SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NAAC-UGC with 'A' Grade

Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai
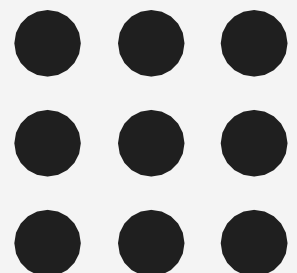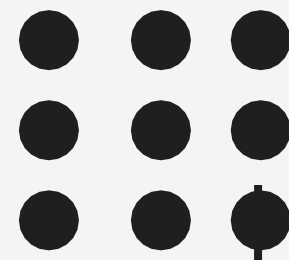
DEPARTMENT OF INFORMATION TECHNOLOGY

Course Code and Name : 19IT602– CRYPTOGRAPHY AND CYBER SECURITY

III YEAR / VI SEMESTER

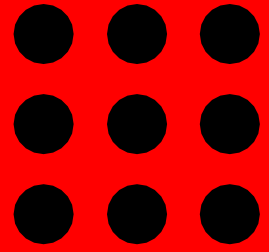**Unit 1:** INTRODUCTION TO NETWORK AND CYBER SECURITY

Topic : Security Policies

Introduction / 19IT602 - Cryptography and Cyber Security / S.Priyanka / IT / SNSCE

How to develop a Policy

- Identify sensitive information and critical systems

- Incorporate local, state, and federal laws, as well as relevant ethical standards

- Define institutional security goals and objectives

- Set a course for accomplishing those goals and objectives

- Ensure that necessary mechanisms for accomplishing the goals and objectives are in place
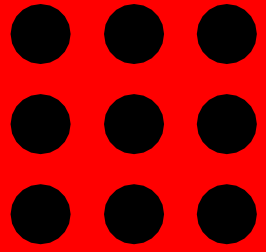
What does a Security Policy include?

- What is the reason for the policy?

- Who developed the policy?

- Who approved the policy?

- Whose authority sustains the policy?

- Which laws or regulations, if any, are the policy based on?

- Who will enforce the policy?

- How will the policy be enforced?

- Whom does the policy affect?

What does a Security Policy include?

- Be **concise**--focus on expectations and consequences, but explain the underlying rationale when appropriate

- **Don't temper** the message--truth is, you're not asking but telling, so don't propose, suggest, or insinuate unless that is specifically what you mean to do

- Use **simple, straightforward language** as is possible

- **Define** any **term** that could potentially **confuse** a reader--no need to make things more difficult than need be

- Be **creative--presentation** should never interfere with content, but checklists and reference cards increase utility

Four basic tasks in designing a particular security service

- Design a suitable algorithm for the security transformation

- Generate the secret information (keys) used by the algorithm

- Develop methods to distribute and share the secret information

- Specify a protocol enabling the principals to use the transformation and secret information for a security service
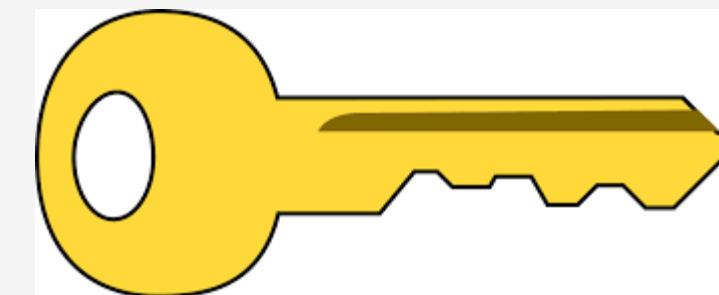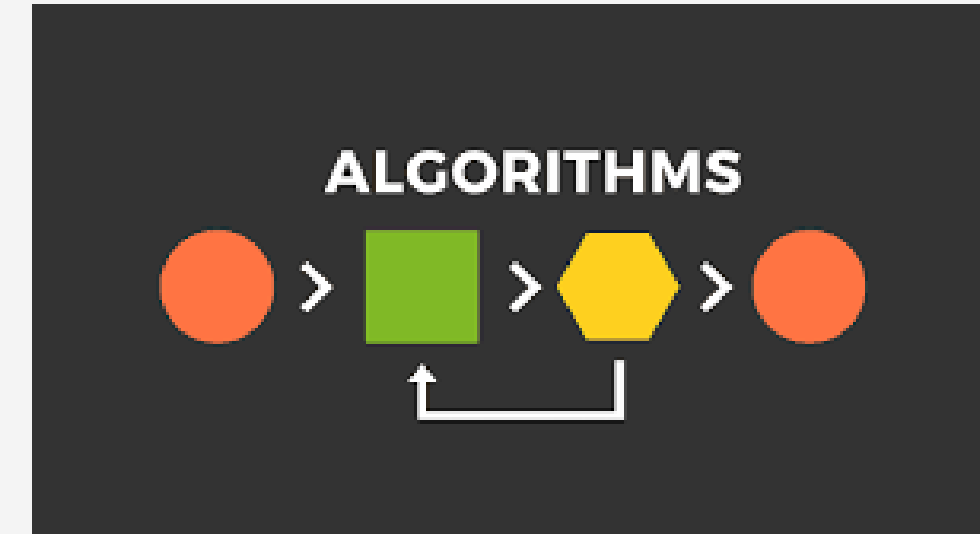
References

- William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006.

- Behrouz A. Foruzan, Cryptography and Network Security, Tata McGraw Hill 2007.