FV 9863 Dssolhg Fubswrjudskb

Mxob-Qry 5358

Frxuvh Lqwurgxfwlrq

28wk Mxob 5358

Gu. Pdqlndqwdq Vulqlydvdq

CS 6530 Applied Cryptography

July-Nov 2025

Course Introduction

28th July 2025

Dr. Manikantan Srinivasan

Course Details

- CS 6530: Applied Cryptography
- Jul-Nov Semester 2025, 'H' Slot; CS 24
- Lecture Slots: Mon (02.00-03.15 PM); TUE (03.30-04.45 PM);
- Tutorial Slot: Thu (5.00 - 5.50 PM) – Needs a discussion due to meeting time clash
- Thursday. slot will be used for any makeup session / for External Guest Lectures.
- Instructor: Dr. Manikantan Srinivasan - Office: SSB 236-B
- Email: mani@cse.iitm.ac.in, manikantan.srinivasan@india.nec.com. Meetings by appointment.
- TA(s): Will be announced Shortly.
- Note: Course related communications will be via emails, WhatsApp group. Efforts for IITM Moodle site (CS6530) would be made; please regularly check the email that is linked to your email account.

COURSE OBJECTIVES

- The objective of this course is to learn the concepts of cryptography, especially from the view of its application in daily life (Practical relevance). The crypto algorithms (Ciphers) and crypto protocols used currently in different deployments such as Enterprise (on-premise) and Cloud (virtualized) would be studied. Focus on crypto application in Communication / Telecommunication networks will be considered. The course will introduce students to the present world security challenges and enable them with tools towards building sound cyber security solutions.

LEARNING OBJECTIVES

- To understand Cryptography aspects from the perspective of Ciphers and Cryptographic / Security Protocols. Focus will be on latest and important Ciphers
- To understand the Security aspects applicable while data is at rest, data is in use, and data is in motion
- Secure cryptographic needs for – Enterprise and Cloud (Virtualized) deployment requirements
- To gain good knowledge on Key Management and associated protocols, with real world applications – Enterprise / Telecom deployments
- To understand aspects to design and build secure systems, addressing the aspects “what could go wrong” for ciphers and protocols

COURSE PREREQUISITES(S)

- You must have good knowledge on
  - Computer Systems, Networks, ideally done the course CS3205 or equivalent.
  - If you have done any Crypto Course already and aware of Ciphers, it will be an advantage.
- You must have good programming ability and good knoweledge with data structures.
- Strong experience with Linux environment, Virtualized Systems (Dockers) and Open source tools.

CLASSROOM MODE

- Traditional 75-minute lectures twice a week, with one 50-minute slot (per week) used for tutorials, any additional discussions related to assignments/ demonstrations, external guest lectures or makeup on a need basis.

Planned Syllabus (1/2)

The following topics will be covered, but not necessarily in the order listed below:

- Review of cryptography : conventional and public-key cryptography, hash functions, MAC, authentication, and digital signatures.
- Study of Elliptic Curve Crypto systems
- Study of Post Quantum Cryptography – the NIST Approved Ciphers
- Key Management and Distribution: Symmetric Key Distribution, Distribution of PublicKeys, X.509 Certificates, Public-Key Infrastructure.
- Security protocols which utilize cryptographic algorithms to enable secure data transmission, authentication and authorization
  - IP Security: IP Security Overview, IP Security Policy, Encapsulating Security Payload, Combining Security Associations, Internet Key Exchange (IKE), Virtual Private Networks(VPNs).
  - Transport-Level Security: Web Security Considerations, Secure Sockets Layer / Transport, Layer Security, HTTPS standard, Secure Shell (SSH) application.

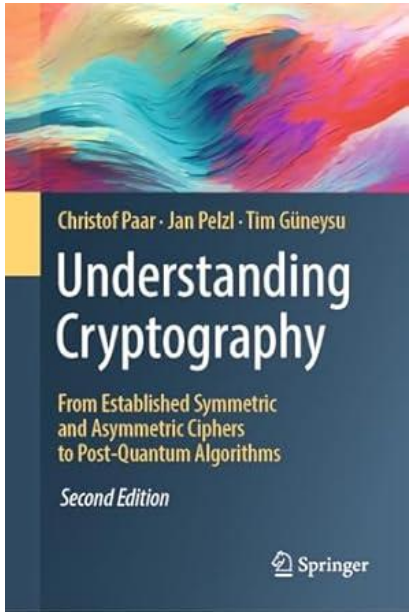
Planned Syllabus (2/2)

The following topics will be covered, but not necessarily in the order listed below:

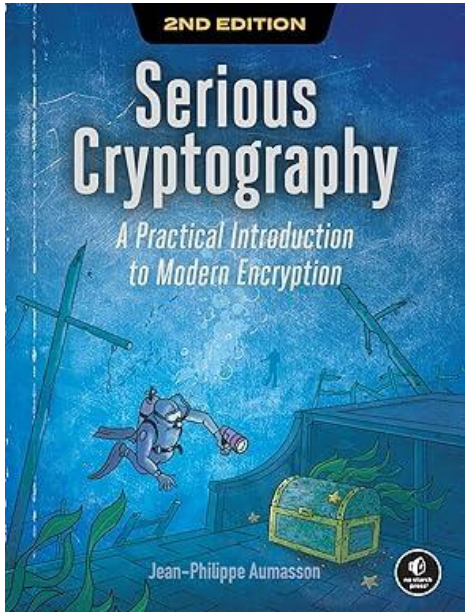
- Threat Modelling, Cyber Threat Intelligence, Introduction to MITRE ATT&CK and tools.
- Design and study of efficient Crypto enabled secure designs – with an emphasis of key management protocols
  - Application to Enterprise deployment, Virtualized (Cloud) deployments
  - Application to Telecommunication Network deployments
- Crypto / Security aspects for securing – AI / ML Model – from development to deployment (Based on ETSI – Securing AI and other material)

REFERENCE BOOKS

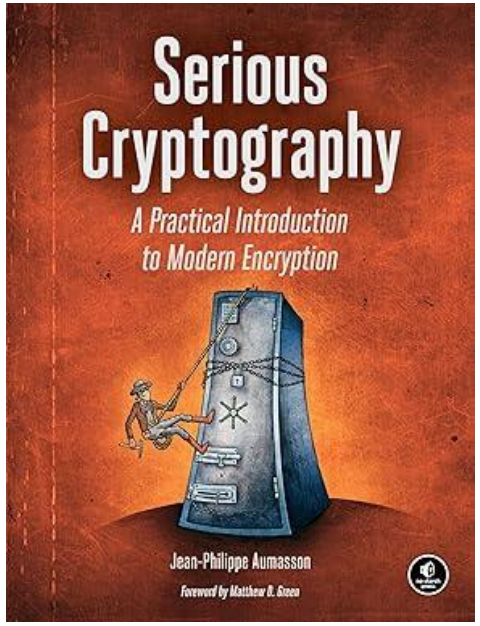
- The following books will be used during the course for the lectures. They can help in understanding the concepts taught in class, and for practice exercises..



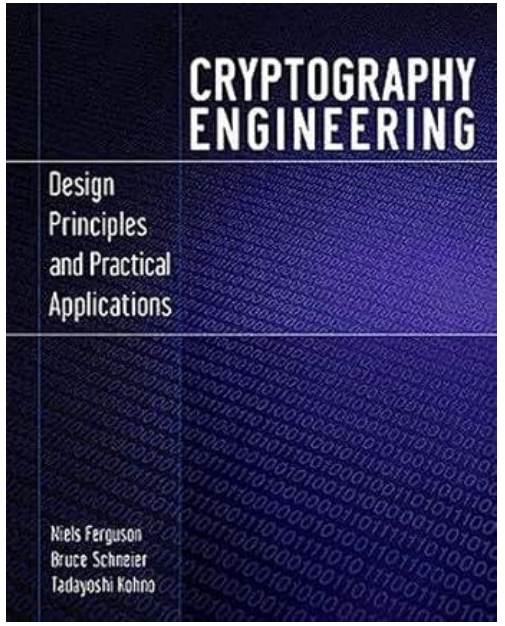
ISBN-13 : 978-3662690062



ISBN-13: 978-1718503847



ISBN-13 : 978-1593278267



ISBN-13: 978-0470474242

- We will consider any relevant latest papers in the field for secure designs

TENTATIVE GRADING POLICY

The following allocation of points is tentative. These may change during the semester.

Component	%
Quiz 1	15 %
Quiz 2	15 %
Programming Assignments (5)	25%
Tutorials/Continuous assessment (Best 5 out of 8)	5%
Course Project (Report submission 30th October, Final Viva 10th/11th Nov 2025, 2 member project)	35%
Class Participation	5%

Thank you – Q&A