

PROGRAMME STRUCTURE

Course Information

Credits Requirement for Graduation:

Students must complete at least 40 credits. The minimum cumulative average is 3.000. The minimum credit distribution for this program is as follows:

Core modules	25 credits
Project paper	9 credits
Field Elective	6 credits
Total	40 credits

A. Core Modules (Compulsory)

No	Course Code	Course Name	Credit
1.	SSK5090	Research Methods in Computer Science	3(3+0)
2.	SSK5207	Cyber Law and Ethics	3(3+0)
3.	SSK5500	Security in Computing	3(3+0)
4.	SSK5501	Information Security Management	3(3+0)
5.	SSK5502	Penetration Testing	3(3+0)
6.	SSK5505	Internet and Cloud Computing Security	3(3+0)
7.	SSK5507	Cryptography and Security Protocol	3(3+0)
8.	SSK5508	Computer Forensics and Investigation	3(3+0)
9.	SSK5980	Seminar in Computer Science	1(1+0)
Total Credit			25

B. Project Paper (Compulsory)

No	Course Code	Course Name	Credit
1.	SSK5990	Project	9(0+9)
Total Credit			9

C. Field Electives (Choose 2)

No	Course Code	Course Name	Credit
1.	SSK5504	Software Security	3(3+0)
2.	SSK5509	Trusted Computing	3(3+0)
3.	SSK5510	Steganography	3(3+0)
4.	SSK5514	Intrusion Detection System	3(3+0)
5.	SSK5517	Advanced Cryptography	3(3+0)
6.	SSK5527	Cryptanalysis	3(3+0)
Total Credit			6

Students must choose at least 2 courses from the list of field electives above.

Lecture Hours:

Lecture hours are based on one (1) credit equivalent to one (1) hour of lecture. Classes are conducted at 6:00pm to 9:00pm, weekdays from Monday to Friday.