Cryptography

Objectives

After completing this unit, you should be able to:

- Understand Cryptography and Crypto System
- Learn about Cryptographic Algorithms
- Know Hash Functions in Cryptography
- Understand about Cryptographic Digital Signature
- Know about Key Agreement & Public Key Infrastructure
- Understand various attacks against Encrypted Data

Cryptography Basics

FTVETI

ICT @ FTVETI

Key Terms

Plaintext: Original data which may be in the form of message, text or object)

Cipher text: Coded data such as message, text or object

Cipher: Algorithm for transforming Plaintext to Cipher text

Key: Information used in Cipher known only to sender & receiver

Encipher (encryption): Process of converting Plaintext to Cipher text

Key Terms

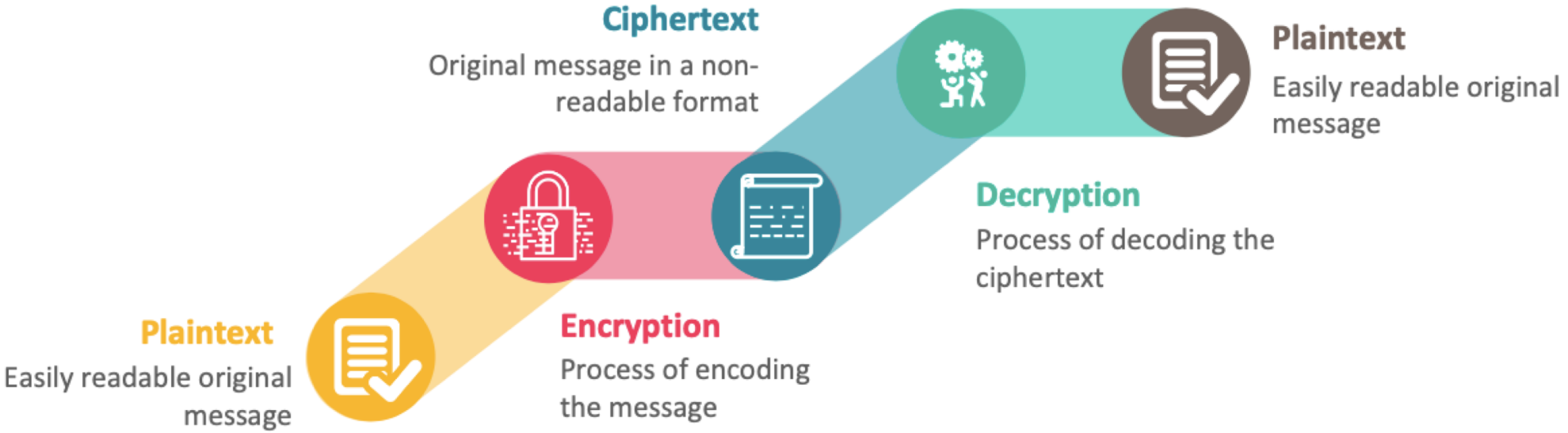
Decipher (decryption): Process of derivation of Plaintext from Cipher text

Cryptography: Study of encryption principles and methods

Cryptanalysis: Study of methods of deciphering Cipher text without knowing the actual Key

Cryptology: Domain of Cryptography and Cryptanalysis

Encryption – Decryption Process Flow



Security Features Of Cryptography

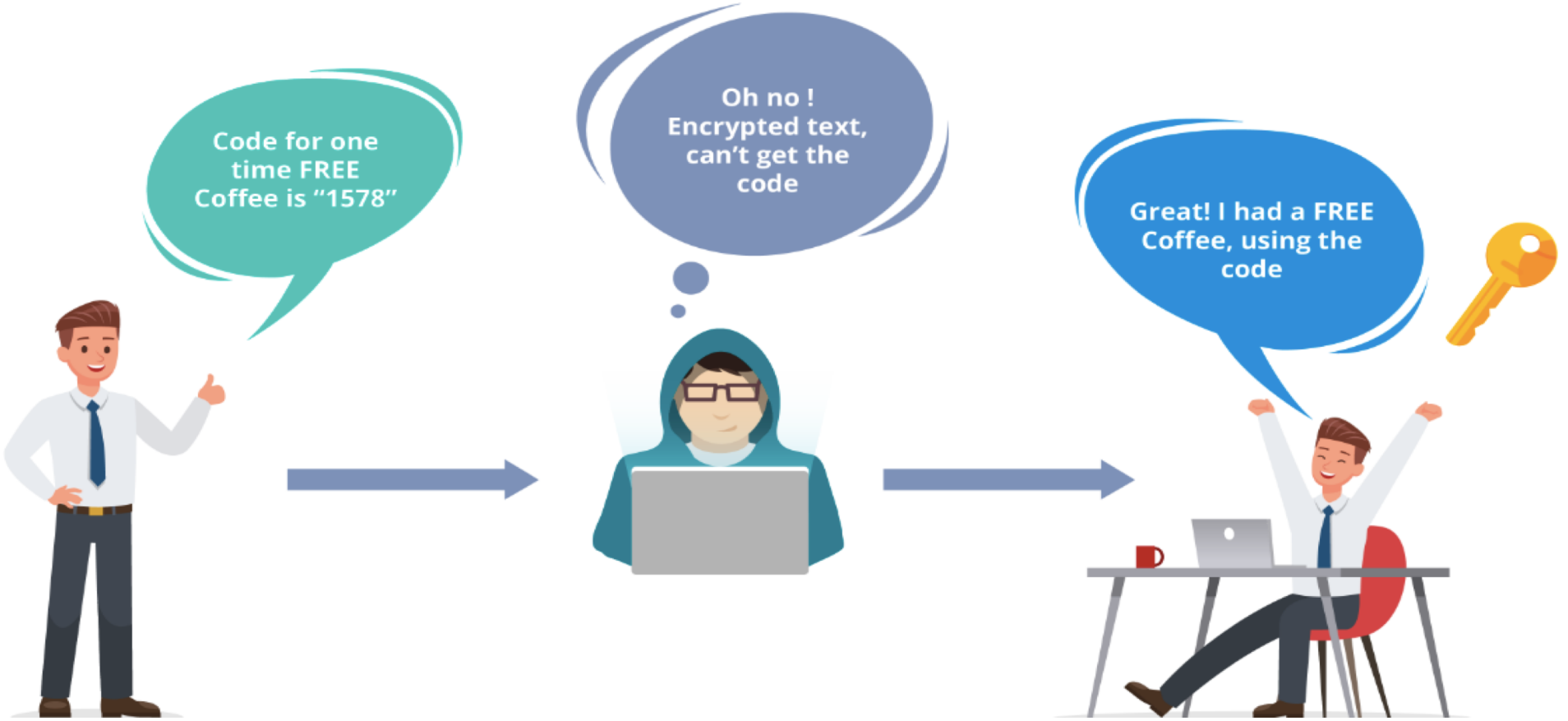
Confidentiality
No one other than authorized party can read the encrypted message

Authentication
Verification of Identity

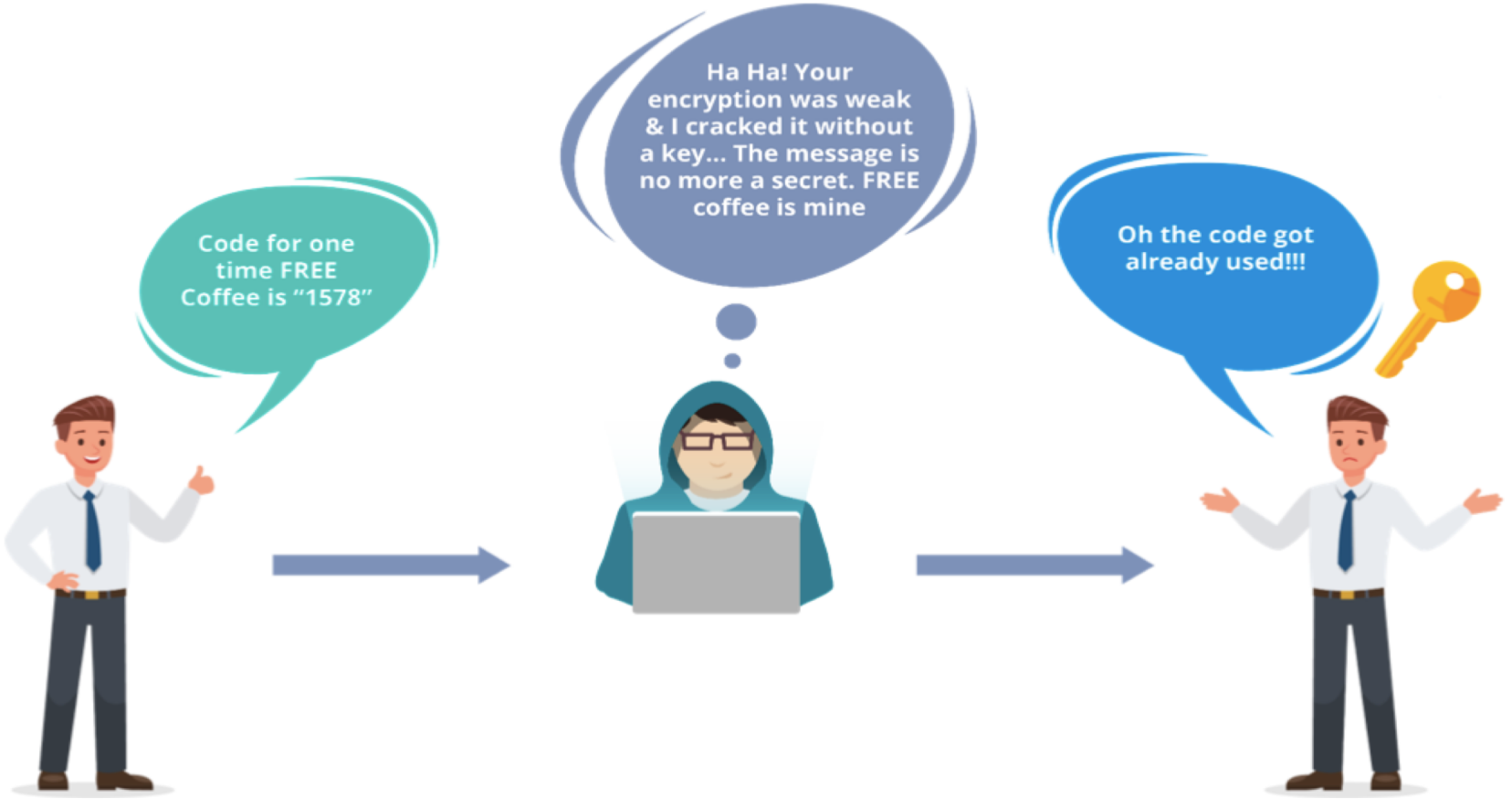
Data Integrity
Was the data tampered?

Non-repudiation
Non Denial

Cryptography – Use Case



Cryptanalysis



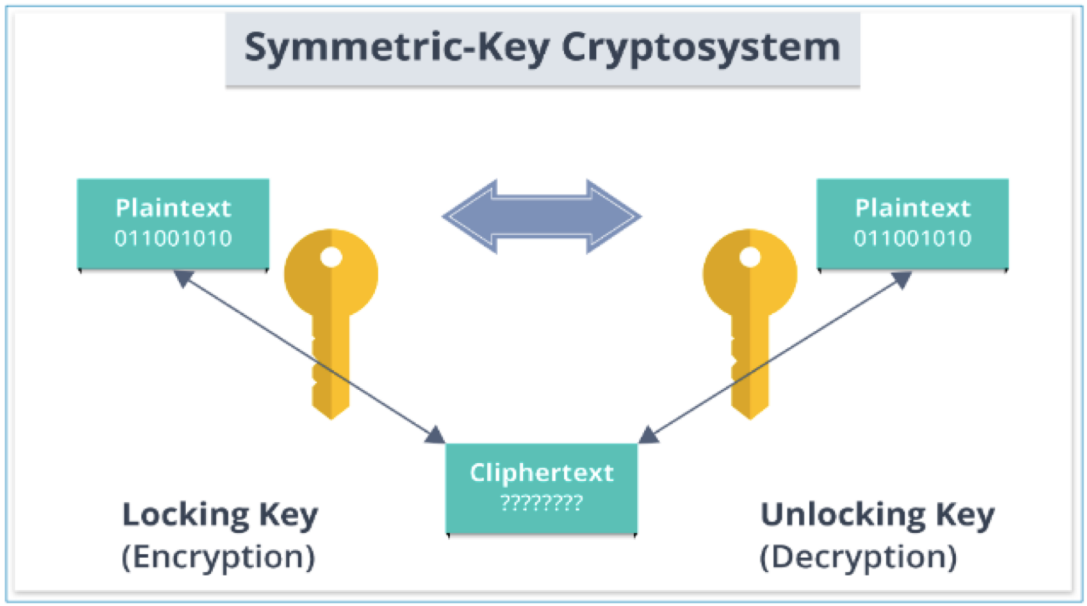
After understanding the ways or techniques used in Cryptography, we need to implement the same, the implementation of cryptographic techniques is know as **Crypto-System**

Crypto – Systems

FTVETI

ICT @ FTVETI

What Is A Cryptosystem?

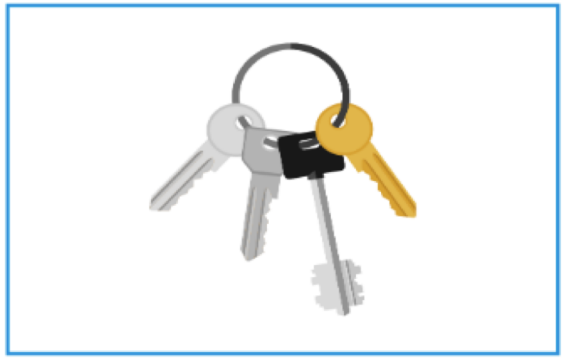


Implementation of cryptographic techniques & their associated infrastructure to provide information security services is known as Cryptosystem

Types Of Cryptosystems

Symmetric Encryption

Same keys are used for encrypting and decrypting the data



Asymmetric Encryption

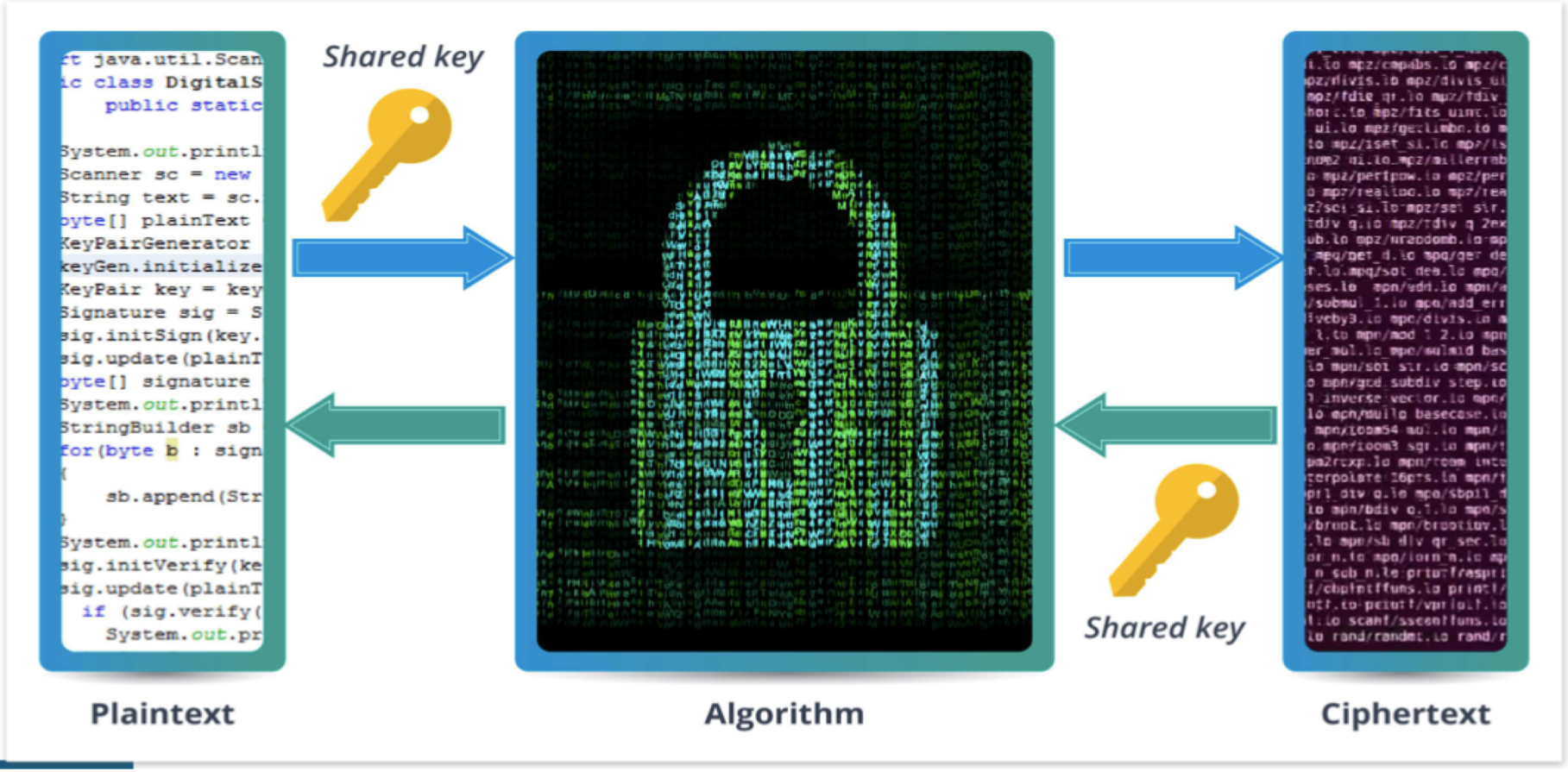
Different keys are used for encrypting and decrypting the data

Symmetric Encryption
(Private Key Cryptography)

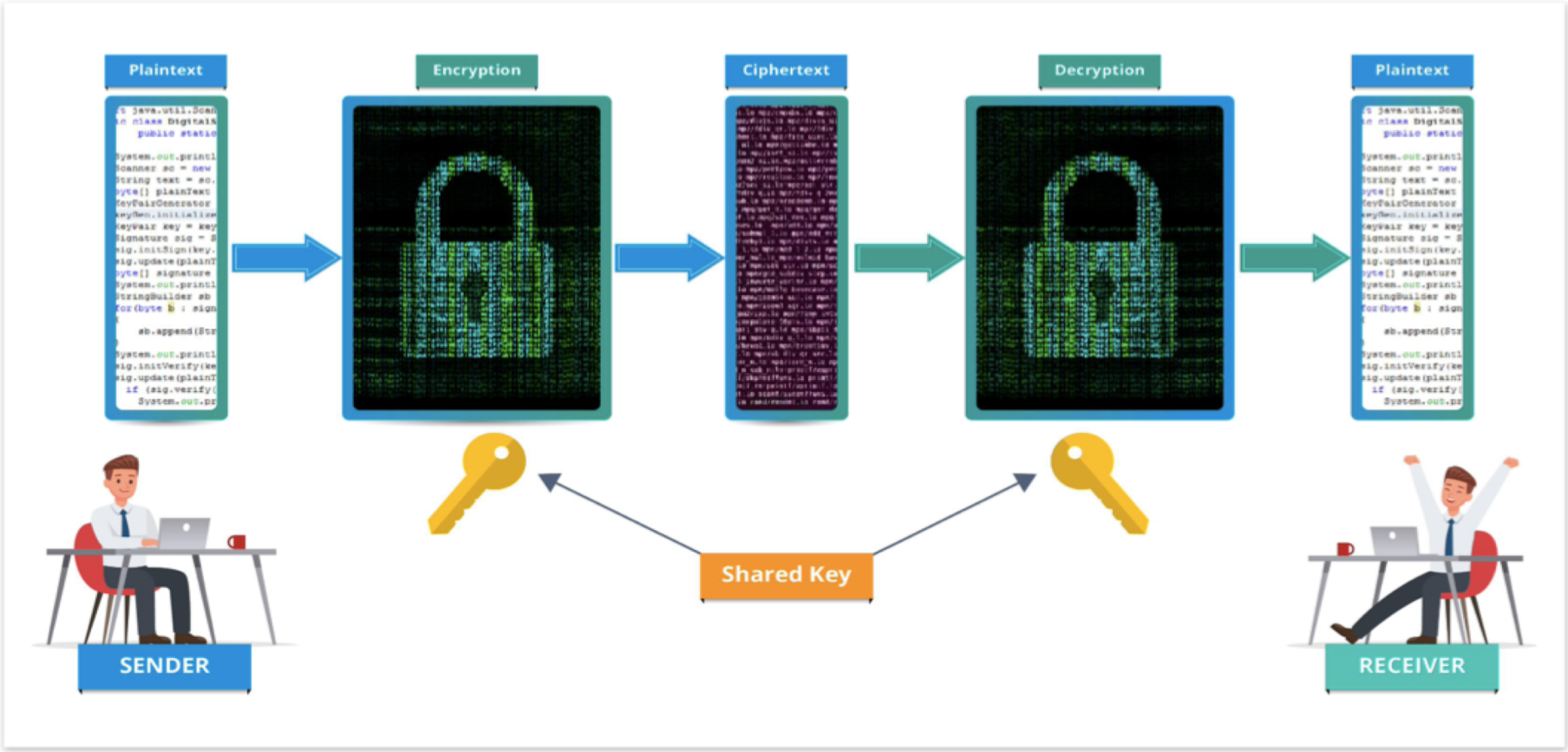
FTVETI

ICT @ FTVETI

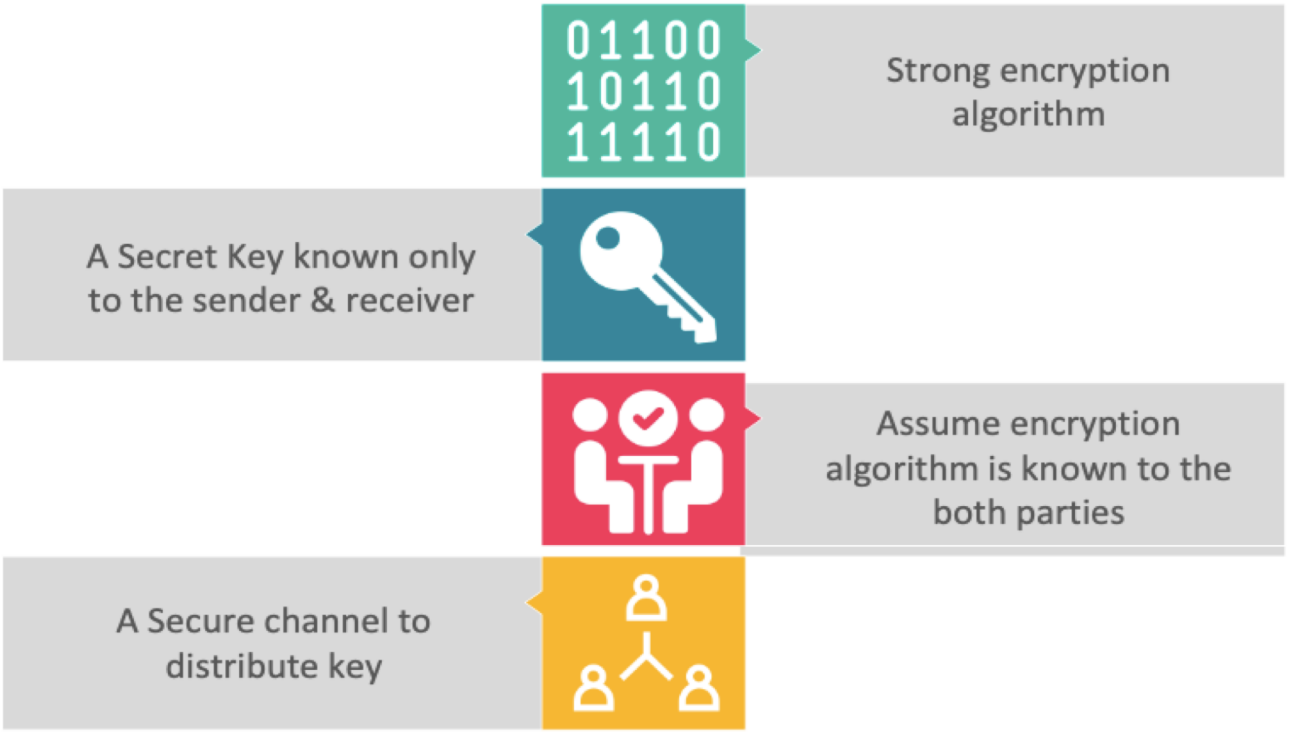
Symmetric – Key Cryptography



Symmetric – Key Cryptography



Requirements Of Symmetric Encryption



How Strong Is Cryptography Components?

Strength of algorithm is determined by the size of the key. The longer the key the more difficult it is to crack

Key length is expressed in bits. Typical key sizes varies between 48 bits and 448 bits

Set of possible keys for a cipher is called key space.

- For 40-bit key there are 2^40 possible keys
- For 128-bit key there are 2^128 possible keys
- Each additional bit added to the key length doubles the security

To crack the key the hacker has to use brute-force

It will take 272 times longer to crack a 128-bit key

Key Challenges Of Symmetric Encryption

Establishment and Sharing of a common KEY

- Before any communication, both the sender and the receiver need to agree on a secret key
- It requires a secure key establishment AND sharing in place
- Secured Key Sharing becomes a biggest challenge !

Maintaining Trust

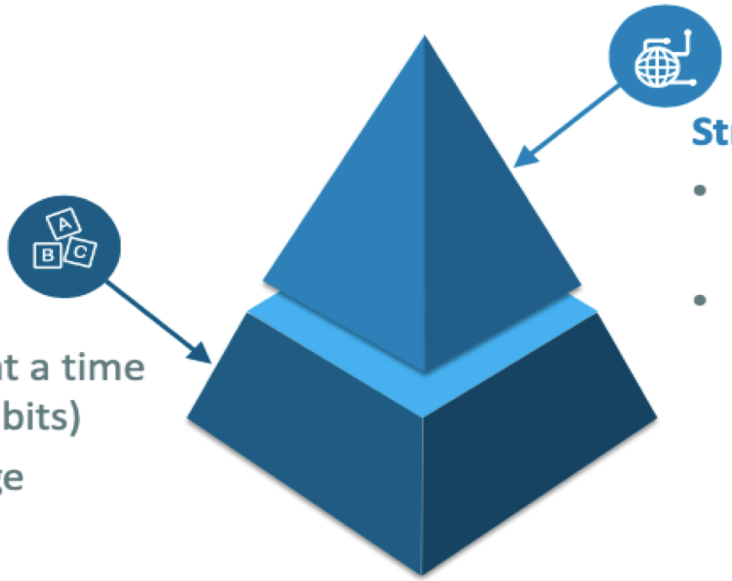
- Since the sender and the receiver use the same secret key, there is an implicit requirement that the sender and the receiver 'trust' each other
- For example, it may happen that the receiver has lost the key to an attacker and the sender is not informed

Symmetric Key Algorithms

There are 2 types of Symmetric Keys:-

Block Ciphers

- Encrypt data one block at a time (typically 64 bits, or 128 bits)
- Used for a single message



Stream Ciphers

- Encrypt data one bit or one byte at a time
- Used if data is a constant stream of information

Example of popular symmetric-key algorithms include Two-fish, Serpent, AES, Blowfish, CAST5, RC4, 3DES, Skipjack and so on

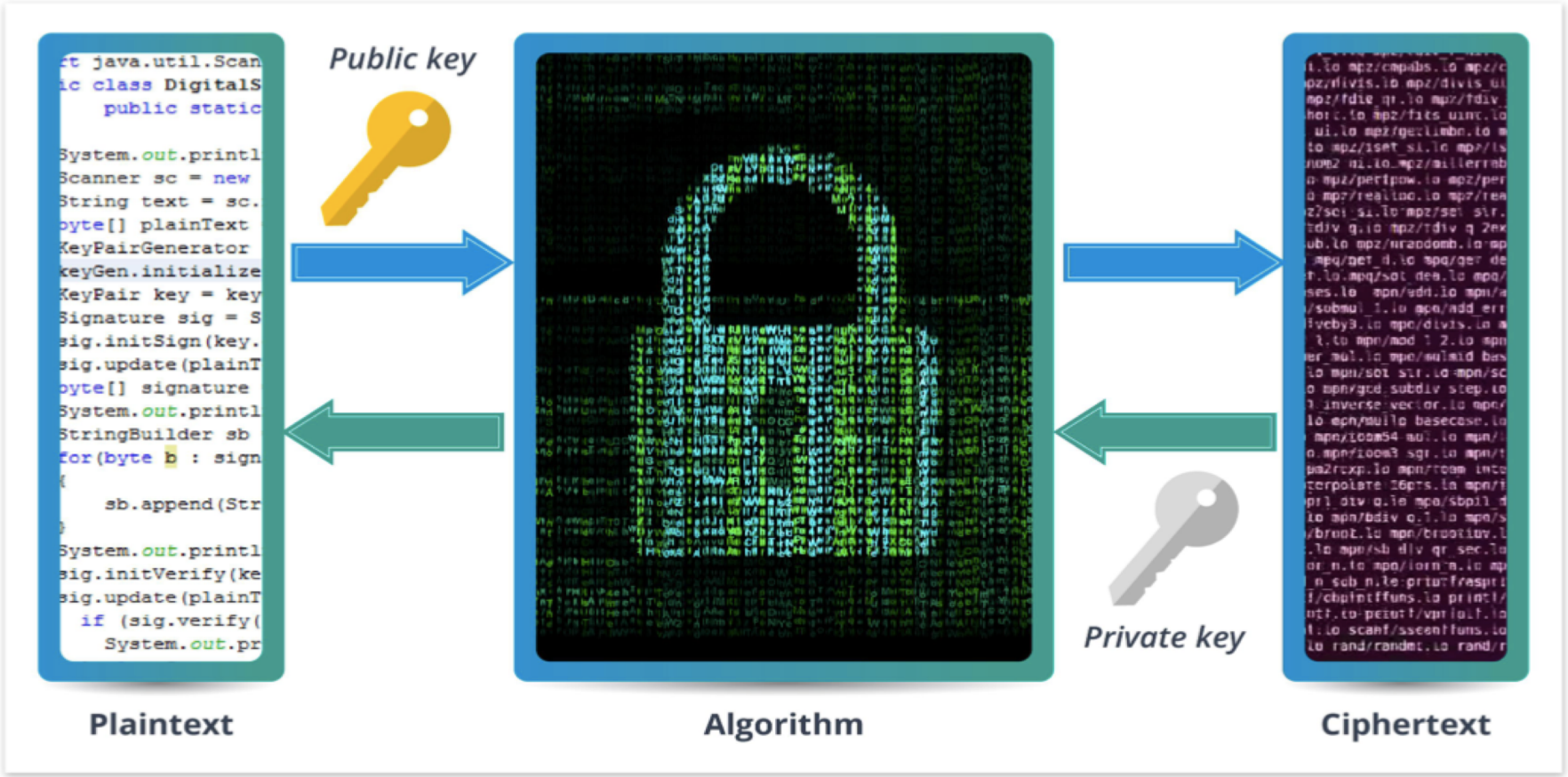
Asymmetric Encryption
(Public Key Cryptography)

What Is Asymmetric Encryption?

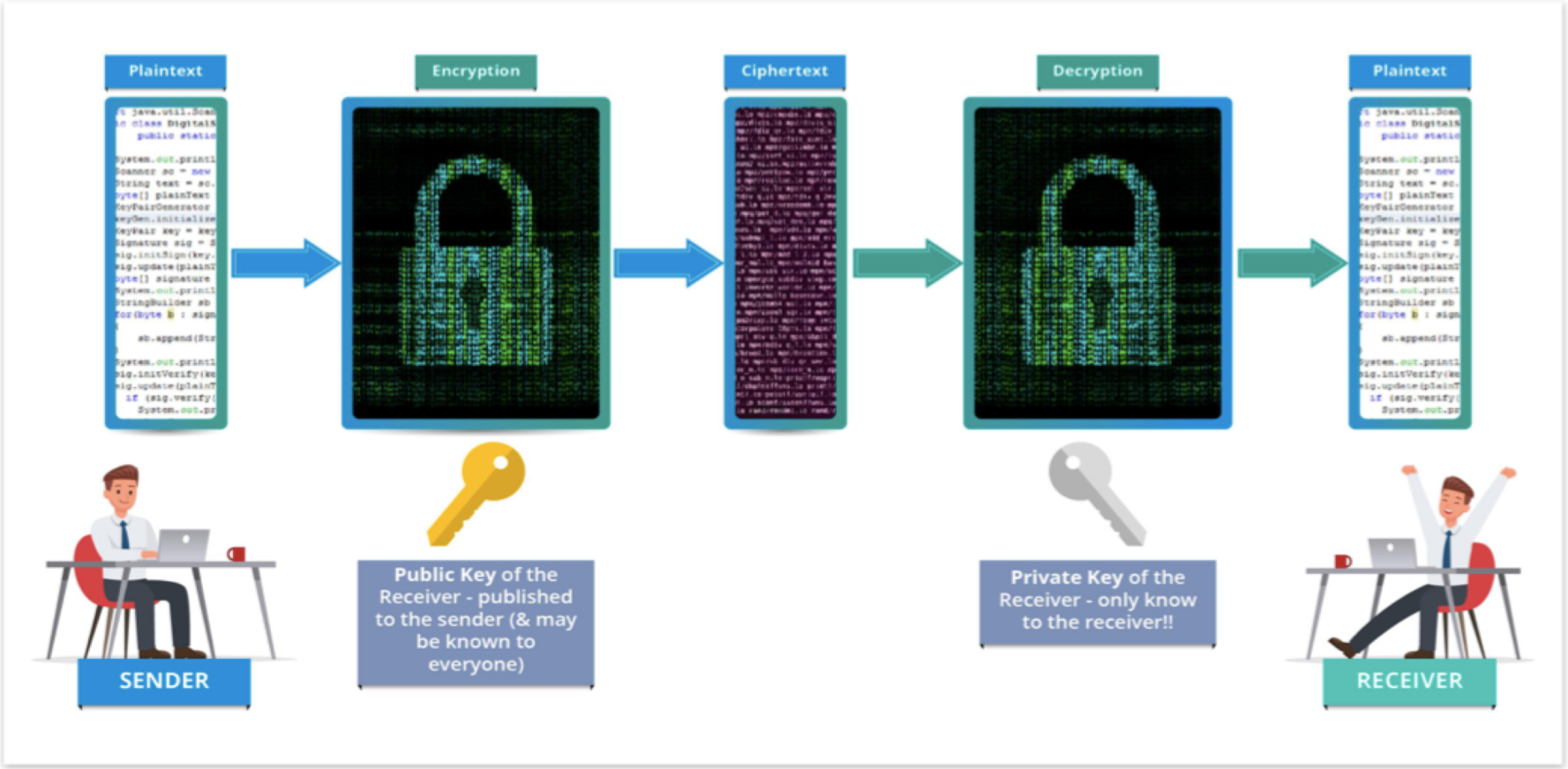
THE ENCRYPTION PROCESS WHERE DIFFERENT KEYS ARE USED FOR ENCRYPTING AND DECRYPTING THE INFORMATION IS KNOWN AS **ASYMMETRIC KEY ENCRYPTION**

KEYS ARE DIFFERENT BUT ARE MATHEMATICALLY RELATED SUCH THAT RETRIEVING THE PLAINTEXT BY DECRYPTING CIPHERTEXT IS FEASIBLE

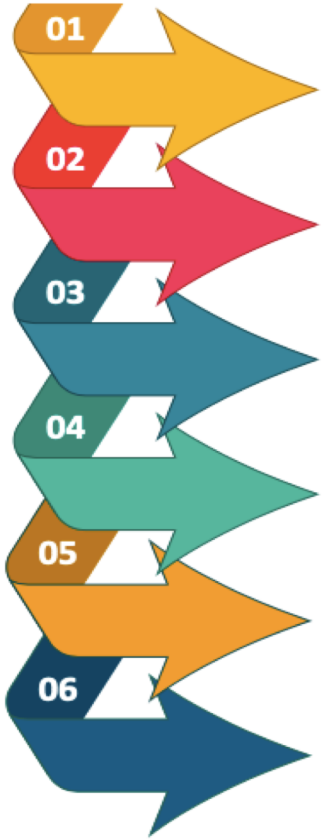
Asymmetric – Key Cryptography



Asymmetric – Key Cryptography



Features Of Public Key Cryptography



Every user in this system needs to have a pair of different keys, [private key and public key]. These keys are mathematically related – when one key is used for encryption, the other can decrypt the Cipher text back to the original plaintext

It requires to put the public key in public repository and the private key as a well-guarded secret. Hence, this scheme of encryption is also called **Public Key Encryption**

Even though the public and private keys are related, it is mathematically not possible to find one from another. This is a strength of this scheme

When a sender needs to send data to the receiver, he obtains the public key of receiver from some repository published by the receiver, encrypts the data, and transmits - Receiver then uses his private key to extract the plaintext

Length of Keys (number of bits) in this encryption is hefty and hence, the process of encryption/decryption is slower as compared to symmetric key encryption

Asymmetric algorithm needs more compute (processing) power as compared to symmetric key encryption

Challenge Of Public Key Cryptography

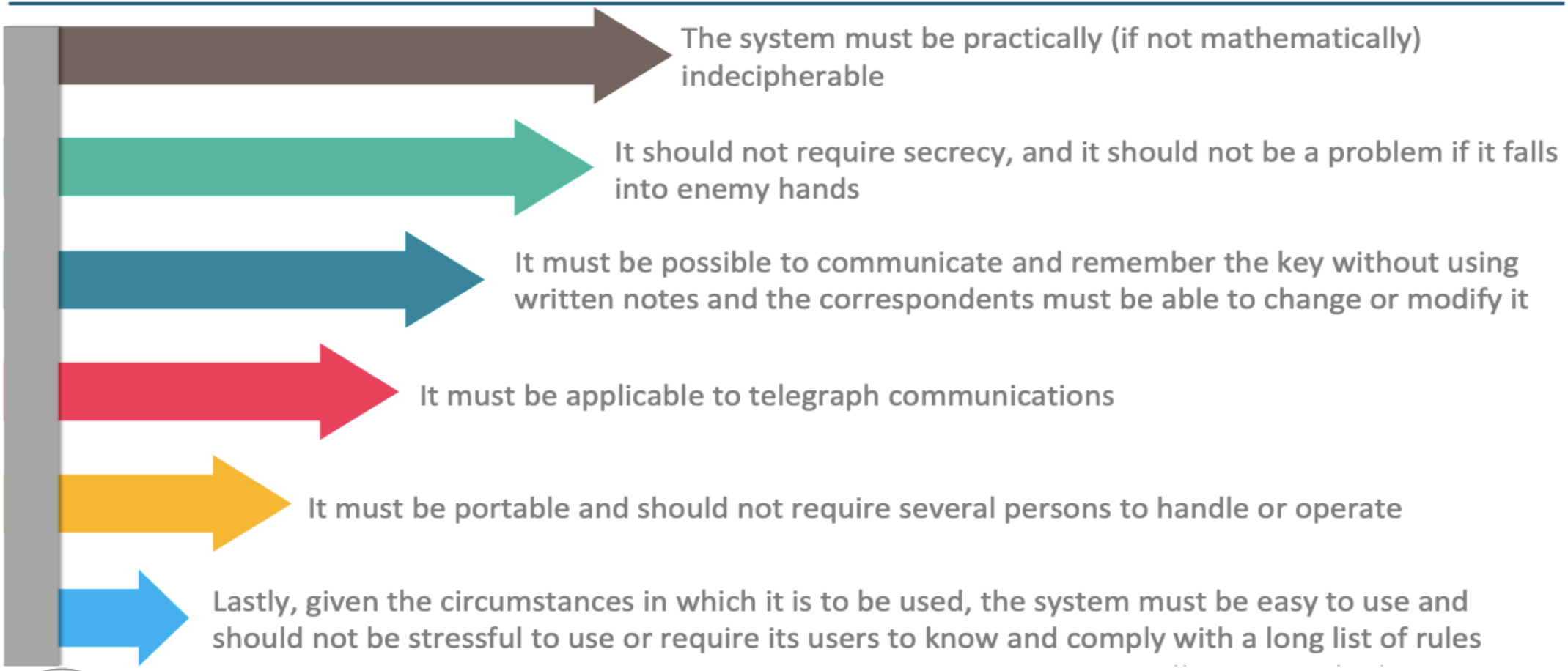
Public Key Cryptosystems have one noteworthy challenge – the user needs to trust that the **Public key** that he is using in communication with a person is an authentic (real) public key of that person and has not been tricked by a miscreant

Demo 1: Image Steganography

- Prevent unwanted people from reading your private information
- Hide a secret message behind an image file
- Use steganography tool **InvisibleSecrets4**
- Download the tool from the below link: http://www.invisiblesecrets.com/download.html

Criterion For A Good Cryptosystem

Kerckhoffs's Principles For Cryptosystem



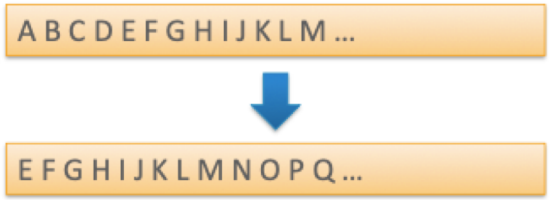
We now know the way to implement cryptography, there are different ways or algorithms to form a key

Assorted Cryptographic Algorithms

Substitution Ciphers: Caesar Cipher

Caesar Cipher is a method in which each letter in the alphabet is rotated by “n” letters :

Example for n = 4



Plaintext	hello
Rot:0	hello
Rot:1	ifmmp
Rot:2	jgnnq
Rot:3	khoor
Rot:4	lipps
Rot:5	mjqqt

Plaintext	all is well
Rot:0	all is well
Rot:1	bmm jt xfmm
Rot:2	cnn ku ygnn
Rot:3	doo lv zhoo
Rot:4	epp mw aipp
Rot:5	fqq nx bjqq

Transposition Cipher: Columnar Transposition

- This involves reorganization of characters in the plain text, into columns [***m*** x ***n*** matrix]
- The following example explains the transformation :
  - If the letters are not exact multiples of the transposition size [***m*** x ***n*** matrix] , infrequent letters such as x or z are padded at the end
  - For Ex: Consider Plaintext = “cryptography is cool”

c	r	y	p	t
o	g	r	a	p
h	y	i	s	c
o	o	l	z	z

c	o	h	o	r
g	y	o	y	r
i	l	p	a	s
z	t	p	c	z

Data Encryption Standard (DES) [Symmetric]

Goal of DES

- Fully Scramble the data and key so that every bit of cipher text depends on every bit of data and ever bit of key

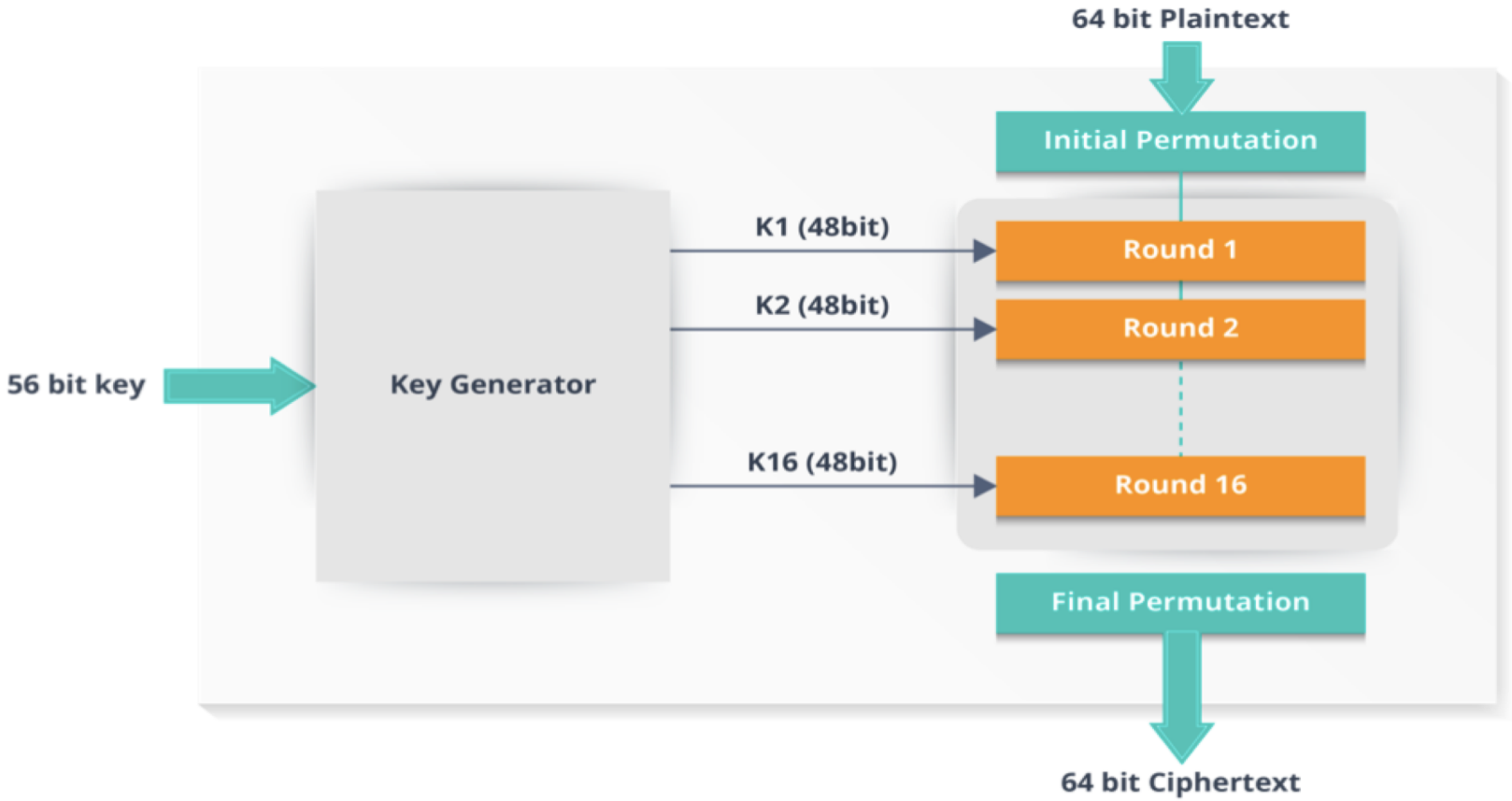
DES is a Block Cipher Algorithm

- Encodes plaintext in 64 bit chunks
- One parity bit for each of the 8 bytes thus it reduces to 56 bits

It is the most used Algorithm

- Standard approved by US National Bureau of Standards for Commercial and non-classified US government use in 1993

DES – Block Diagram



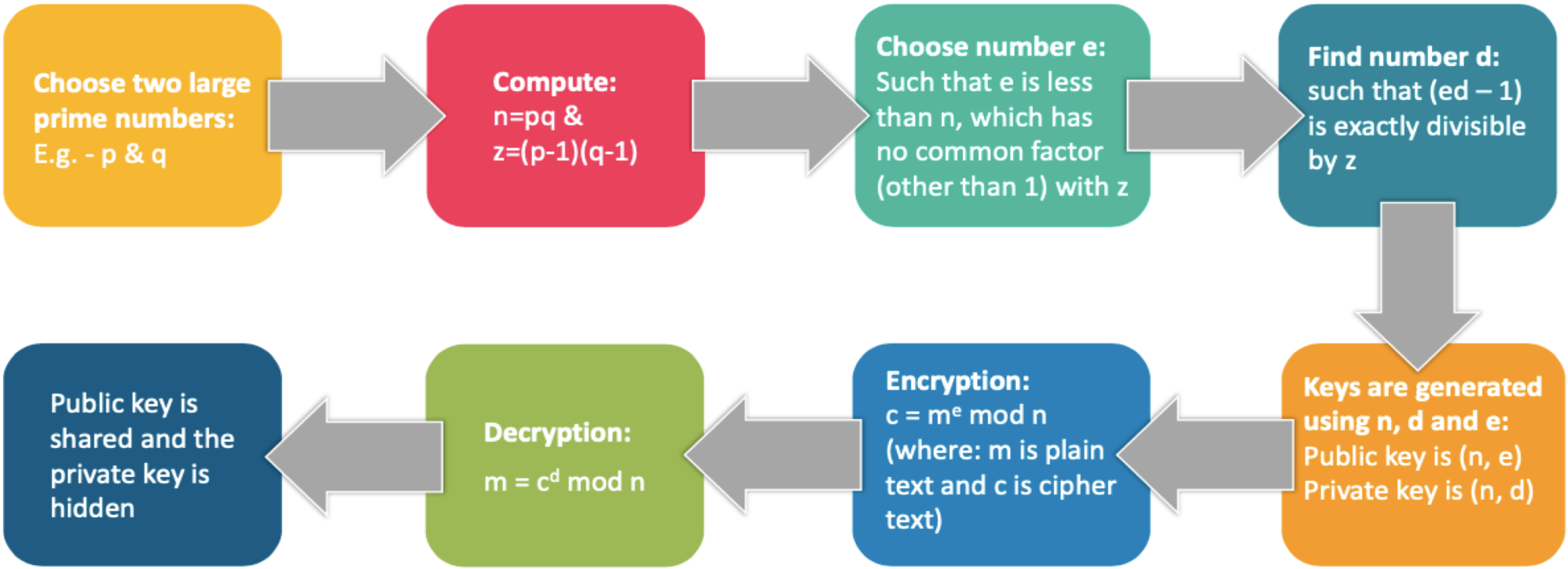
Comparison Of Symmetric Key Algorithms

Algorithm	Type	Key Size	Features
DES	Block Cipher	56 bits	Most Common, Not strong enough
TripleDES	Block Cipher	168 bits (112 effective)	Modification of DES, Adequate Security
Blowfish	Block Cipher	Variable (Up to 448 bits)	Excellent Security
AES	Block Cipher	Variable (128, 192, or 256 bits)	Replacement for DES, Excellent Security
RC4	Stream Cipher	Variable (40 or 128 bits)	Fast Stream Cipher, used in most SSL implementations

What Is RSA?

- RSA stands for Rivest, Shamir, and Adelman, inventors of this technique
- It is an Asymmetric key algorithm
- Both public and private key are inter-changeable
- Variable Key Size (512, 1024, or 2048 buts)
- Most popular public key algorithm

RSA [Asymmetric] Key Generation Process




Next is our Hash Function, that converts one numerical value into another compressed numerical value for better security

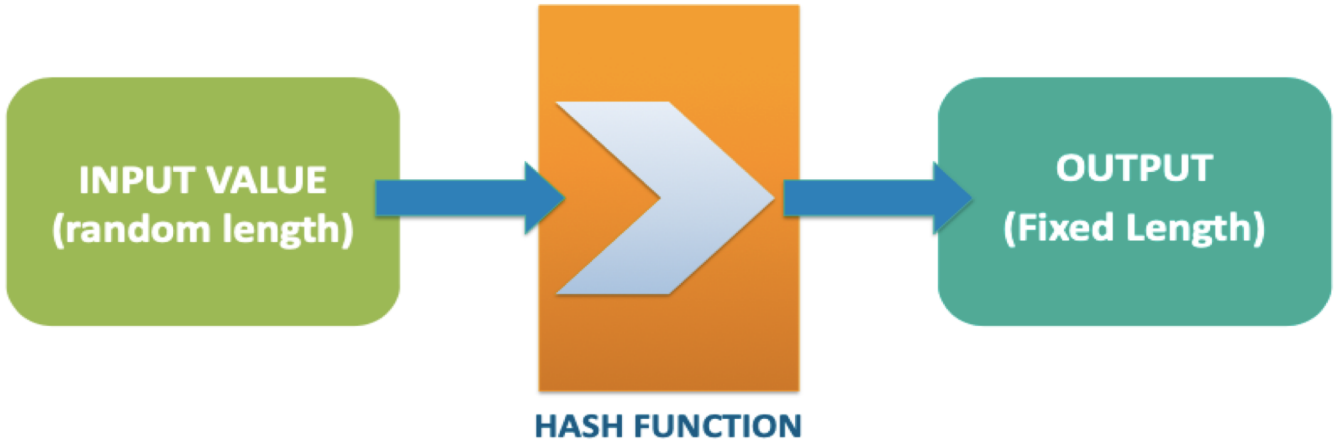
Cryptographic Hash Functions

FTVETI

ICT @ FTVETI

Hash Functions

- A mathematical function or process, that converts one numerical value into another compressed numerical value is know as a **Hash Function**, such as: **F(x) = y**
- The **input** to the hash function may be of any length but **output** is always of **fixed length**
- The **output** is expected to be **unique and consistent** for a given pair of function and Input. A slight change in the input value creates unpredictable change in output value



Properties Of Hash Functions

Second Pre-Image Resistance

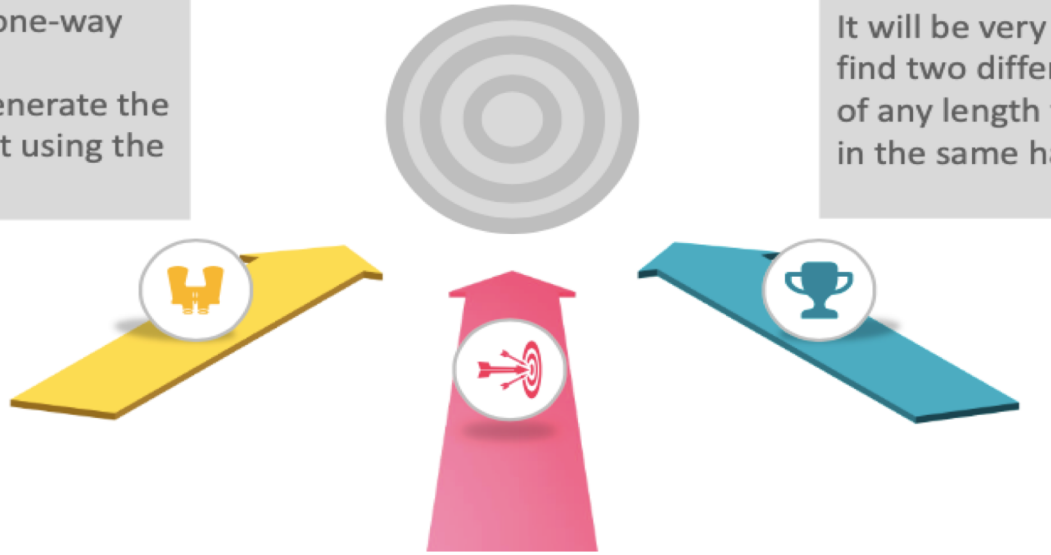
If an input and its hash value is given, it will be very difficult to find another input with the same hash

Pre-Image Resistance

- Irreversible one-way function
- No way to generate the original Input using the output hash

Collision Resistance

It will be very difficult to find two different inputs of any length that results in the same hash



Common Hash Functions

Message Digest (MD)

The MD family contains hash functions MD2, MD4, MD5 & MD6 (RFC 1321) - MD5 being the most popular

It is a 128-bit hash function

MD5 digests have been extensively used to provide assurance about integrity of a file

In 2004, collisions were reported in MD5. Collisions were said to be found within an hour's time

Due to the collision attack , MD5 is no longer recommended for use. However, the usage continues for some basic requirements

Secure Hash Function (SHA)

01 Family of SHA consists of 4 SHA algorithms; SHA-0, SHA-1, SHA-2, and SHA-3. Though from same family, they are all structurally different.

02 SHA-1 is the most widely used of the existing SHA hash functions. It is employed in several widely used applications and protocols including Secure Socket Layer (SSL) security

03 In 2005, a method was found for finding collisions for SHA-1 within pragmatic time-frame making long-term employability of SHA-1 uncertain

04 SHA-2 family has 4 more SHA variants, SHA-224, SHA-256, SHA-384, and SHA-512 subject to the number of bits in their hash value

05 No successful attacks have yet been reported on SHA-2 hash function

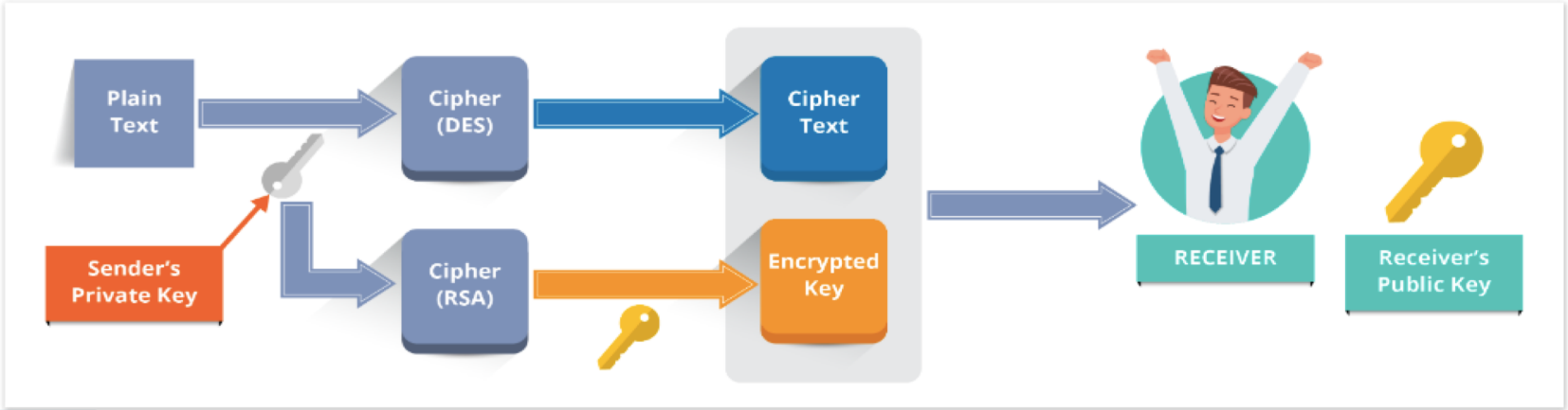
06 Though SHA-2 is a strong hash function. Though significantly different, its basic design is still follows design of SHA-1

07 In October 2012, the NIST chose the Keccak algorithm (cryptographic primitive family) as the new SHA-3 standard

08 Keccak (cryptographic primitive family) offers many benefits, such as efficient performance and good resistance for attacks

Session Key Encryption

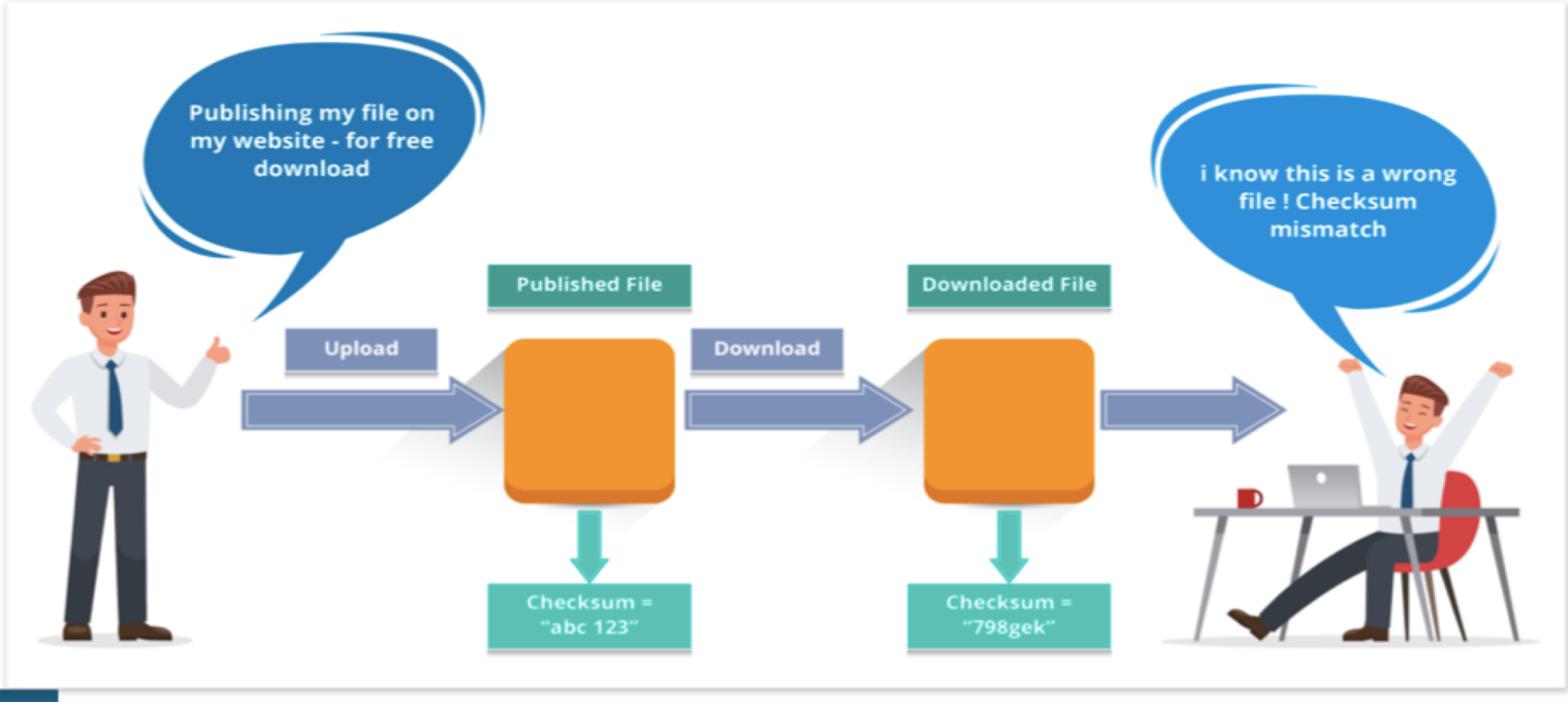
- Session-key encryption is employed to improve efficiency of communication
- “Symmetric key” is used for encrypting data – being more efficient !
- “Asymmetric key” is used just for encrypting the “symmetric key”- for the purpose of transmission ease (Public key of the receiver is used)



Application Of Hash Functions

Data Integrity Verification

- Data Integrity Verification is the most common application of the hash functions
- Accomplished by generating the checksum of the data in question
- Matching Result after recalculation of checksum gives an assurance to the user about correctness of the data



Secure Password Storage

- Hash functions provide a strong layer of defense to “plaintext” password storage
- Instead of storing password in cleartext (plaintext), mostly all logon processes primarily store the hash values of passwords in the file
- The Password file consists of a table of pairs which are in the form {user_id, Hash(pwd)}
- A successful Hacker – can just see the hashes of passwords. He can neither logon using the retrieved hash nor can derive the password from hash value since hash functions are irreversible

Demo 2: Hashing

- Calculate hash values for text, files or hex strings
- Use **HashCalc** to calculate the hash values
- Compare the hash values of text files by different hashing algorithms
- Download and install HashCalc tool from this link: https://www.slavasoft.com/hashcalc/


Let's us see how we can digitally encode a message using the Cryptographic digital signature

Cryptographic Digital Signatures

FTVETI

ICT @ FTVETI

What's It All About?

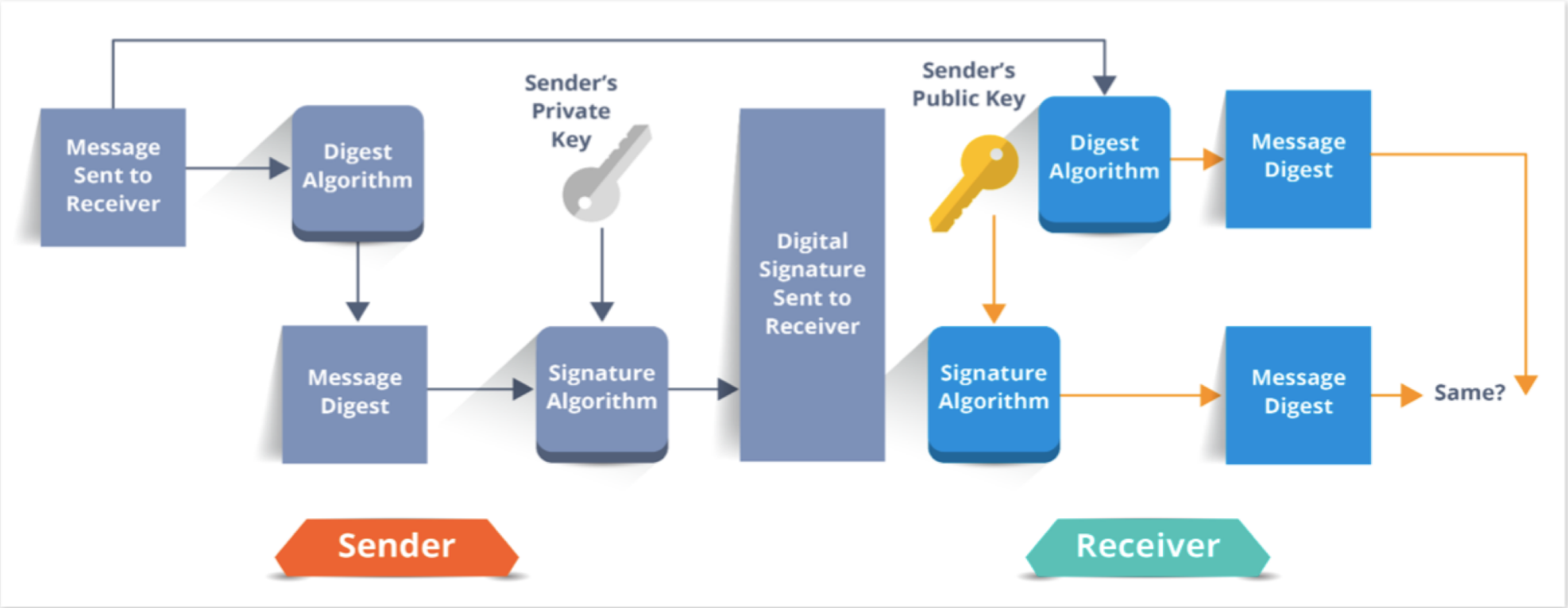
What is Digital Signature ?

A digital signature is a data-item which is linked with or is logically associated with a digitally encoded message

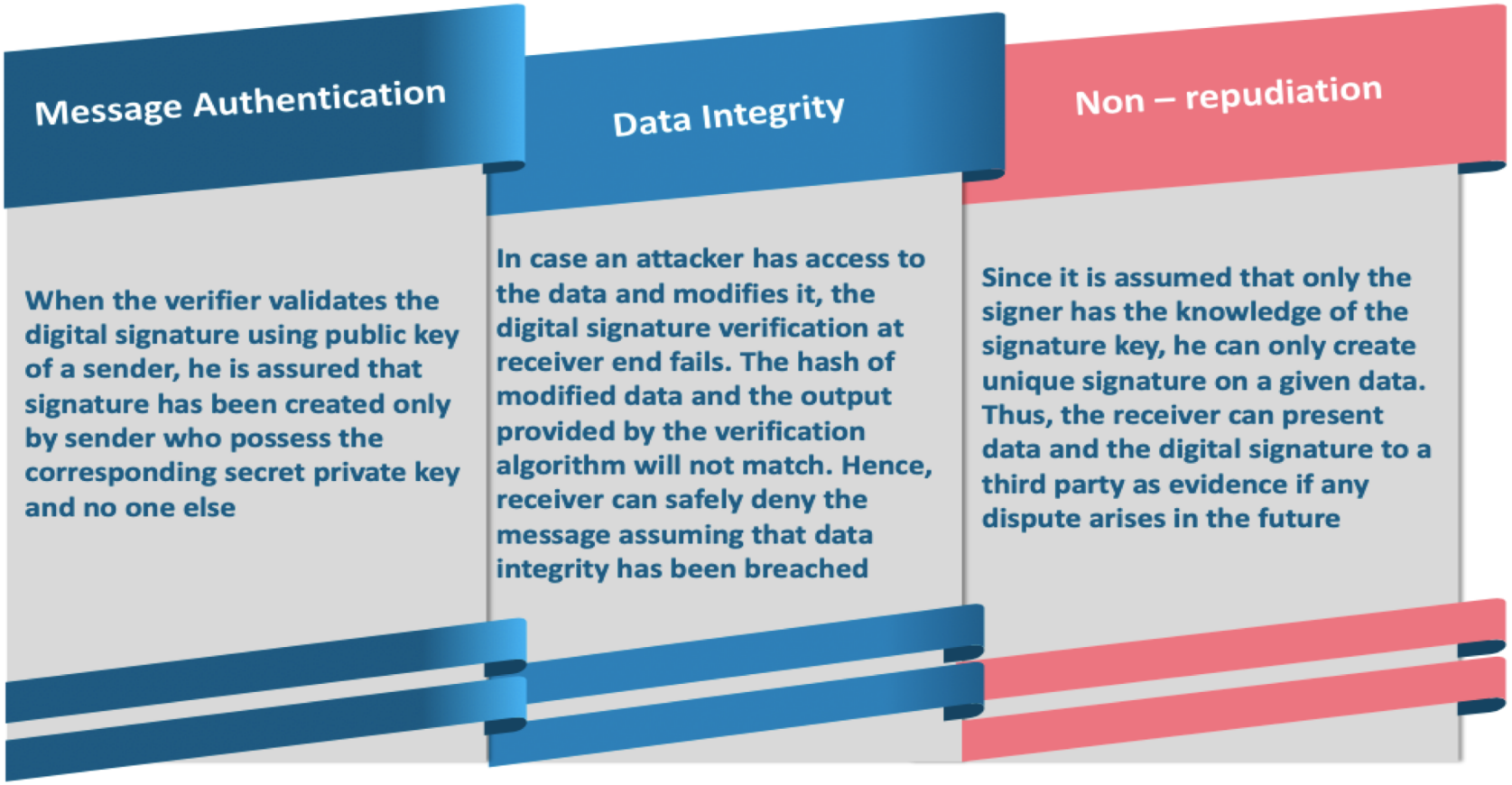
Goals of Digital Signature

- Assurance of the "source" of the data
- Proof that the data has not been tampered

Digital Signature



Features Of Digital Signatures



Digital Certificates

Digital Certificate

A digital certificate is a signed statement by a trusted party that another party's public key belongs to them

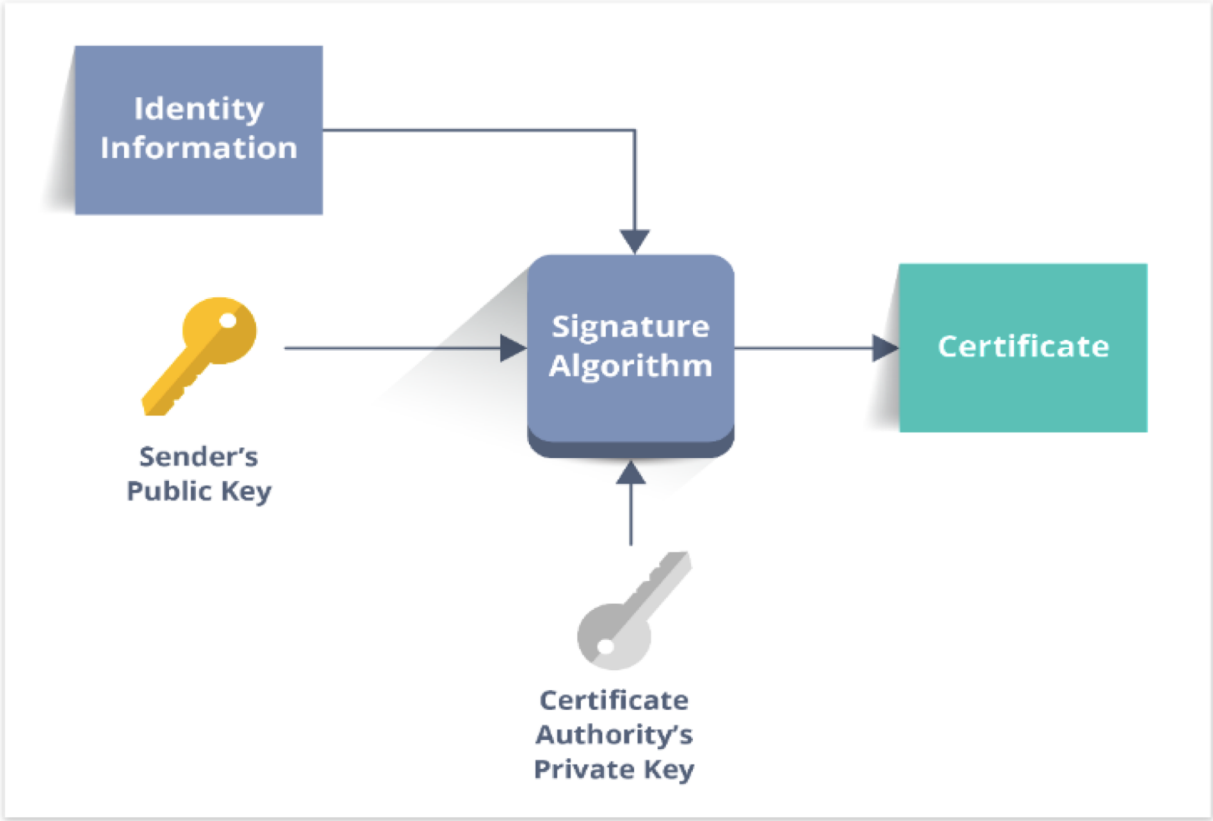
Authorization

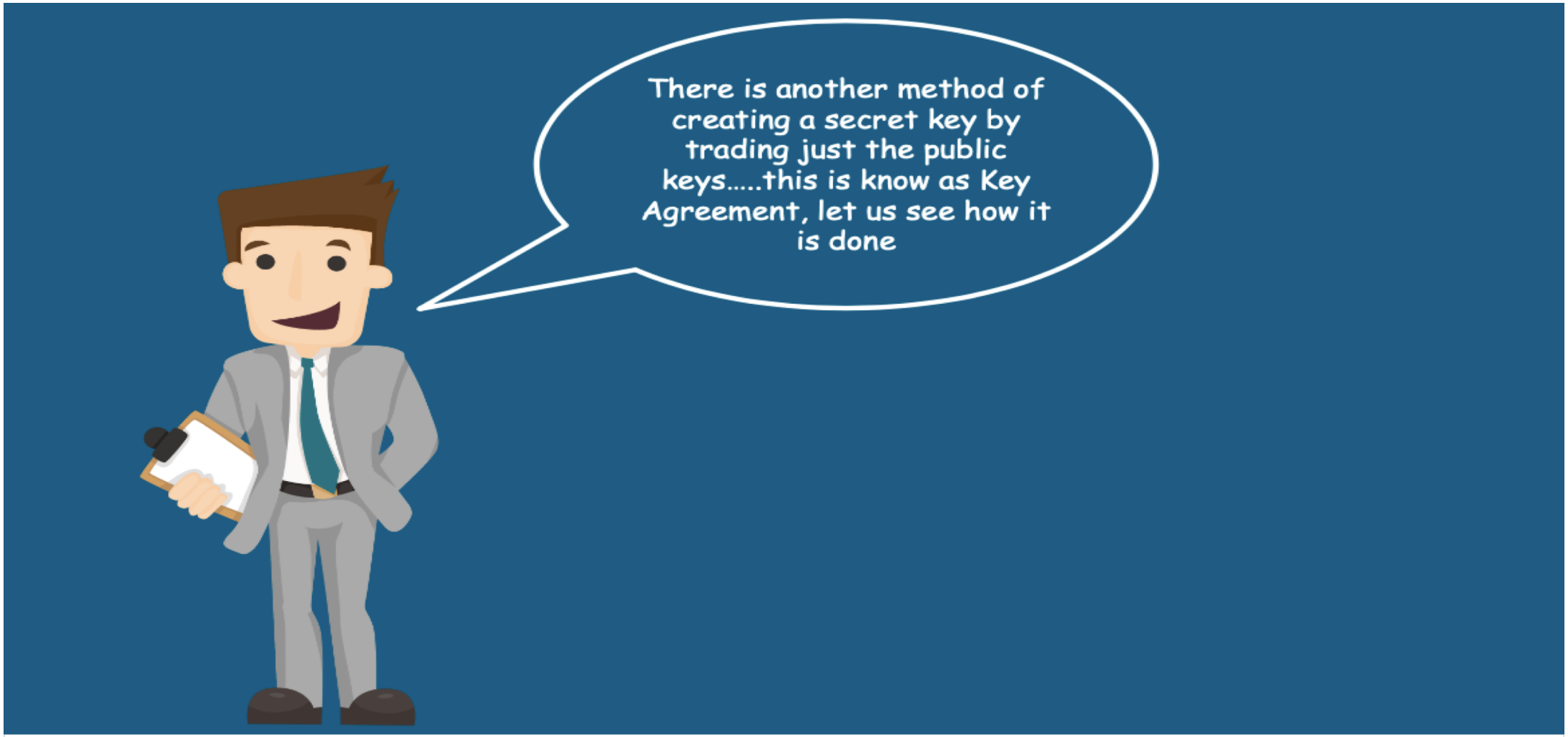
- This allows one certificate authority to be authorized by a different authority (root CA)
- Top level certificate must be self signed

CA – Certificate Authority

- Any one can start a certificate authority!
- Brand recognition is key to some one recognizing a certificate authority

Digital Certificates

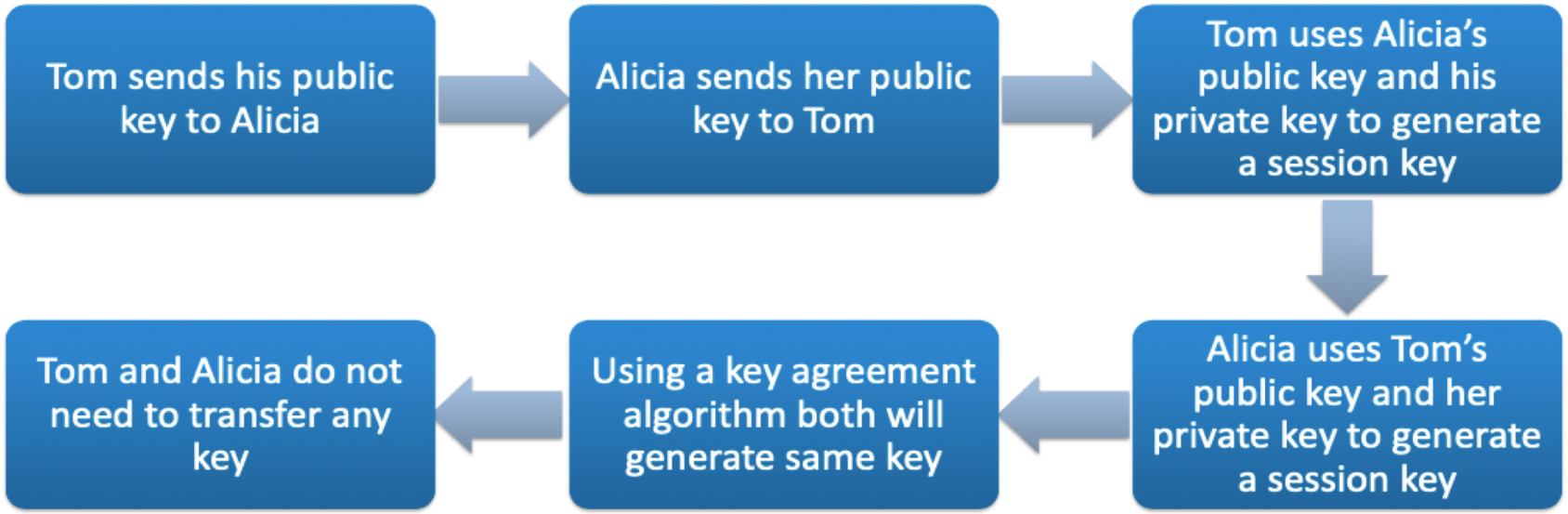



There is another method of creating a secret key by trading just the public keys.....this is know as Key Agreement, let us see how it is done

Key Agreement

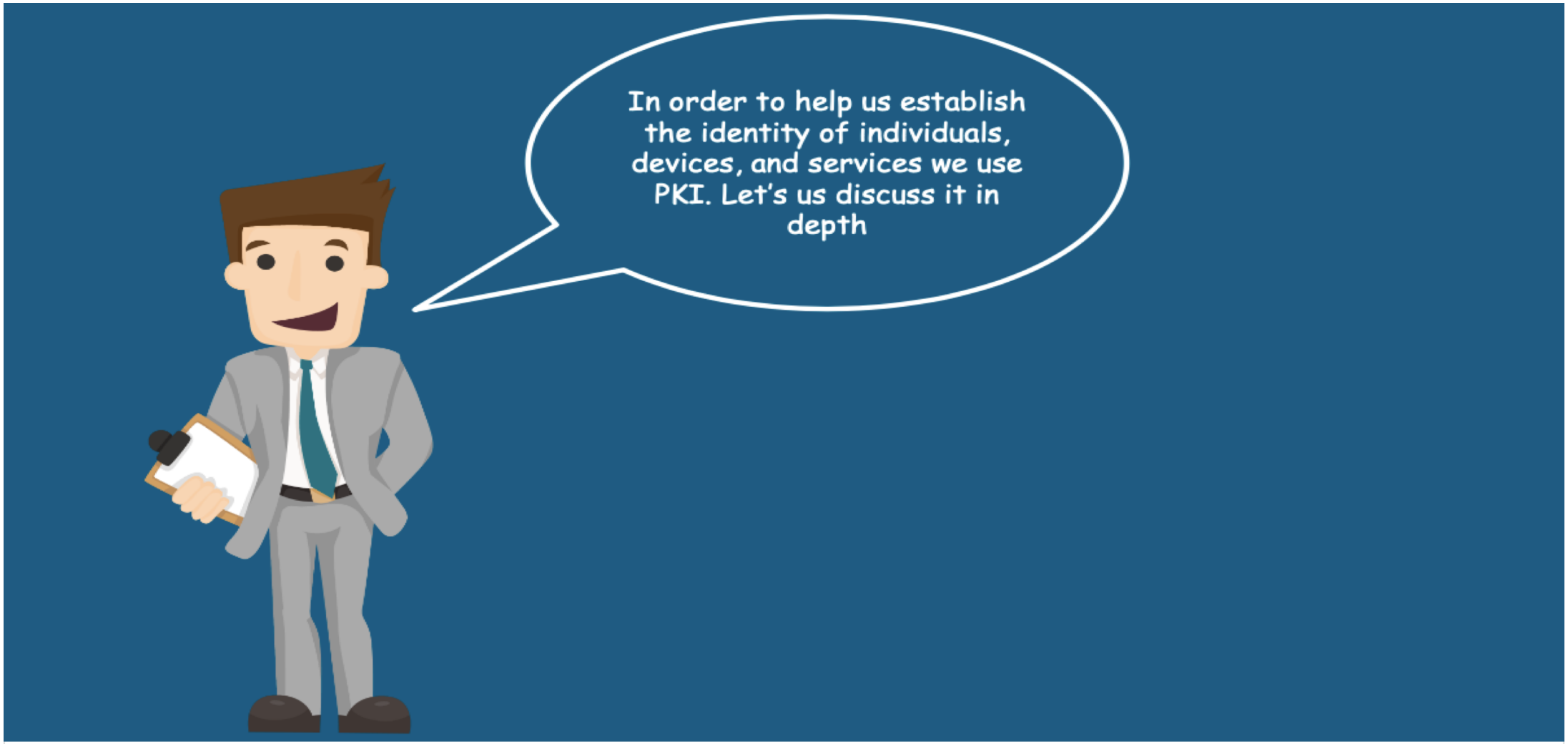
What Is Key Agreement?

Key agreement is a technique, to create a secret key by trading just the public keys



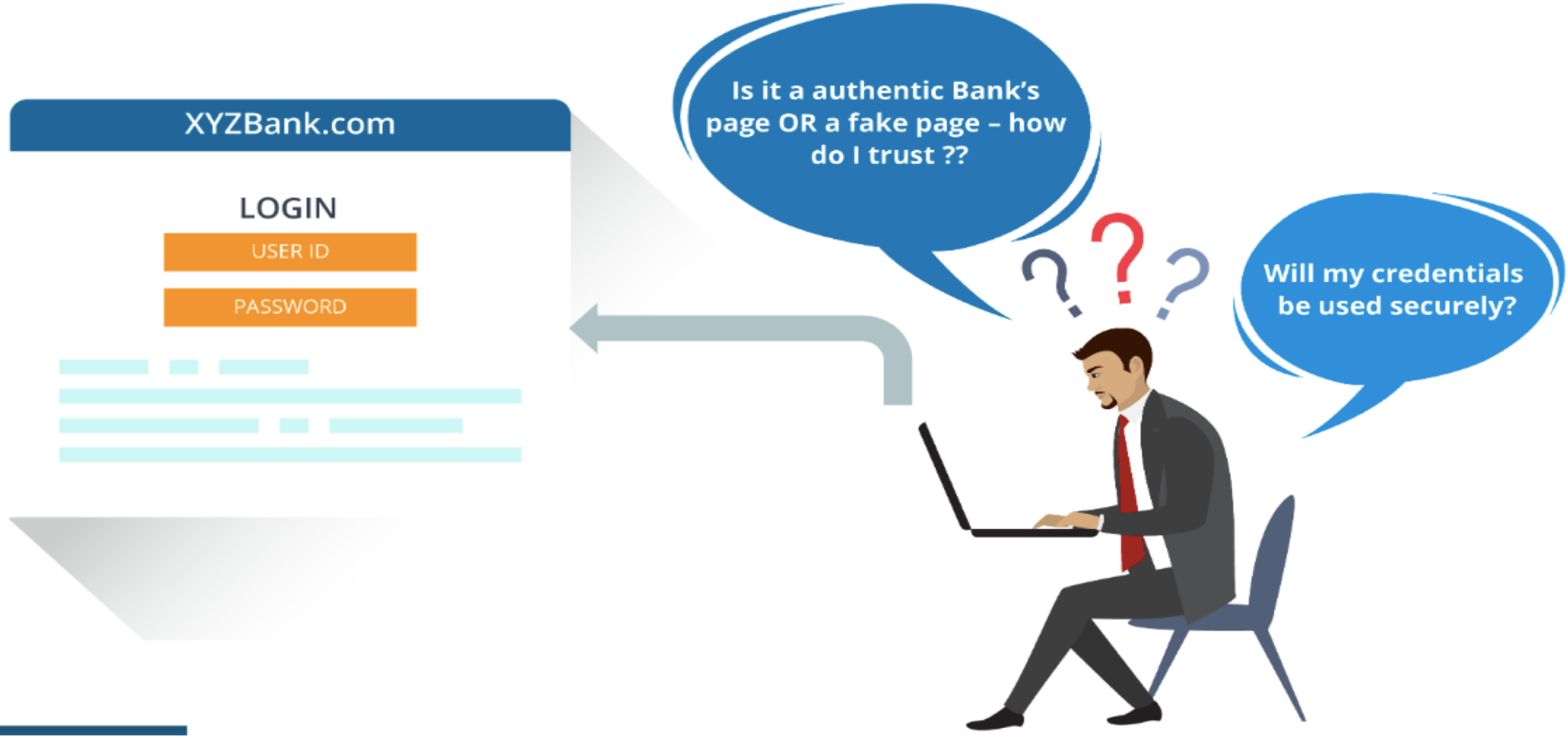
Diffie – Hellman Algorithm: Highlights

- Diffie-Hellman is the first key agreement algorithm (Invented by Whitfield Diffie & Martin Hellman)
- It helps in messages to be exchanged securely without the need of sharing some secret information previously
- Foundation of public key cryptography, which allowed keys to be exchanged in the open environment
- No need to exchange secret keys
- Man-in-the middle attack avoided


In order to help us establish the identity of individuals, devices, and services we use PKI. Let's us discuss it in depth

Public Key Infrastructure (PKI)

Need Of PKI


XYZBank.com
LOGIN
USER ID
PASSWORD
Is it a authentic Bank's page OR a fake page – how do I trust ??
Will my credentials be used securely?

Background – PKI

- Businesses are becoming increasingly dependent on digital information & electronic transactions, and consequently face rigorous data privacy compliance challenges and data security regulations. With the enterprises under constant threat of both external & internal cyber attacks, business applications and networks are now more dependent on using the digital credentials for controlling the way users and entities access sensitive / confidential data & critical system resources!
- Public key infrastructures (PKIs) are necessary to help establish the identity of individuals, devices, and services. PKIs go way beyond the use of user IDs and passwords, employing cryptographic technologies such as digital signatures and digital certificates to create unique credentials that can be reasonably validated with a scalable proportion
- PKI is a foundation of how data is encrypted as it is passed over the internet using SSL/TLS. In the absence of PKI, e-commerce wouldn't be pragmatically secure
- Asymmetric cryptography is used to provide all users in a particular group with a set of **cryptographic keys**: A public key is published & available to anyone in the group and a private key is to be kept secret and only to be used by the entity to which it belongs, usually for the tasks such as decryption or for the creation of digital signatures
- Since the public keys are in open domain, they are likely to be tampered or abused. It is, thus, necessary to institute and maintain some kind of "trusted infrastructure" to manage these keys so as to establish trust and verification of origin!

PKI Components

Digital Certificate

Private Key tokens

Certification Authority (CA)

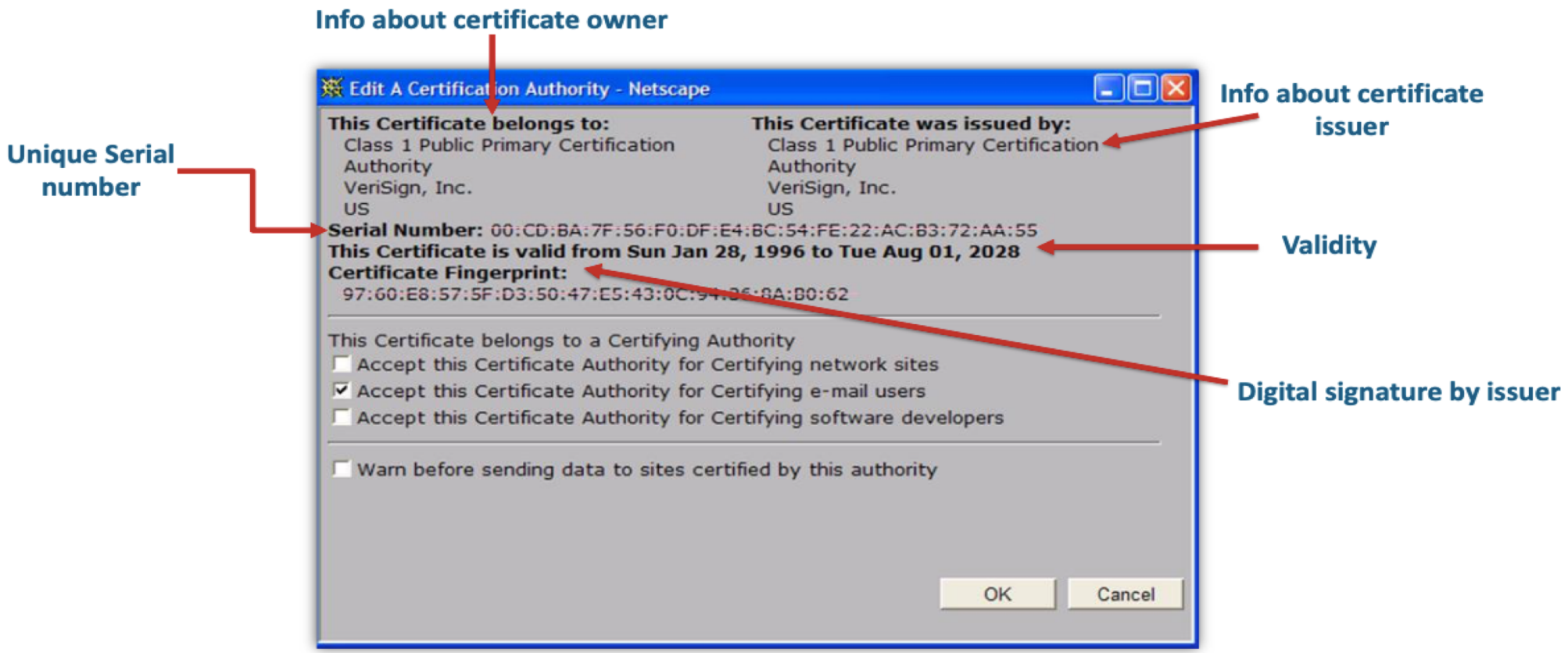
Registration Authority (RA)

Certificate Management System (CMS)

Digital Certificate (ITU Standard X.509)

- A digital certificate in virtual world is similar to an Identity-card issued to an individual in physical world
- Digital Certificates may not only be issued to individuals but also to computers, software packages or anything else that need to prove the identity in the electronic space
- ITU standard X.509 defines a standard certificate format for public key certificates and certification validation. Hence digital certificates are sometimes also referred to as X.509 certificates
- Public key pertaining to the user client, is stored in digital certificates by The Certifying Authority (CA) along with other relevant information such as client information, expiration date, usage, issuer and so on
- A Certifying Authority (CA) digitally signs this entire information and includes digital signature in the certificate
- Anyone who needs the assurance about the public key and associated information of client, carries out the signature validation process using CA's public key
- Successful validation assures that the public key given in the certificate corresponds & belongs to the entity whose details are given in the certificate

Certificate Contents



Private Key Tokens

Public key of a client is stored on the certificate, the associated secret private key can be stored on the key owner's computing device

This method is risky, because if a hacker gains an access to the owner's computing device, he can easily gain access to private key

The private key is usually stored on a 'secure removable storage', access to which is protected through a password

Certifying Authority (CA)

- CA issues certificate to a client and assist other users to verify the certificate
- The CA takes responsibility for identifying the identity of the client asking for a certificate to be issued, and ensures that the information contained within the certificate is correct and digitally signs it

Key Functions Of Certifying Authority

Issuing Digital Certificates

The CA could be thought of as the PKI equivalent of a passport agency – the CA issues a certificate after client provides the credentials to confirm his identity. The CA then signs the certificate to prevent modification of the details contained in the certificate

Generating Key Pairs

The CA may generate a key pair independently or jointly with the client

Publishing Certificates

The CA need to publish certificates so that users can find them. There are two ways of achieving this. One is to publish certificates in the equivalent of an electronic telephone directory. The other is to send your certificate out to those people who need it by one means or another

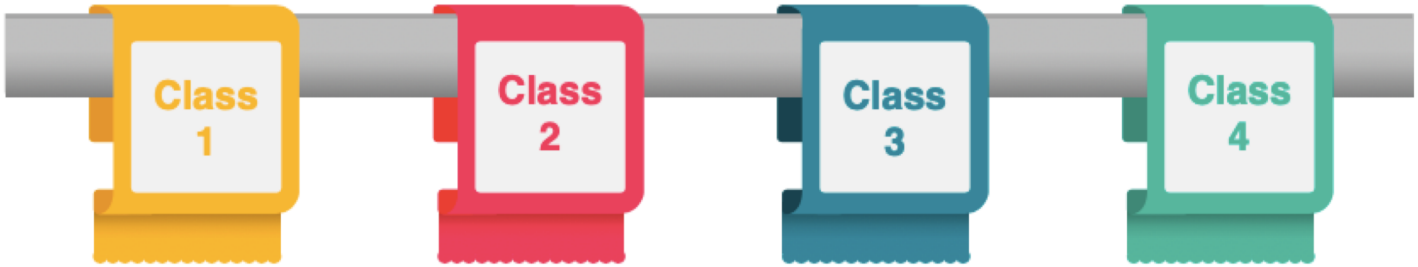
Verifying Certificates

At times, CA revokes the certificate issued due to some reason such as compromise of private key by user or loss of trust in the client. After revocation, CA maintains the list of all revoked certificate that is available to the environment

Revocation of Certificates

The CA makes its public key available in environment to assist verification of his signature on clients' digital certificate

Classes Of Certificates



Class 1

These certificates can be easily acquired by supplying an email address

Class 2

These certificates require additional personal information to be supplied

Class 3

These certificates can only be purchased after checks have been made about the requestor's identity

Class 4

They may be used by governments and financial organizations needing very high levels of trust

Registration Authority (RA)

Registration Authority is a third party used by a CA to perform the necessary verification on the entity (person or company) requesting a digital certificate to confirm their identity

The RA may work on the behalf of a CA (Certifying Authority), but RA does not actually sign the certificate that is finally issued to the certificate request

Certificate Management System (CMS)

CMS is a management system used for

- Publishing certificates
- Temporarily or permanently suspending certificates
- Renewal of certificates
- Revocation of certificates

Deletion of Certificates

- CMS do not normally delete the certificates permanently from the records, especially for legal / retention requirements

Tracking

- A CA & the allied RA uses CMS to be able to track their operations, responsibilities and liabilities

We need to understand the different Cryptographic Attacks which can destroy our system, so that we can make our data more secure

Attacks On Cryptographic Systems

Known Cryptographic Attacks

- Ciphertext-only attack
- Known plaintext attack
- Chosen plaintext attack
- Chosen ciphertext attack
- Differential cryptanalysis
- Linear cryptanalysis
- Implementation attacks
- Replay attack
- Algebraic attack
- Rainbow table
- Frequency analysis attack
- Dictionary attack
- Brute force attack
- Reverse engineering
- Attacking the random number generators
- Temporary files

Ciphertext – Only Attack

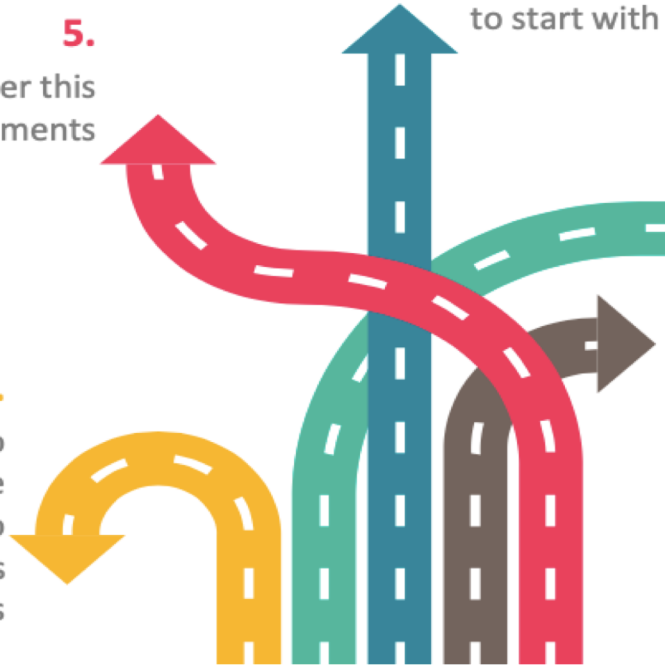
1. The ciphertext-only attack is one of the most difficult cryptography attacks as the attacker has little information to start with

2. Attacker starts with some jumbled data that he suspects may be an important encrypted message. The attack becomes easier when the attacker is able to gather several pieces of ciphertext to decipher trends by statistical analysis

3. Moore's law states that available computing power doubles every 18 months

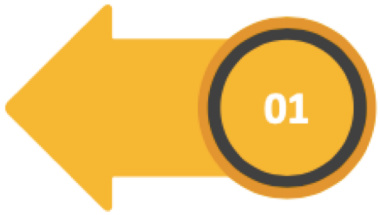
4. Encryption strength that is considered to be adequate today may probably not be sufficient a few years from now due to advances in CPU and CPU technologies and new attack techniques

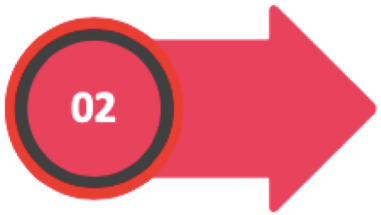
5. Security professionals should consider this when defining encryption requirements



Known Plaintext Attack

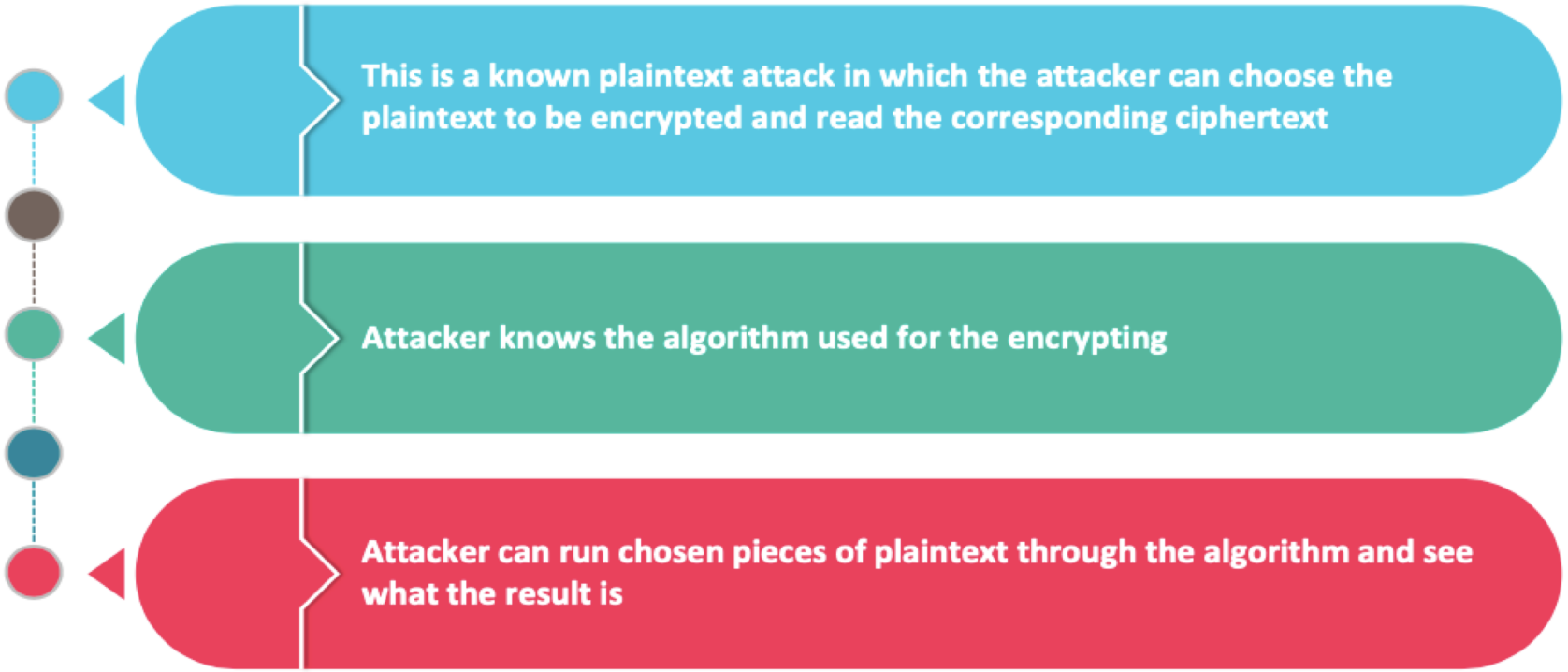
The attacker has a collection of plaintext-ciphertext pairs and is trying to find the key or to decrypt some other ciphertext that has been encrypted with the same key





Once the key has been found, the attacker would then be able to decrypt all messages that had been encrypted using that key

Chosen Plaintext Attack



Chosen Cipher – Text Attack

01 This is similar to the chosen plaintext attack, where the attacker has an access to the decryption device for decrypting chosen pieces of ciphertext to discover the key

02 The attacker has the able to select any ciphertext and study the plaintext produced by decrypting them

Computationally Secure Encryption

- An encryption scheme is said to be computationally secure if:
  - The cost of breaking the cipher exceeds the value of the encrypted information
  - The time required to break the cipher exceeds the useful lifetime of the information

Cryptanalytic Attacks

Differential Cryptanalysis

- Also called a side-channel attack
- More complex attack
- Aim is to determine the value of the key and the algorithm used, by measuring the exact execution times and power required by the crypto device to perform encryption/decryption

Linear Cryptanalysis

- Linear cryptanalysis is a known plaintext attack and uses a linear approximation to describe the behaviour of the block cipher
- Needs sufficient pairs of plaintext and corresponding ciphertext,
- Aim is to one can obtain bits of information about the key
- More sample data more accuracy

Implementation Attacks

Replay attack

- Meant to disrupt processing by resending repeated files to the host. In absence of controls such as time-stamping, use of one-time tokens or sequence verification codes in the receiving service, the system might process duplicate files

Algebraic attack

- Rely for their success on block ciphers exhibiting a high degree of mathematical structure

Rainbow table

- This attack involves creating a repository of hashing known possible plaintexts and then using a reverse lookup. Such tables are called rainbow tables

Frequency analysis attack

- It is especially useful when attacking a substitution cipher where the statistics of the plaintext language (repeating chars) are known

Implementation Attacks

Birthday attack

- This is based on "Birthday Paradox" (If there are 23 people in a room, the probability that two of them have the same birthday is approximately 0.5)
- The point of the birthday attack is that it is easier to find two messages that hash to the same message digest than to match a specific message and its specific message digest

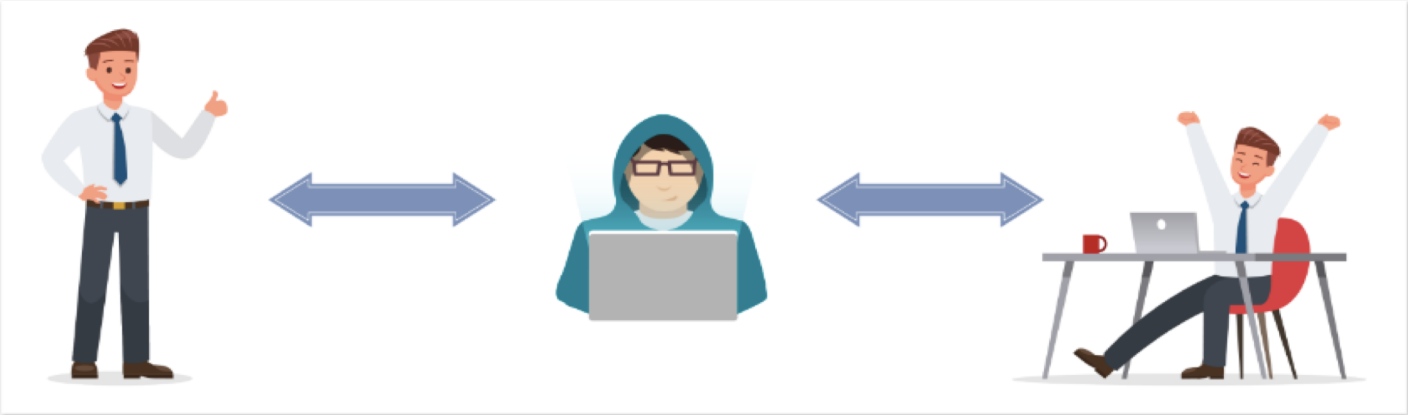
Brute force attack

- Brute force is trying all possible keys until one is found that decrypts the ciphertext
- Length is thus an important factor in determining the strength of a cryptosystem, as effort to brute force increases with length of a plaintext

Dictionary attack

- The dictionary attack is used most commonly against password files
- It exploits the poor habits of users who choose simple passwords based on natural words
- The dictionary attack merely encrypts all of the words in a dictionary and then checks whether the resulting hash matches an encrypted password stored in the SAM file or other password file

MITM: Man In The Middle Attack



Attacker generates a key pair, and distributes his public key in the name of somebody else

Other party believes it and uses this public key for encryption, resulting in the attacker being able to read the messages

(as he can decrypt it using his private key)

The attacker encrypts the messages again with the public key of the real recipient and passes on either the real or tampered message and continues. This way he goes undetected & keeps either spying OR tampering a supposedly secure communication

Quiz #1

- Tom wants to send a confidential email to Jerry. He decides to encrypt the email. Tom wants to ensure that Jerry can verify the sender as Tom. Which of the following does Jerry need to meet this requirement?
  a. Tom's public key
  b. Tom's private key
  c. Jerry's public key
  d. Jerry's private key

Answer #1

- Tom wants to send a confidential email to Jerry. He decides to encrypt the email. Tom wants to ensure that Jerry can verify the sender as Tom. Which of the following does Jerry need to meet this requirement?
  a. **Tom's public key**
  b. Tom's private key
  c. Jerry's public key
  d. Jerry's private key

Answer a:
Explanation: If the message gets decrypted by the public key of a said sender, it ensures that the message was sent by the said sender as it was encrypted by the sender's private key

Quiz #2

- An organization is looking for a secure method for sharing encryption keys over a public network. What could be the logically best option?
  a. Scrypt
  b. Diffie-Hellman
  c. Steganography
  d. Symmetric Cryptography

Answer #2

- An organization is looking for a secure method for sharing encryption keys over a public network. What could be the logically best option?
  a. Scrypt
  b. Diffie-Hellman
  c. Steganography
  d. Symmetric Cryptography

Answer b:
Explanation: Diffie-Hellman is a favoured algorithm often used for distributing a shared secret between two communicating parties. It is typically a method of choice for exchanging cryptographic keys while the usage of symmetric key algorithms

Quiz #3

- Jack wants to send a secure email to Jill thus he decides to encrypt it. Jack wants to ensure that only Jill can decrypt it. Which of the following does Jill need to decrypt it?
  a. Jack's private key
  b. Jack's public key
  c. Jill's private key
  d. Jill's public key

Answer #3

- Jack wants to send a secure email to Jill thus he decides to encrypt it. Jack wants to ensure that only Jill can decrypt it. Which of the following does Jill need to decrypt it?
  a. Jack's private key
  b. Jack's public key
  c. **Jill's private key**
  d. Jill's public key

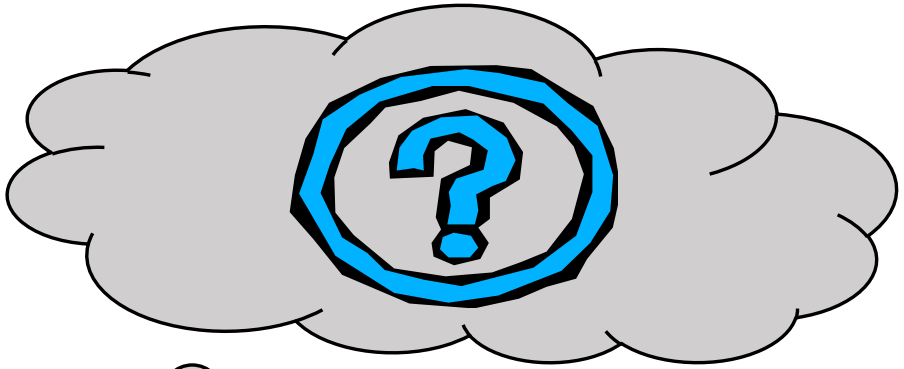
Answer c:
Explanation: In this scenario, sender would encrypt the message using the Receiver's Public key and thus only the intended receiver can then decrypt that message using his/her private key

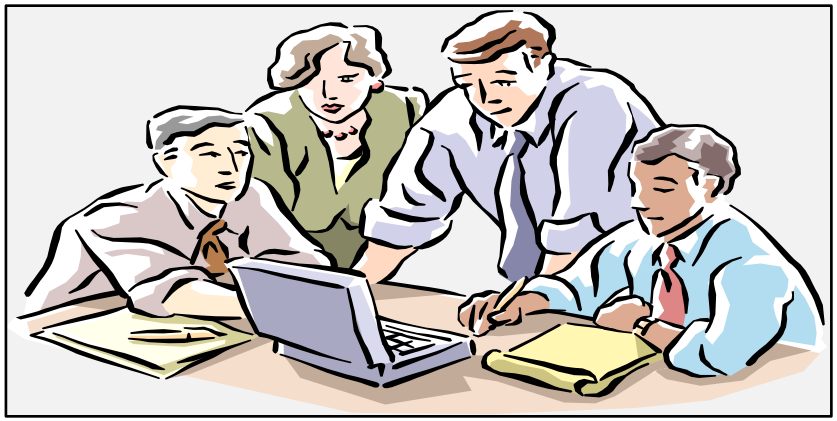
Summary

In this unit, you should have learnt:

- Cryptography and Crypto System
- Cryptographic Algorithms
- Hash Functions in Cryptography
- Cryptographic Digital Signature
- Key Agreement & Public Key Infrastructure
- Various attacks against Encrypted Data

QUESTIONS PLEASE ☺





FTVETI

ICT @ FTVETI