

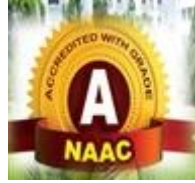


Savitribai Phule Shikshan Prasarak Mandal's
SKN SINHGAD COLLEGE OF ENGINEERING PANDHARPUR.

(Approved by AICTE, Recognized by D.T.E & Affiliated to Solapur University, Solapur.)
At Post- Korti, Taluka-Pandharpur, District-Solapur, Pin-413304.MS.India.

Phone: 02186-250160, Fax: 02186-245195 Website: www.spspm.org & www.sknscoe.ac.in

Department of Computer Science & Engineering.



About Resource Person

Name: Mr. Mahesh Dange

Education: B.Tech. Computer Engineering (BATU, Lonere)

M.Tech (BATU, Lonere)

Experience: More than 12 years in IT Security.

Presently he is working as a Principal Engineer, OpenText Corp., Bangalore.

Principal engineers perform leadership tasks such as training staff, establishing budgets and assigning tasks. They also set deadlines for projects and work on multiple projects at the same time. Provide technical guidance in software design and development activities. Assist in maintenances and upgrades of existing software applications. Provide support in all phases of SDLC and ensure to deliver high-quality products.





Savitribai Phule Shikshan Prasarak Mandal's
SKN SINHGAD COLLEGE OF ENGINEERING PANDHARPUR.

(Approved by AICTE, Recognized by D.T.E & Affiliated to Solapur University, Solapur.)
At Post- Korti, Taluka-Pandharpur, District-Solapur, Pin-413304.MS.India.
Phone: 02186-250160, Fax: 02186-245195 Website: www.spspm.org & www.sknscoe.ac.in

Department of Computer Science & Engineering.



Report

Resource/ Mentor Name	Mr. Mahesh Dange
Designation /Company Name	Principal Engineer, OpenText Corp., Bangalore.
Session Date & Time	02/10/2018 02.30 am
Session Topic	" Network Security"
Venue	CSE Seminar Hall
Target Audience	T.E. Class

About Session:

Mr. Mahesh briefed about his roles & responsibilities related to his job profile.

Then he told objective of this session is to provide the participate with an insight into recent developments in the field of network security and cryptography, with particular regard to digital signatures .cryptography was used as a tool to protect national secrets and strategies. The proliferation of computers and communications systems in the 1960s brought with it a demand from the private sector for means to protect information in digital form and to provide security services. DES, the Data Encryption Standard, is the most well-known cryptographic mechanism. It remains the standard means for securing electronic commerce for many financial institutions around the world. The most striking development in the history of cryptography came in 1976 when Diffie and Hellman published *New Directions in Cryptography*.

A *digital signature* of a message is a number dependent on some secret known only to the signer, and, additionally, on the content of the message being signed. Signatures must be verifiable; if a dispute arises as to whether a party signed a document (caused by either a lying signer trying to *repudiate* a signature it did create, or a fraudulent claimant), an unbiased third party should be able to resolve the matter equitably, without requiring access to the signer's secret information.



Savitribai Phule Shikshan Prasarak Mandal's
SKN SINHGAD COLLEGE OF ENGINEERING PANDHARPUR.

(Approved by AICTE, Recognized by D.T.E & Affiliated to Solapur University, Solapur.)

At Post- Korti, Taluka-Pandharpur, District-Solapur, Pin-413304.MS.India.

Phone: 02186-250160, Fax: 02186-245195 Website: www.spspm.org & www.sknscoe.ac.in

Department of Computer Science & Engineering.



The first method discovered was the RSA signature scheme, which remains today one of the most practical and versatile techniques available. Sub-sequent research has resulted in many alternative digital signature techniques. The Feige-Fiat-Shamir signature scheme requires a one-way hash function.

Information security and cryptography

Cryptography, an understanding of issues related to information security in general is necessary. Information security manifests itself in many ways according to the situation and requirement. Over the centuries, an elaborate set of protocols and mechanisms has been created to deal with information security issues when the information is conveyed by physical documents. Often the objectives of information security cannot solely be achieved through mathematical algorithms and protocols alone, but require procedural techniques and abidance of laws to achieve.

The concept of *information* will be taken to be an understood quantity. For example, privacy of letters is provided by sealed envelopes delivered by an accepted mail service.

Prof.S.B.Thigale conveyed introduction about a resource person Mr. Mahesh. Then As part of tradition Prof.P.R.Gadaker took privilege and offering vote of thanks to Resource person.



Savitribai Phule Shikshan Prasarak Mandal's
SKN SINHGAD COLLEGE OF ENGINEERING PANDHARPUR.

(Approved by AICTE, Recognized by D.T.E & Affiliated to Solapur University, Solapur.)
At Post- Korti, Taluka-Pandharpur, District-Solapur, Pin-413304.MS.India.

Phone: 02186-250160, Fax: 02186-245195 Website: www.spspm.org & www.sknscoe.ac.in

Department of Computer Science & Engineering.

