CYBER SECURITY ENGINEERING

www.ece.iastate.edu (http://www.ece.iastate.edu/)

Administered by the Department of Electrical and Computer Engineering

For the undergraduate curriculum in cyber security engineering leading to the degree Bachelor of Science.

The Department of Electrical and Computer Engineering (ECpE) at Iowa State University provides undergraduate students with the opportunity to learn computer engineering fundamentals, study applications of the most recent advances in state-of-the-art technologies, and to prepare for the practice of cyber security engineering. The student-faculty interaction necessary to realize this opportunity occurs within an environment that is motivated by the principle that excellence in undergraduate education is enhanced by an integrated commitment to successful, long-term research and outreach programs.

The program objectives for the cyber security engineering program describe accomplishments that graduates are expected to attain within five years after graduation. Graduates will have applied their expertise to contemporary problem solving, be engaged professionally, have continued to learn and adapt, and have contributed to their organizations through leadership and teamwork. More specifically, the objectives for expertise, engagement, learning, leadership and teamwork are defined below for the program.

The objectives of the cyber security engineering program at Iowa State University are:

- Graduates, within five years of graduation, should demonstrate peer-recognized **expertise** in computer security principles together with the ability to articulate that expertise and use it for contemporary problem solving in the analysis, design, and operation of the physical, software and human components of a system, including system integration and implementation.
- Graduates, within five years of graduation, should demonstrate **engagement** in the engineering profession, locally and globally, by contributing to the ethical, competent, and creative practice of engineering or other professional careers.
- Graduates, within five years of graduation, should demonstrate sustained **learning** and adapting to a constantly changing field through graduate work, professional development, and self study.
- Graduates, within five years of graduation, should demonstrate **leadership** and initiative to ethically advance professional and organizational goals, facilitate the achievements of others, and obtain substantive results.
- Graduates, within five years of graduation, should demonstrate a commitment to **teamwork** while working with others of diverse cultural and interdisciplinary backgrounds.

As a complement to the instructional activity, the ECpE department provides opportunities for each student to have experience with broadening activities. Through the cooperative education and internship program, students have the opportunity to gain practical industry experience. Students have the opportunity to participate in advanced research activities, and through international exchange programs, students learn about engineering practices in other parts of the world. Well-qualified juniors and seniors in cyber security engineering who are interested in graduate study may apply for concurrent enrollment in the Graduate College to simultaneously pursue both the Bachelor of Science and Master of Science.

Curriculum in Cyber Security Engineering

Administered by the Department of Electrical and Computer Engineering.

Leading to the degree Bachelor of Science.

Total credits required: 125
Any transfer credit courses applied to the degree program require a grade of C or better (but will not be calculated into the ISU cumulative GPA, Basic Program GPA or Core GPA). See also Basic Program and Special Programs.
Note: Department does not allow Pass/Not Pass credits to be used to meet graduation requirements.
International Perspectives: 3 cr. [1]
U.S. Diversity: 3 cr. [1]
Communication Proficiency/Library requirement:

ENGL 150	Critical Thinking and Communication (Must have a C or better in this course)	3
ENGL 250	Written, Oral, Visual, and Electronic Composition (Must have a C or better in this course)	3
LIB 160	Information Literacy	1
One of the following:		3
ENGL 314	Technical Communication (C or better in this course)	
ENGL 309	Proposal and Report Writing (C or better in this course)	

General Education Electives: 21 cr. [3]

ENGL 250	Written, Oral, Visual, and Electronic Composition (Must have a C or better in this course.)	3
ENGL 314	Technical Communication (Must have a C or better in this course.)	3
or ENGL 309	Proposal and Report Writing	
Complete minimum of 6 cr. from Approved General Education Component 300 level and above. [3]		6

Complete additional 9cr. from Approved General Education Component. [3]		9
Total Credits		**21**

Basic Program: 24 cr.
A minimum GPA of 2.00 required for this set of courses (please note that transfer course grades will not be calculated into the Basic Program GPA). See Requirement for Entry into Professional Program in College of Engineering Overview section.

CHEM 167	General Chemistry for Engineering Students	4
or CHEM 177	General Chemistry I	
ENGL 150	Critical Thinking and Communication (Must have a C or better in this course)	3
ENGR 101	Engineering Orientation	R
CPR E 185	Introduction to Computer Engineering and Problem Solving I [2]	3
LIB 160	Information Literacy	1
MATH 165	Calculus I	4
MATH 166	Calculus II	4
PHYS 221	Introduction to Classical Physics I	5
Total Credits		**24**

Math and Physical Science: 17 cr.

COM S 227	Object-oriented Programming	4
COM S 228	Introduction to Data Structures	3
MATH 267	Elementary Differential Equations and Laplace Transforms	4
STAT 330	Probability and Statistics for Computer Science	3
Math Elective [3]		3
Total Credits		**17**

Cyber Security Engineering Core: 37 cr.
(A minimum GPA of 2.00 required for this set of courses, including any transfer courses; please note that transfer course grades will not be calculated into the Core GPA).

CYB E 230	Cyber Security Fundamentals	3
CYB E 231	Cyber Security Concepts and Tools	3
CYB E 234	Legal, Professional, and Ethical Issues in Cyber Systems	3
CYB E 331	Application of Cryptographic Concepts to Cyber Security	3
CPR E 281	Digital Logic	4
CPR E 288	Embedded Systems I: Introduction	4
CPR E 308	Operating Systems: Principles and Practice	4
CPR E 310	Theoretical Foundations of Computer Engineering	3
CPR E 381	Computer Organization and Assembly Level Programming	4
COM S 309	Software Development Practices	3
CPR E 315	Applications of Algorithms in Computer Engineering	3
or COM S 311	Introduction to the Design and Analysis of Algorithms	
Total Credits		**37**

Other Remaining Courses: 26 cr.

CPR E 491	Senior Design Project I and Professionalism	3
CPR E 492	Senior Design Project II	2
Cyber SecurityTechnical Electives [3]		12
Computer Engineering Technical Electives [3]		3
Technical Electives [3]		6
Total Credits		**26**

Seminar/Co-op/Internships [4]:

CPR E 166	Professional Programs Orientation	R
CPR E 294	Program Discovery	R
CPR E 494	Portfolio Assessment	R

Transfer Credit Requirements

The degree program must include a minimum of 30 credits at the 300-level or above in professional and technical courses earned at ISU in order to receive a B.S. in computer engineering. These 30 credits must include CPR E 491 Senior Design Project I and Professionalism, CPR E 492 Senior Design Project II, and credits in the core professional curriculum and/or in technical electives. The Electrical and Computer Engineering Department requires a grade of C or better for any transfer credit course that is applied to the degree program.

1. These university requirements will add to the minimum credits of the program unless the university-approved courses are also approved by the department to meet other course requirements within the degree program. U.S. diversity and international perspectives courses may not be taken Pass/Not Pass, but are used to meet the general education electives.
2. See Basic Program for Professional Engineering Curricula for accepted substitutions for curriculum designated courses in the Basic Program.
3. From department approved lists. (http://www.ece.iastate.edu/academics/bachelors-degree-requirements/)
4. Co-op / Internships are optional

See also: A 4-year plan of study grid showing course template by semester. (http://catalog.iastate.edu/previouscatalogs/2021-2022/collegeofengineering/cybersecurityengineering/#fouryearplantext)

Note: International perspectives and U.S. diversity courses are used to meet the general education electives.

Cyber Security Engineering, B.S.

First Year

Fall	Credits	Spring	Credits
CHEM 167	4	COM S 227	4
CPR E 185	3	CPR E 166	R
ENGL 150	3	MATH 166	4
ENGR 101	R	PHYS 221	5
LIB 160	1	General Education Elective	3
MATH 165	4		
	15		**16**

Second Year

Fall	Credits	Spring	Credits
CPR E 281	4	CPR E 288	4
COM S 228	3	ENGL 250	3
CPR E 294	R	Math Elective	3
MATH 267	4	CYB E 231	3
CYB E 230	3	CYB E 234	3
	14		**16**

Third Year

Fall	Credits	Spring	Credits
CPR E 381	4	COM S 311 or CPR E 315	3
CPR E 310	3	CPR E 308	4
COM S 309	3	ENGL 314 or ENGL 309	3
CYB E 331	3	General Education Elective	3
General Education Elective	3	Cyber Security Elective	3
	16		**16**

Fourth Year

Fall	Credits	Spring	Credits
CPR E 491	3	CPR E 492	2
CPR E 494	R	Tech Elective	6
STAT 330	3	General Education Elective	3
Cyber Security Elective	6	Cyber Security Elective	3
CPR E Elective	3		
General Education Elective	3		
	18		**14**

Courses primarily for undergraduates:

CYB E 230: Cyber Security Fundamentals

(Cross-listed with CPR E). (2-2) Cr. 3. F.

Prereq: COM S 227 or E E 285 or MIS 207.

Introduction to computer and network infrastructures used to support cyber security. Basic concepts of computer and network configuration used to secure environments. Computer virtualization, network routing and address translation, computer installation and configuration, network monitoring, in a virtual environment. Laboratory experiments and exercises including secure computer and network configuration and management.

CYB E 231: Cyber Security Concepts and Tools

(Cross-listed with CPR E). (2-2) Cr. 3. S.

Prereq: CPR E 230 or CYB E 230

Basic concepts of practical computer and Internet security and the tools used to protect and attack systems and networks. Computer and network security methods including: user authentication, access control, firewalls, intrusion detection, use of vulnerability assessment tools and methods, and penetration testing. Ethics and legal issues in cyber security will also be covered. Laboratory experiments and exercises including evaluating systems for vulnerabilities, understanding potential exploits of the systems, and defenses for the systems.

CYB E 234: Legal, Professional, and Ethical Issues in Cyber Systems

(Cross-listed with CPR E). (3-0) Cr. 3. S.

Prereq: COM S 227, or E E 285, or MIS 207

Emphasizes legal, ethical, and professional issues in cyber systems. Other topics include privacy, government regulation, and compliance as applied to professional practice. Guest lecturer from government and industry, as well as discussions including current legal and ethical issues found in the main stream.

CYB E 331: Application of Cryptographic Concepts to Cyber Security

(Cross-listed with CPR E). Cr. 3. F.S.

Prereq: CPR E 231 or CYB E 231

Basic cryptographic underpinnings used in modern cyber security encryption suites. Encryption benefits to cyber security and its use in protocols. Topics include cryptographically secure hash functions and pseudorandom numbers, key distribution techniques, secure authentication including single sign on. Detection and prevention of security threats such as covert communication, malicious code, and other security threats in protocols are included. In addition to laboratory experiments and exercises, students complete a project focused on cyber security problem and solution.