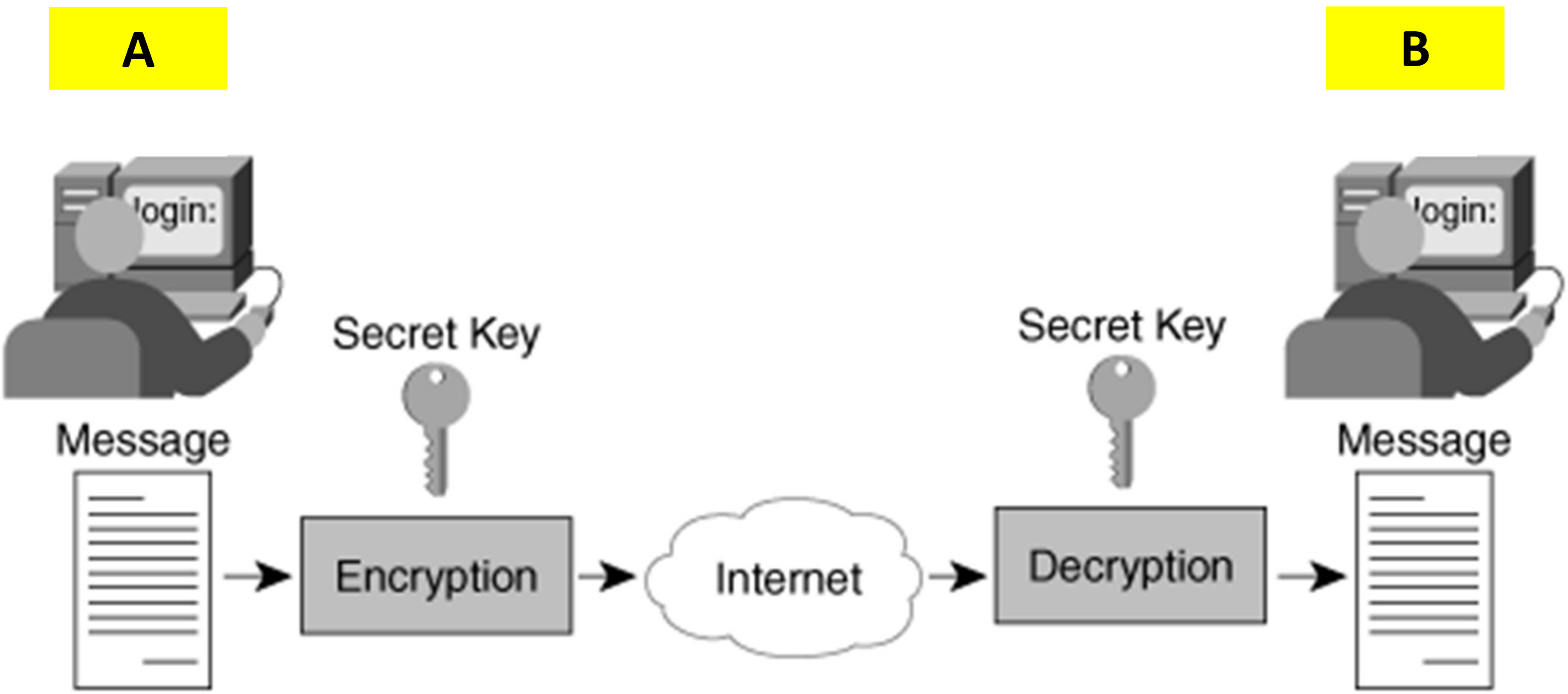
45. Which of the following statements is true concerning asymmetric key cryptography?

a) The sender encrypts the files by using the recipient's private key.

b) The sender and receiver use the same key.

c) Asymmetric keys cannot be used for digital signatures.

d) The sender and receiver have different keys


A
B
login:
login:
Secret Key
Secret Key
Message
Message
Encryption
Internet
Decryption

46. Using public-key interchange (PKI) encryption, which key is used by the sender for authentication of the receiving party?

a) Sender's private key

b) Recipient's private key

c) Recipient's public key

d) Sender's public key

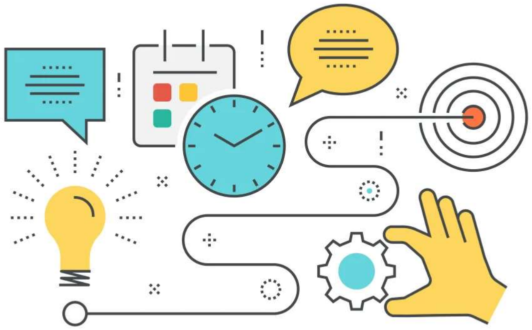
47. When auditing the use of encryption, which of the following would be the primary concern of the auditor?

a) Management's level of control over the use of encryption

b) Strength of encryption algorithm in use

c) Key sizes used in the encryption and decryption process

d) Using the correct encryption method for compliance



48. Which of the following common methods is typically not used by hackers to remotely control encryption keys which exist unencrypted in executable RAM memory?

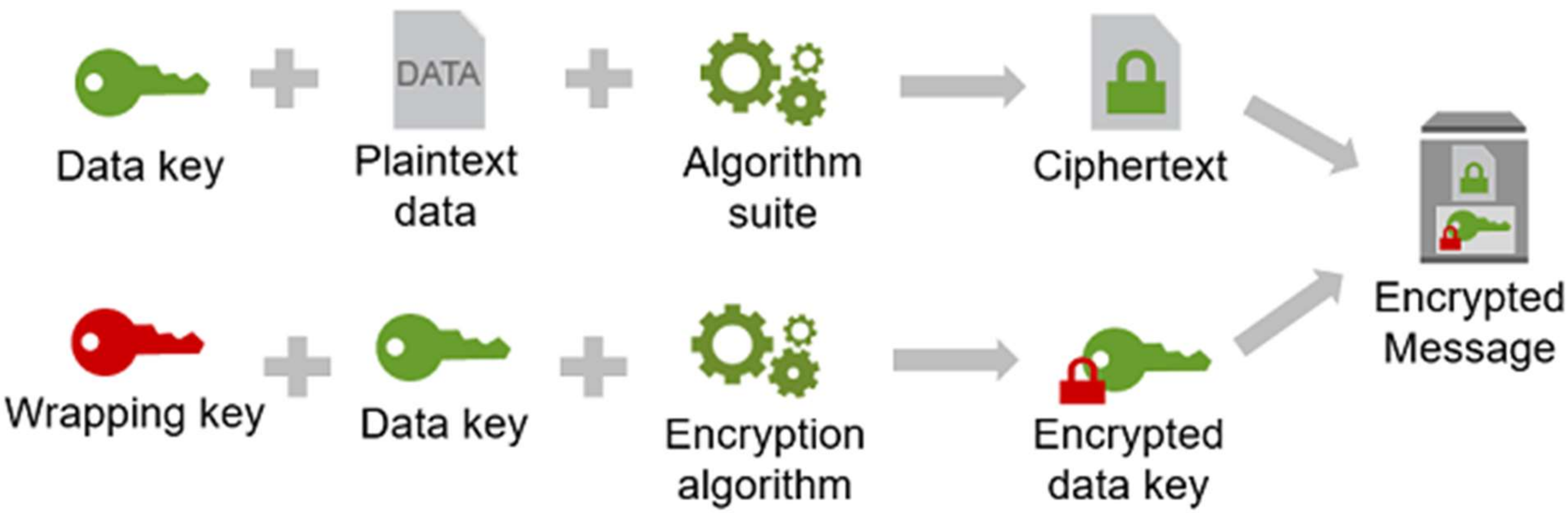
a) Malware downloading and installing a Trojan horse utility without the user's knowledge

b) Remotely gaining unencrypted access to POS/computers on the internal store LAN before encryption occurs for transmission

c) Gaining physical access into the system using social engineering

d) Gaining unauthorized access using static passwords in configuration files intended for program-to-program access

Key Wrapping



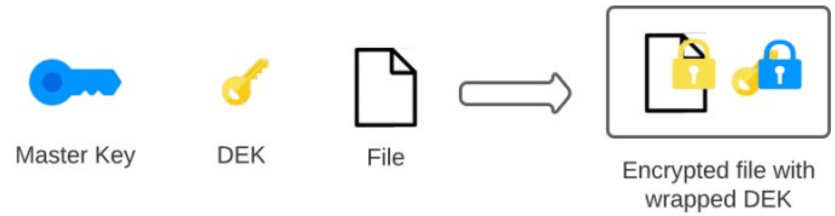
49. Which of the following techniques is used in the storage and transmission of a symmetric encryption key?

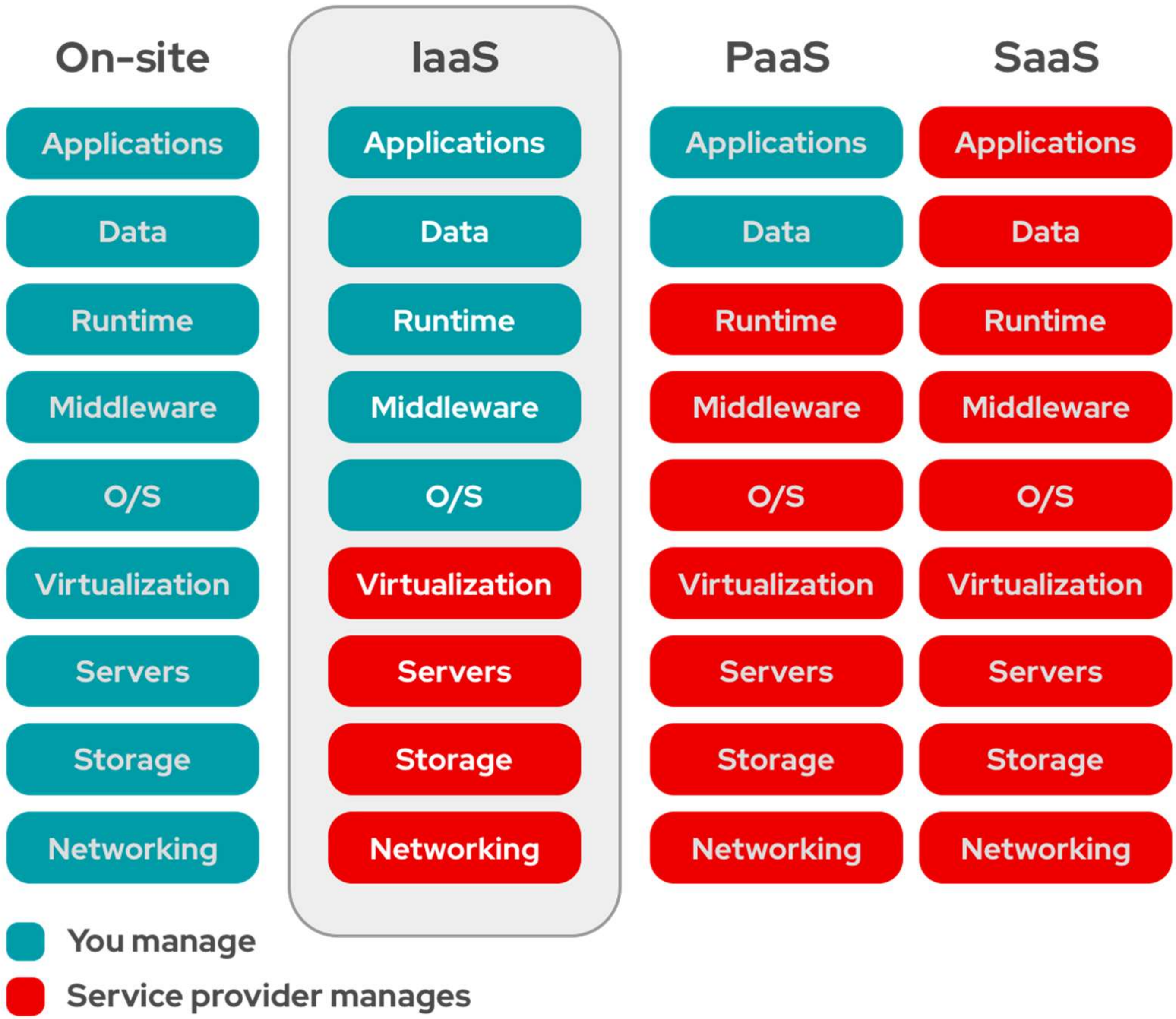
a) Key rotation

b) Generating a unique encryption key

c) Key wrapping

d) Generating a shared encryption key




On-site
IaaS
PaaS
SaaS
Applications
Data
Runtime
Middleware
O/S
Virtualization
Servers
Storage
Networking
You manage
Service provider manages

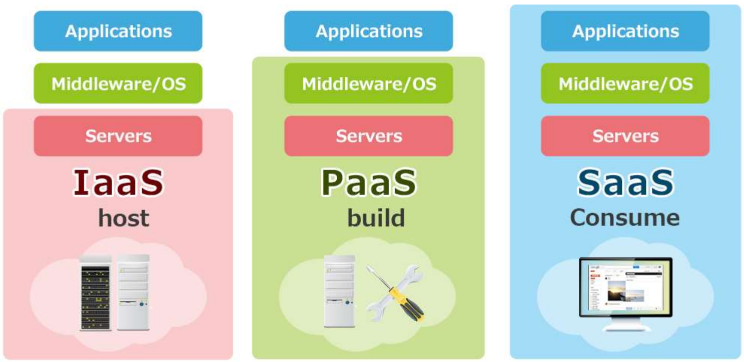
50. When using an Infrastructure as a Service (IaaS) solution, what is the **primary benefit** for the customer?

a) Scalability

b) Metered service

c) Energy and cooling efficiencies

d) Transfer of ownership cost



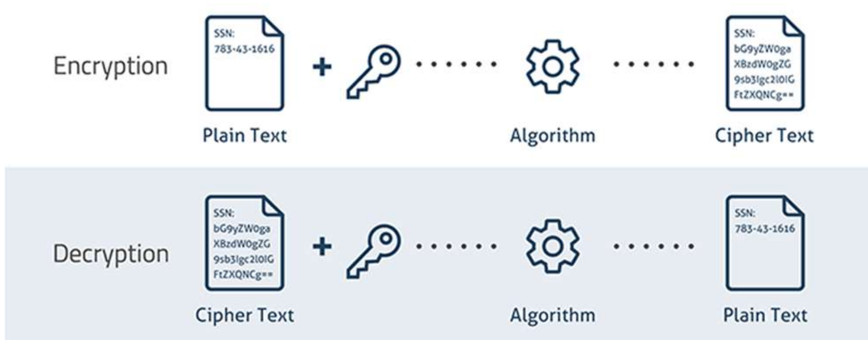
51. What is a special mathematical code that allows encryption hardware/software to encode and then decipher an encrypted message called?

a) PKI

b) Encryption key

c) Public key

d) Masking



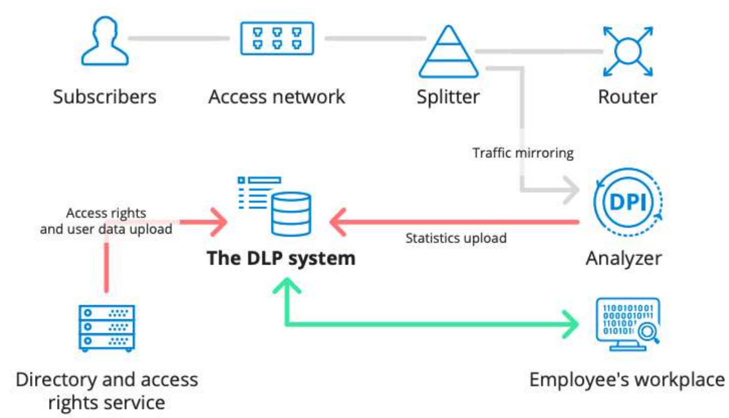
52. What is the term for the assurance that a specific author actually created and sent a specific item to a specific recipient, and that the message was successfully received?

a) Public Key Infrastructure - PKI

b) Data Loss Prevention - DLP

c) Nonrepudiation

d) Bit splitting



Non-Repudiation

- Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

In digital security, non-repudiation means:

- A service that provides proof of the integrity and origin of data.
- An authentication that can be said to be genuine with high confidence.
- An authentication that the data is available under specific circumstances, or for a period of time: data availability.

Obfuscation

- **Obfuscation** is the obscuring of the intended meaning of communication by making the message difficult to understand, usually with confusing and ambiguous language.
- **Cyber Obfuscation** refers to the process of concealing something important, valuable, or critical. Cybercriminals use obfuscation to conceal information such as files to be downloaded, sites to be visited, etc.

Shredding

- **Cyber-Shredding :** The process of destroying data stored on tapes, hard disks and other forms of electronic media so that it is completely unreadable and cannot be accessed.
- **Crypto-shredding :** Is the practice of 'deleting' data by deliberately deleting or overwriting the encryption keys. This requires that the data have been encrypted.

53. What is the correct term for the process of deliberately destroying the encryption keys used to encrypt data?

a) Poor key management

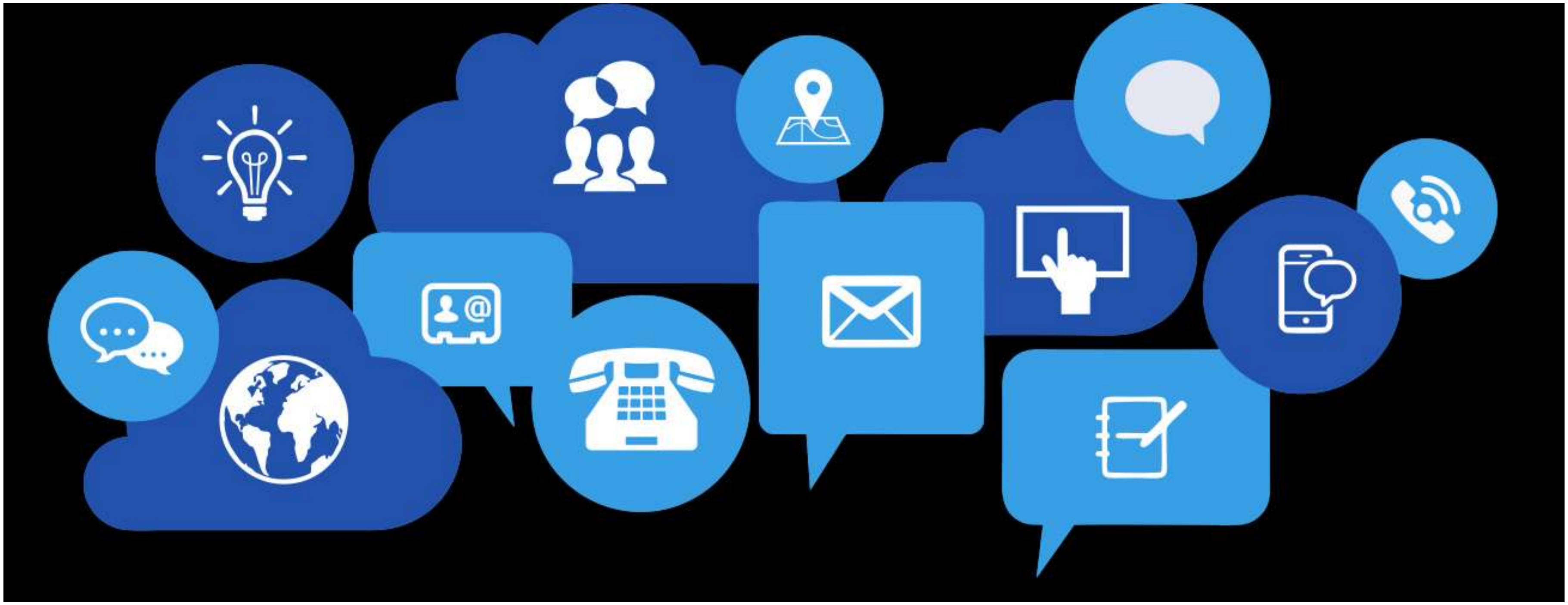
b) PKI

c) Obfuscation

d) Crypto-shredding

1		**11**		**21**		**31**		**41**		**51**	
2		**12**		**22**		**32**		**42**		**52**	
3		**13**		**23**		**33**		**43**		**53**	
4		**14**		**24**		**34**		**44**		**54**	
5		**15**		**25**		**35**		**45**		**55**	
6		**16**		**26**		**36**		**46**		**56**	
7		**17**		**27**		**37**		**47**		**57**	
8		**18**		**28**		**38**		**48**		**58**	
9		**19**		**29**		**39**		**49**		**59**	
10		**20**		**30**		**40**		**50**		**60**	

Please share your answers in the blog with your email-id to get the key



CA Dr GOPAL KRISHNA RAJU

Chartered Accountant, Insolvency Professional & Registered Valuer

Partner : K GOPAL RAO & CO | Chartered Accountants | Mumbai, Chennai, Bengaluru, Hyderabad, Trichy, Madurai & Tiruvallur

Email: gkr@icai.org Blog: www.3spro.blogspot.com

Mobile: 98400 63269 | 98401 63269