GOVERNMENT POLYTECHNIC COLLEGE,NANDED.
INFORMATION TECHNOLOGY ,DEPARTMENT

MINDLER

APRIL 2020

VISION AND MISSION

VISION

- "Become premier center in Information Technology with value based education that will prepare students for ever changing technological challenges of 21st century"

MISSION

- To train the students in the latest technologies Provide an environment that inculcates ethics and effective soft-skills Develop the skill sets among students that will benefit employer and society

PROGRAM OUTCOMES (POS)

* **Basic and Discipline specific knowledge** : Apply knowledge of basic mathematics, science and engineering fundamentals and engineering specialization to solve the engineering problems

- **Problem analysis** : Identify and analyses well defined engineering problems using codified standard methods
- **Design/ development of solutions** : Design solutions for well-defined technical problems and assist with the design of systems components or processes to meet specified needs
- **Engineering Tools, Experimentation and Testing** : Apply modern engineering tools and appropriate technique to conduct standard tests and measurement
- **Engineering practices for society, sustainability and environment** : Apply appropriate technology in context of society, sustainability, environment and ethical practices.
- **Project Management** : Use engineering management principles individually, as a team member or a leader to manage projects and effectively communicate about well defined engineering activities
- **Life-long learning** : Ability to analyses individual needs and engage in updating in the context of technological changes

PROGRAM EDUCATIONAL OBJECTIVE (PEOS) PROGRAM SPECIFIC OUTCOMES (PSOS)

(PEOs)

- Become competent Information Technology engineer to work as a programmer or an administrator in a team or as an individual.
- Pursue higher studies in relevant field of engineering with a desire for lifelong learning.
- Become a successful professional with ethical and societal responsibilities.

(PSOs)

- Information Technology: Use latest technologies for operation and application of information.
- Information Technology Process: Maintain the information processes using modern information and communication technology

CONTENT:-

- Introduction
- What is Cryptography
- Encryption
- Decryption
- Architecture of cryptography

- Types of Cryptography
- Process of Cryptography
- Features of Cryptography
- Benefits and Drawbacks
- Conclusion
- References

INTRODUCTION :-

- *Cryptography, art and science of preparing coded or protected communications intended to be intelligible only to the person possessing a key.*

- *Cryptography (Greek kryptos, "secret" ; graphos, "writing") refers both to the process or skill of communicating in or deciphering secret writings (codes, or ciphers).*

- *Cryptographers call an original communication the clear text or plaintext.*

- *Once the original communication has been scrambled or enciphered, the result is known as the cipher text or cryptogram.*

WHAT IS CRYPTOGRAPHY :-

- Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure net-works (like the Internet) so that it cannot be read by anyone except the intended recipient.

- Cryptography is the practice and study of hiding information. It is the Art or Science of converting a plain intelligible data into an unintelligible data and again retransforming that message into its original form.

- It provides Confidentiality, Integrity, and Accuracy.

ENCRYPTION:-

- In cryptography, **encryption** is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot.

- In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm-a cipher-generating ciphertext that can be read only if decrypted.

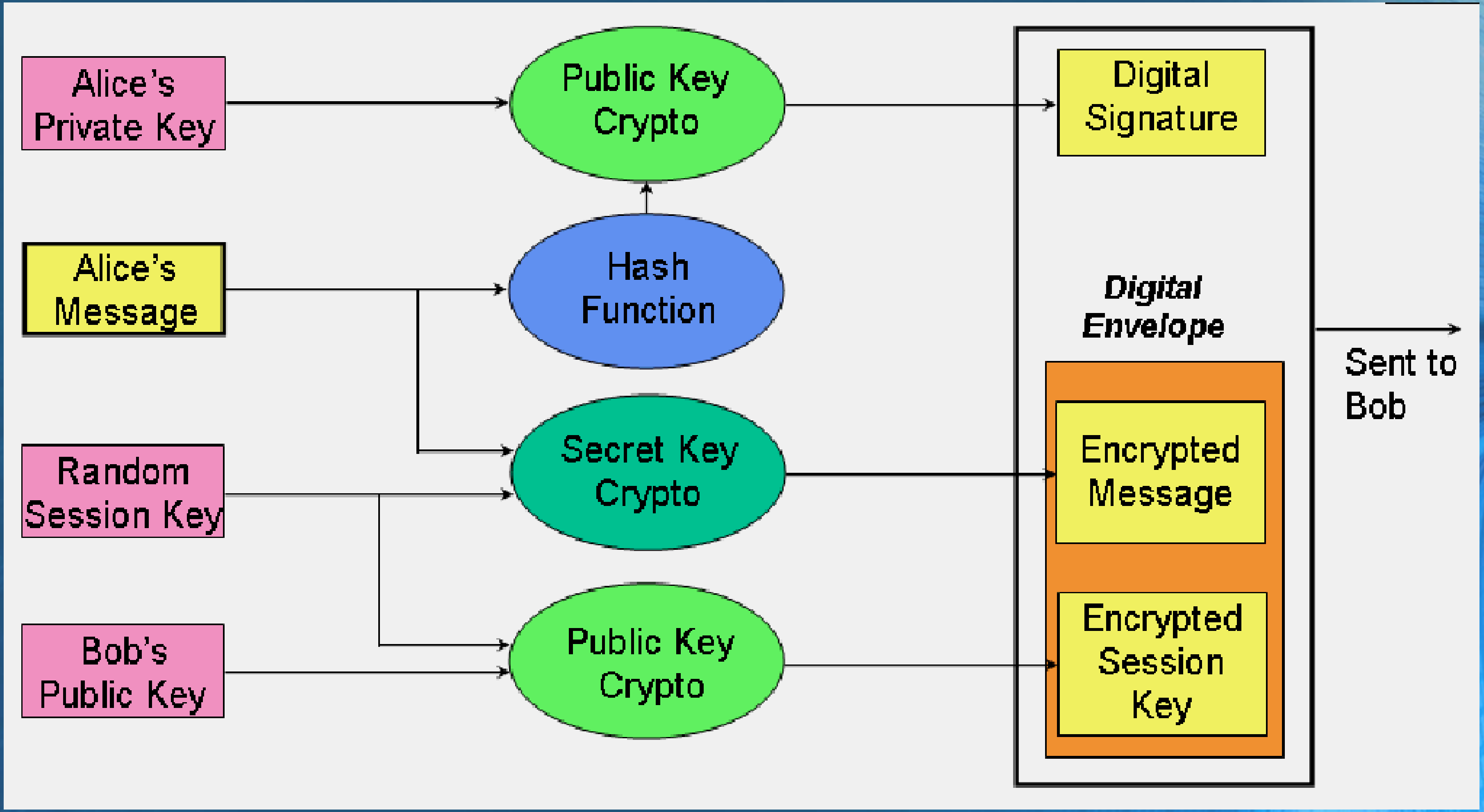
DECRYPTION :-

- The conversion of encrypted data into its original form is called Decryption.

- It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.

- Decryption can be done manually or automatically. It may also be performed with a set of keys or passwords.

ARCHITECTURE OF CRYPTOGRAPHY :-



TYPES OF CRYPTOGRAPHY :-

- **Symmetric Key Cryptography:-**

  It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages.

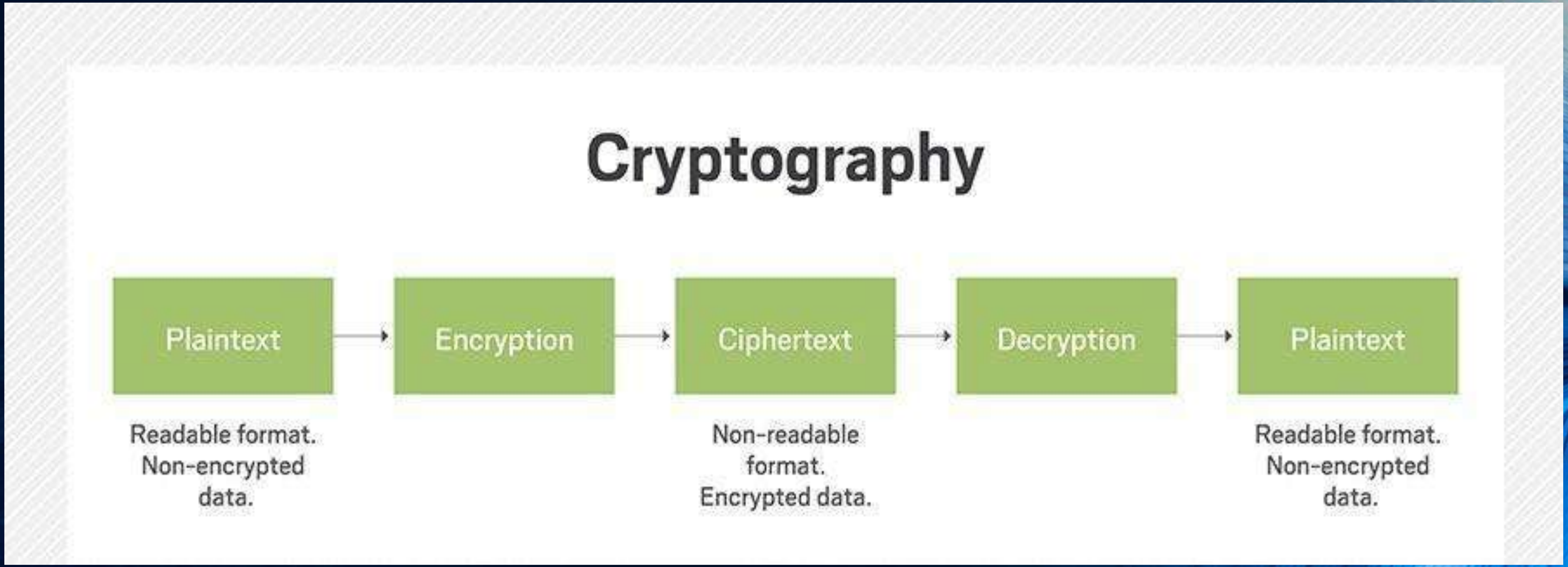
- **Hash Functions:-**

  There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered.

- **Asymmetric Key Cryptography:-**

  Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption.

Process of Cryptography :-


Cryptography
Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Readable format. Non-encrypted data.
Non-readable format. Encrypted data.
Readable format. Non-encrypted data.

FEATURES OF CRYPTOGRAPHY :-

- ***Confidentiality:-***

Information can only be accessed by the person for whom it is intended and no other person except him can access it.

- ***Integrity:-***

Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

- ***Non repudiation :-***

The creator/sender of information cannot deny his or her intention to send information at later stage.

- ***Authentication :-***

The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

BENEFITS OF THE CRYPTOGRAPHY :-

- *It hides the messages and keeps your privacy safe.*
- *It is simple to implement .*
- *We can send cipher text through e-mail or FAX.*
- *Less resources needed to maintain it.*
- *No one would be able to know what it says unless there is a key to the code.*
- *You are able to use Cryptography during lessons without theTeachers knowing.*

DRAWBACKS :-

- *Takes a long time to Figure out the code.*

- *It takes long to create the c ode .*

- *If you were to send the code to another person in the past ,it will take long time to get to that person.*

- *Cryptography comes at cost. The cost is in terms of time and money :-*

- *Addition of cryptographic techniques in the information processing leads to delay.*

- *The use of public key cryptography requires setting up and maintenance of public key infrastructure requiring the handsome financial budget.*

CONCLUSION :-

- As the internetand the other form of electronic communication become more prevalent, electronic security is becoming increasingly imortant.

- Cryptography is used to protect e-mail messages ,credit cards information's and corporate data.

- one of the most popular cryptography system used on internet is preety good Privacy because its very effective and free.

- we use the different types of algorithms to establish security services in different service mechanism.

- IEC 62351 is one of the recommended standards developed by WG15 of IEC TC57

REFRENCES :-

- eSTREAM - The ECRYPT Stream Cipher Project.
- Wikipedia .
- Geeks for Geek.

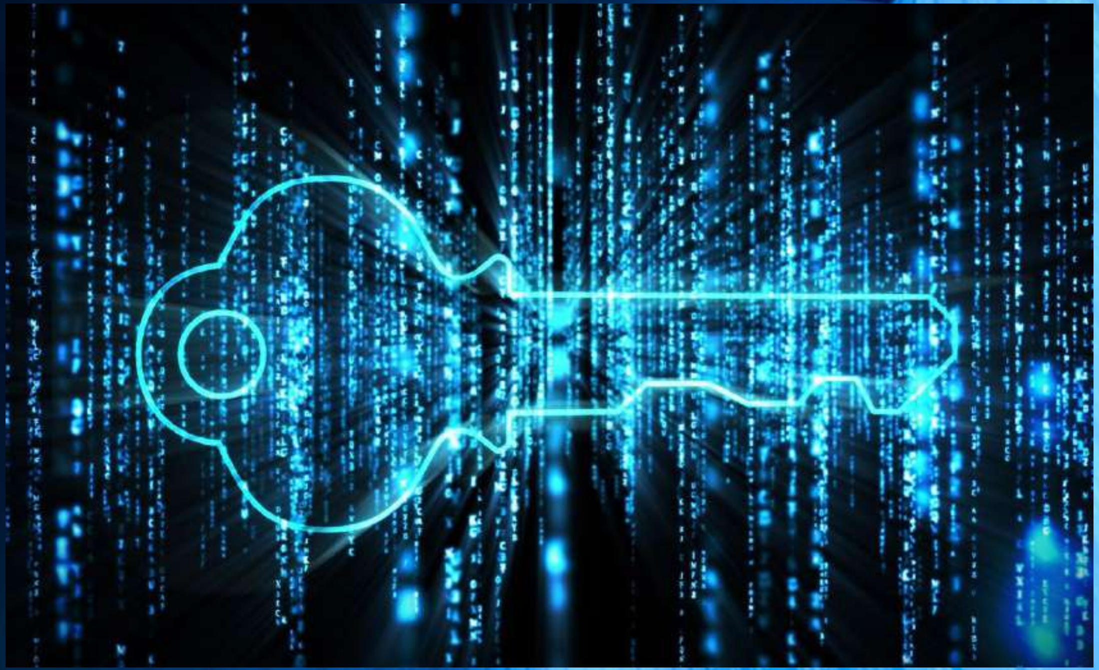
Topic Name:- Cryptography

Principal: Dr .G .V . Garje

Head Of the Department : S . N . Dhole

Mentors : A . G . Rampure , B . K . Bokare , S . G . Mundhe

Roll No : 920



Presented by :- ADITI CHINTAWAR

Class :- Polytechnic IT II Year