

2. “A Course in Cryptography”, Heiko Knospe, American Mathematical Society, 2019 3. “Introduction to Modern Cryptography”, Jonathan Katz, Yehuda Lindell, Chapman & Hall/CRC, 2008 4. “Foundations of Cryptography - Basic Tools”, Oded Goldreich, Cambridge University Press, 2004 5. “Foundations of Cryptography - Basic Applications”, Oded Goldreich, Cambridge University Press, 2009
CSCS 455 - CYBER THREAT INTELLIGENCE
Course Objectives : 1. To make the student aware of the different threats existing from the dark web and to study their behaviour and strategies 2. To employ Machine learning and AI for the same purposes of learning their behaviour
Course Outcomes : 1. Student gets the ability to choose between different AI and ML strategies for gathering threat intelligence 2. Student gets the right skills required for defending the modern day industry infrastructure from attackers
UNIT I Moving to Proactive Cyber Threat Intelligence: Proactive Intelligence beyond the Deepweb and Dark Web, Understanding Darkweb Malicious Hacker Forums: Forum Structure and Community Social Organization.
(12 Hours)
UNIT II Basics of Machine Learning in Cybersecurity : What is machine learning, Different types of machine learning algorithm, Algorithms in machine learning, Knocking Down CAPTCHAs: Characteristics of CAPTCHAs, Using artificial intelligence to crack CAPTCHAs, Using Data Science to Catch Email Fraud and Spam
(12 Hours)
UNIT III Automatic Mining of Cyber Intelligence from the Darkweb, Analysing Products and Vendors in Malicious Hacking Markets: Marketplace Data Characteristics, Users Having Presence in Markets/Forums, Discovery of Zero-Day Exploits, Exploits Targeting Known Vulnerabilities.
(12 Hours)