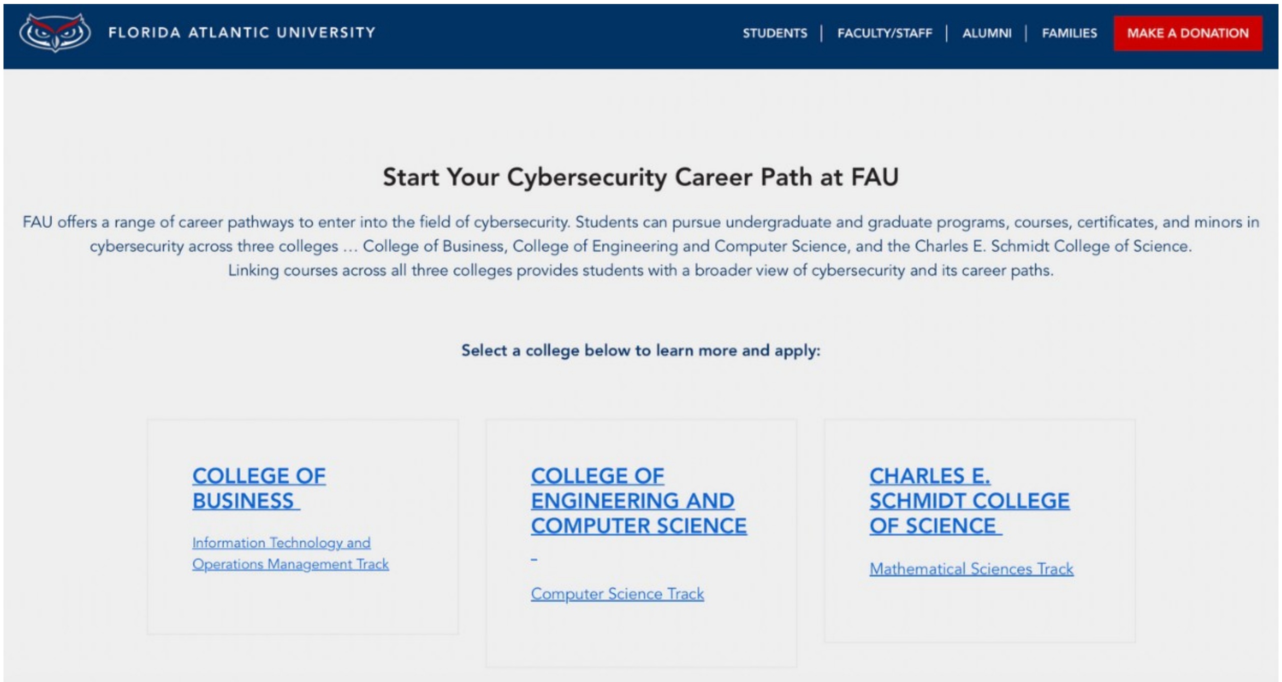
This document, prepared by the Department of Mathematics and Statistics and the College of Science, outlines the College of Science's concerns in response to the proposal from the College of Engineering and Computer Science (CoECS) to develop and implement an AI + Cybersecurity Bachelor of Science program.

1) We Have an Existing Program in Cybersecurity

Cybersecurity is fundamentally rooted in rigorous mathematical foundations. At its core, it protects information and systems by managing risk through confidentiality, integrity, availability, layered defenses, cryptography, and sound design principles. These principles depend on mathematically intensive disciplines such as cryptography (provable security, key exchange, digital signatures), number theory, algebra, information theory, complexity theory, and probability theory. Such depth resides naturally within a mathematics department. If cybersecurity education becomes detached from these disciplines, it risks becoming procedural rather than principled. At the university level, education must be grounded in research and foundational understanding, especially in an era of rapid technological change.

Our department already offers a Bachelor of Science in Mathematics with a concentration in Cryptology, which we plan to rename as a concentration in Cybersecurity to better reflect its scope. The program combines strong theoretical preparation with meaningful applications, including blockchain security, data science, and the study of quantum algorithms and their implications for modern security systems. Students also make use of AI tools where appropriate. This integrated approach ensures that students understand both the underlying principles of security and the evolving technologies built upon them.

The FAU Mathematics track is officially recognized by Florida Atlantic University on its cybersecurity website (https://www.fau.edu/cybersecurity/) as an established pathway into the field, affirming the central role of mathematics in the university's cybersecurity ecosystem.


FLORIDA ATLANTIC UNIVERSITY
STUDENTS | FACULTY/STAFF | ALUMNI | FAMILIES
MAKE A DONATION

Start Your Cybersecurity Career Path at FAU

FAU offers a range of career pathways to enter into the field of cybersecurity. Students can pursue undergraduate and graduate programs, courses, certificates, and minors in cybersecurity across three colleges … College of Business, College of Engineering and Computer Science, and the Charles E. Schmidt College of Science. Linking courses across all three colleges provides students with a broader view of cybersecurity and its career paths.

Select a college below to learn more and apply:

COLLEGE OF BUSINESS
Information Technology and Operations Management Track

COLLEGE OF ENGINEERING AND COMPUTER SCIENCE
-
Computer Science Track

CHARLES E. SCHMIDT COLLEGE OF SCIENCE
Mathematical Sciences Track

2) In Our College We Are Developing AI Components for the Curriculum

We fully recognize the growing importance of artificial intelligence in cybersecurity and are actively strengthening our curriculum accordingly. Within the College of Science, AI is naturally embedded across programs - not merely as a practical tool, but from its scientific and mathematical foundations. Our approach emphasizes understanding the theory that drives AI, including mathematical principles that it is based on.

In the cybersecurity concentration, students already engage with AI tools where appropriate, and we are developing a dedicated course on the mathematical foundations of AI to deepen this preparation. This ensures that students understand how AI methods work, what assumptions they rely on, and how to evaluate their reliability and limitations in security contexts. A strong theoretical foundation not only enhances present applications but also prepares students to address future technological developments and unforeseen challenges with analytical rigor and adaptability.

While the AI + Cybersecurity program proposed by CoECS significantly overlaps with our existing concentration, it does not provide the depth of mathematical foundations that characterize our program. Our curriculum is built upon rigorous training in cryptography, algebra, number theory, probability, complexity theory, and information theory - disciplines essential for principled and research-driven cybersecurity education. Without this foundation, a program risks emphasizing tools and applications without ensuring long-term conceptual strength. For these reasons, duplication would not only be unnecessary but would also create competing pathways of unequal academic depth within the same institution.

(A direct comparison of the two programs and highlighted overlap is added at the end of this document).

3) AI in Cybersecurity Without Foundations Will Not Do Well

AI-based tools can enhance anomaly detection, malware classification, and network monitoring, but they do not establish security guarantees. Trust in digital systems ultimately depends on encryption, authentication, secure key establishment, and formal security proofs. AI operates on top of this cryptographic infrastructure; it strengthens detection and response but does not replace foundational mechanisms.

A cybersecurity program that is not closely integrated with mathematical foundations, cryptography and information theory risks training students to operate tools without understanding adversarial models, formal guarantees, or risk frameworks. The long-term value of a cybersecurity degree lies in conceptual depth and mathematical reasoning, not in familiarity with short-lived technologies. Professionals prepared in this way are better equipped to address emerging threats and future technological revolutions.

4) Engineering Program Competing with Our Student Enrollment

If CoECS proposes a shared program, we would be open to collaboration only if the CIP code is formally housed within the Department of Mathematics and Statistics, where the intellectual and theoretical foundation of cybersecurity resides. Maintaining the CIP designation in Mathematics ensures academic coherence, preserves the program’s research-based identity, and reflects the department’s established expertise in the field.

Collaboration under alternative terms is not feasible, as it would shift enrollment away from Mathematics and weaken the sustainability of our existing program. To safeguard academic integrity, prevent fragmentation, and maintain a strong and principled cybersecurity identity at the university, the structure outlined above is essential.

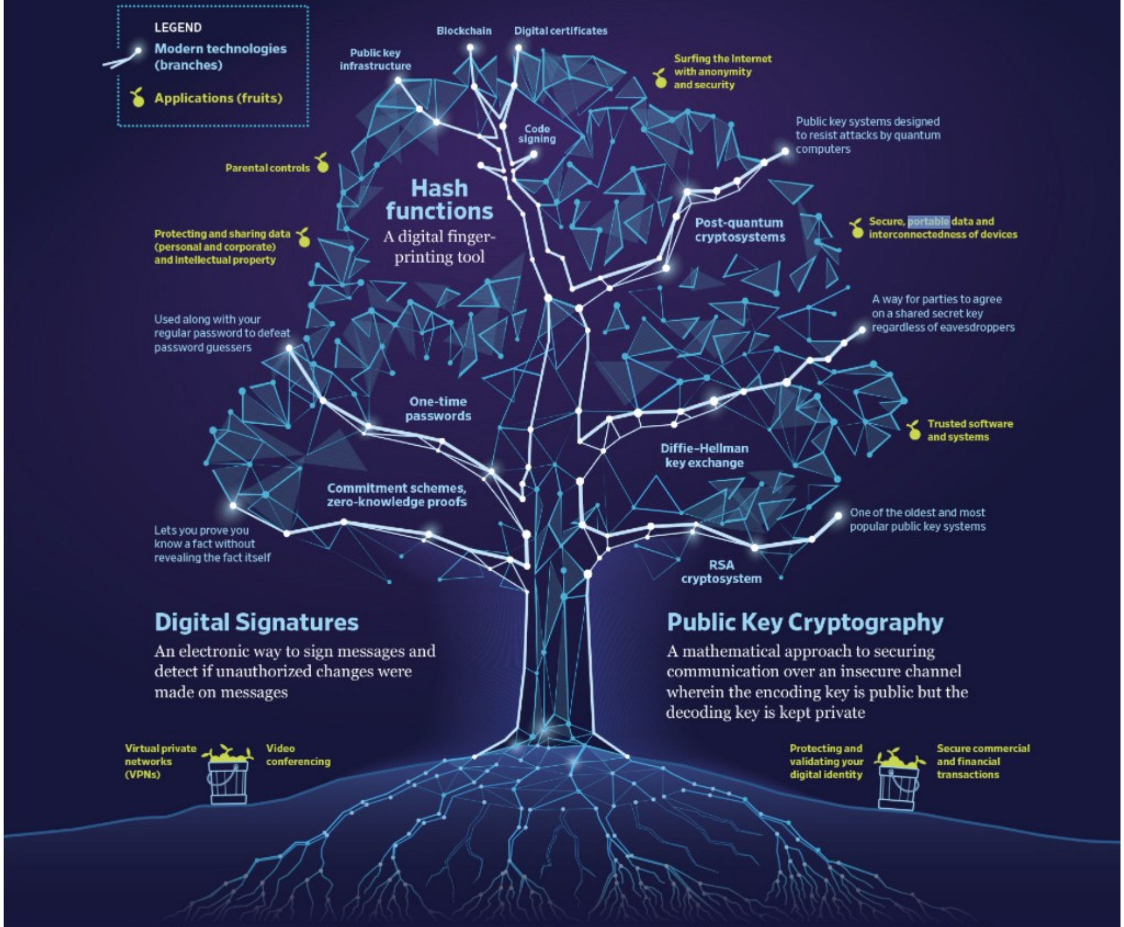
We would like to share a poster from the National Academies of Sciences which indicates the fundamental role of mathematics in cybersecurity. (https://nap.nationalacademies.org/resource/other/deps/illustrating-math/interactive/jpg/Securing-the-internet.jpg)

The Mathematics of Internet Security

The Internet is a transformative network that is an integral part of our daily lives—but, unfortunately, its use involves many security challenges. With roots in abstract mathematics, some new and some very old, a tree of technologies (cryptosystems and authentication schemes) has grown to meet evolving threats. As users of the Internet, we routinely enjoy this tree's fruits and may not appreciate their origins.

Mathematics helps protect against evolving threats

- Bots and fake accounts
- Corporate espionage
- Malicious websites
- Financial fraud and hacking
- Identity theft
- Intellectual property theft
- Malware or spyware
- Phishing, trojans, and spam
- Stolen medical records


LEGEND
Modern technologies (branches)
Applications (fruits)
Blockchain
Digital certificates
Public key infrastructure
Surfing the Internet with anonymity and security
Code signing
Public key systems designed to resist attacks by quantum computers
Parental controls
Hash functions
A digital finger-printing tool
Post-quantum cryptosystems
Secure, portable data and interconnectedness of devices
Protecting and sharing data (personal and corporate) and intellectual property
A way for parties to agree on a shared secret key regardless of eavesdroppers
Used along with your regular password to defeat password guessers
One-time passwords
Trusted software and systems
Diffie–Hellman key exchange
Commitment schemes, zero-knowledge proofs
One of the oldest and most popular public key systems
Lets you prove you know a fact without revealing the fact itself
RSA cryptosystem
Virtual private networks (VPNs)
Video conferencing
Protecting and validating your digital identity
Secure commercial and financial transactions

Digital Signatures

An electronic way to sign messages and detect if unauthorized changes were made on messages

Public Key Cryptography

A mathematical approach to securing communication over an insecure channel wherein the encoding key is public but the decoding key is kept private

Intractable computations

Cryptosystems aim to force an eavesdropper to solve intractable problems that often involve large numbers while the intended users simply verify known solutions. These intractable problems include finding the shortest vector in a lattice (1998) and decoding random linear codes (1978).

Algebra on elliptic curves

An elliptic curve over a finite field is a simplified solution set to a polynomial equation. In the 1980s, it was noticed that translating cryptographic algorithms into this setting allowed the use of smaller numbers while achieving the same level of security.

Concentration inequalities

Concentration inequalities, such as Bernstein's Inequalities (ca. 1930), are used to analyze the security of cryptosystems. These limit the chances that a random variable, a quantity that changes upon repeated measurements, is significantly different from what is expected.

Computational number theory

This field studies ways to use computers to solve arithmetic problems. The RSA cryptosystem uses the unique prime factorizations of numbers (ca. 300 BCE) and Euler's theorem (1763), and its security relies on the obstacle of identifying such factors for select large numbers.

High-dimensional geometry

Structured collections of points called lattices are useful settings for cryptosystems and problems in cryptology. Lattices in high dimensions were used to create the first proof-of-concept system for homomorphic encryption (2009).

[INTERNET SECURITY IS ROOTED IN MATHEMATICS]

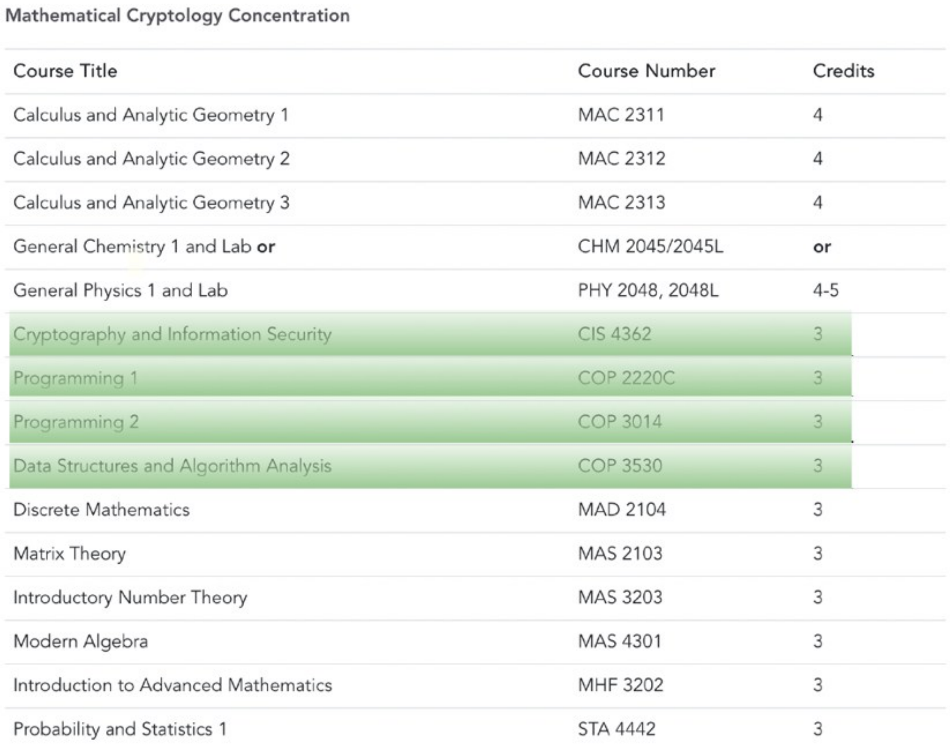
NATIONAL ACADEMIES
Sciences
Engineering
Medicine

This information is from Illustrating the Impact of the Mathematical Sciences, available online at http://nas.edu/illustrating-math.

Comparison of the existing program of BS in Mathematics with Concentration in Cryptology with the newly proposed program BS in AI+Cybersecurity.

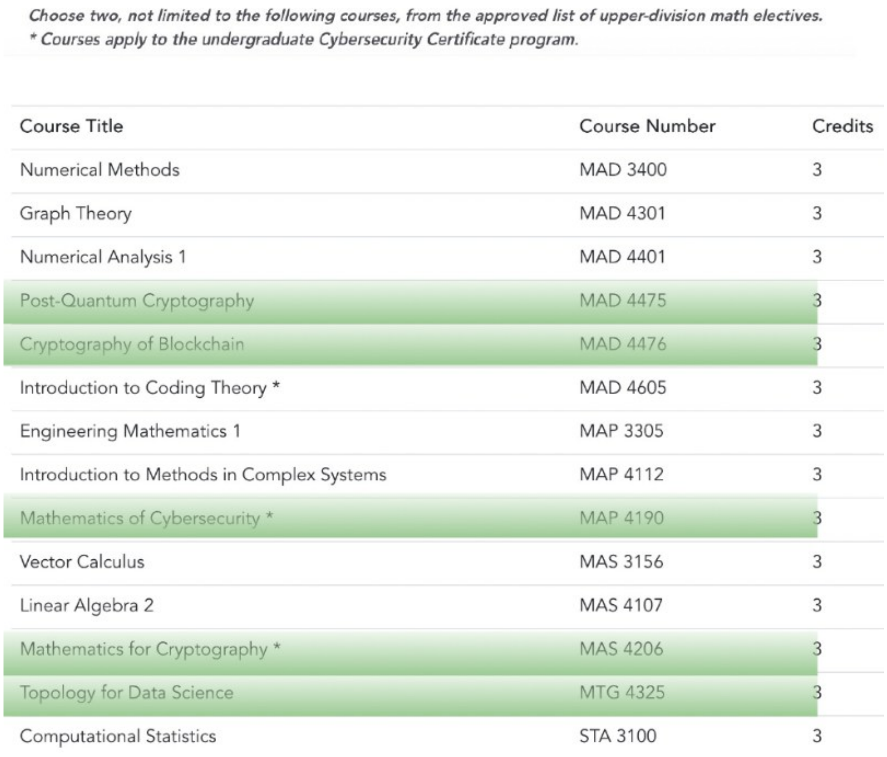
The highlighted courses indicate significant overlap in content between the two programs.

1) Bachelor of Science in Mathematics with Concentration in Cryptology



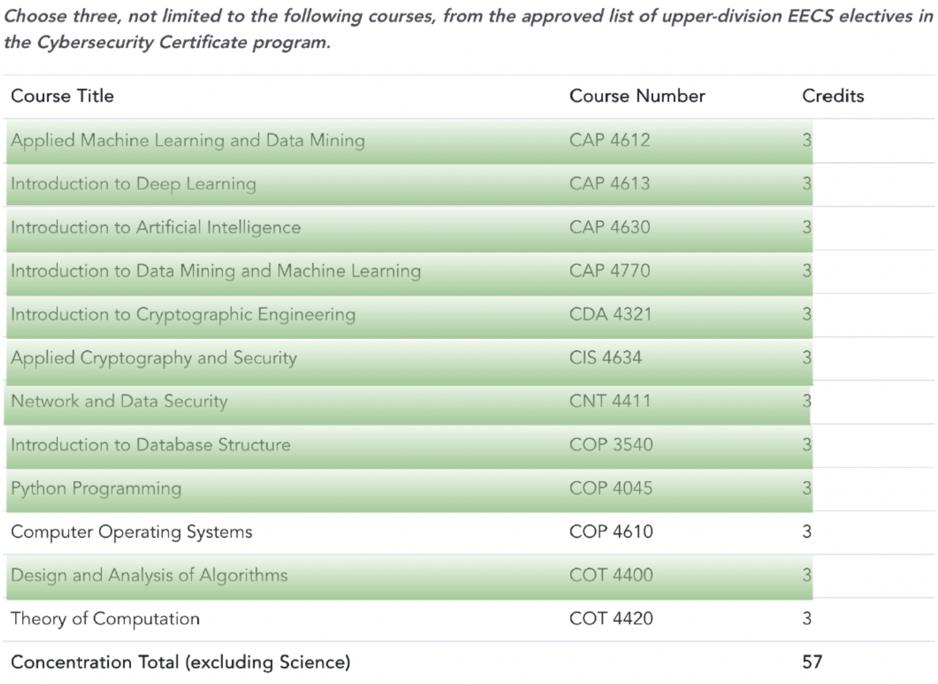
Mathematical Cryptology Concentration

Course Title	Course Number	Credits
Calculus and Analytic Geometry 1	MAC 2311	4
Calculus and Analytic Geometry 2	MAC 2312	4
Calculus and Analytic Geometry 3	MAC 2313	4
General Chemistry 1 and Lab **or**	CHM 2045/2045L	**or**
General Physics 1 and Lab	PHY 2048, 2048L	4-5
Cryptography and Information Security	CIS 4362	3
Programming 1	COP 2220C	3
Programming 2	COP 3014	3
Data Structures and Algorithm Analysis	COP 3530	3
Discrete Mathematics	MAD 2104	3
Matrix Theory	MAS 2103	3
Introductory Number Theory	MAS 3203	3
Modern Algebra	MAS 4301	3
Introduction to Advanced Mathematics	MHF 3202	3
Probability and Statistics 1	STA 4442	3



Choose two, not limited to the following courses, from the approved list of upper-division math electives.
** Courses apply to the undergraduate Cybersecurity Certificate program.*

Course Title	Course Number	Credits
Numerical Methods	MAD 3400	3
Graph Theory	MAD 4301	3
Numerical Analysis 1	MAD 4401	3
Post-Quantum Cryptography	MAD 4475	3
Cryptography of Blockchain	MAD 4476	3
Introduction to Coding Theory *	MAD 4605	3
Engineering Mathematics 1	MAP 3305	3
Introduction to Methods in Complex Systems	MAP 4112	3
Mathematics of Cybersecurity *	MAP 4190	3
Vector Calculus	MAS 3156	3
Linear Algebra 2	MAS 4107	3
Mathematics for Cryptography *	MAS 4206	3
Topology for Data Science	MTG 4325	3
Computational Statistics	STA 3100	3

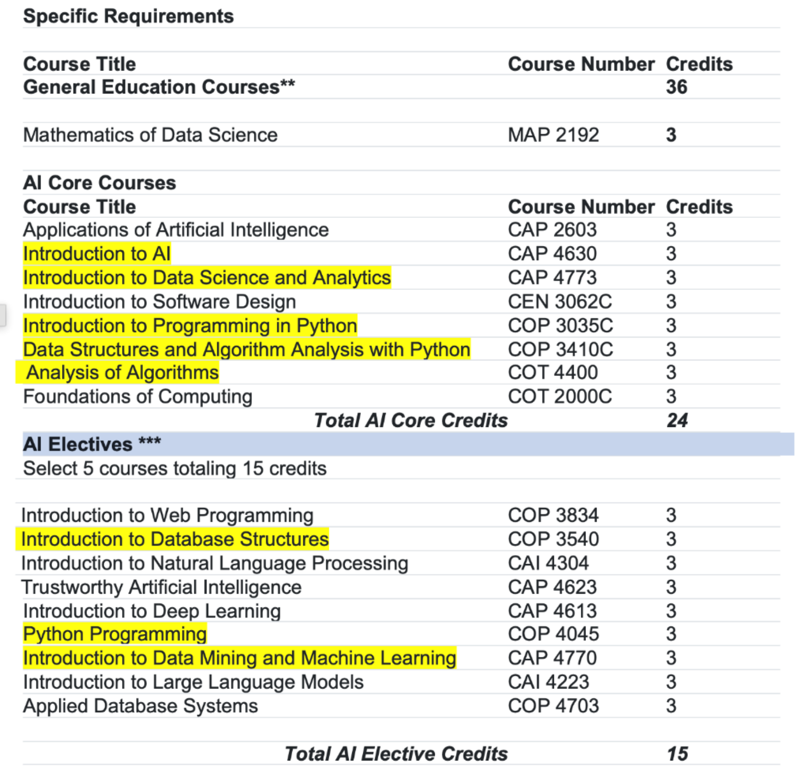


Choose three, not limited to the following courses, from the approved list of upper-division EECS electives in the Cybersecurity Certificate program.

Course Title	Course Number	Credits
Applied Machine Learning and Data Mining	CAP 4612	3
Introduction to Deep Learning	CAP 4613	3
Introduction to Artificial Intelligence	CAP 4630	3
Introduction to Data Mining and Machine Learning	CAP 4770	3
Introduction to Cryptographic Engineering	CDA 4321	3
Applied Cryptography and Security	CIS 4634	3
Network and Data Security	CNT 4411	3
Introduction to Database Structure	COP 3540	3
Python Programming	COP 4045	3
Computer Operating Systems	COP 4610	3
Design and Analysis of Algorithms	COT 4400	3
Theory of Computation	COT 4420	3
Concentration Total (excluding Science)		57

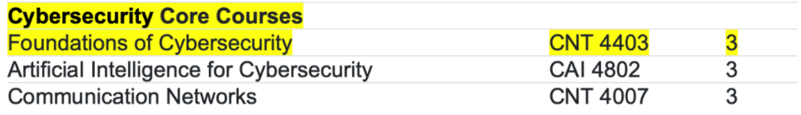
2) Bachelor of Science in AI+Cybersecurity (by CoECS)

(the highlighted courses are an overlap with the courses we offer in our Math Cryptology concentration)

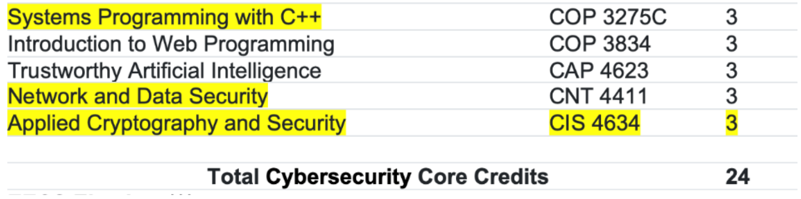


Specific Requirements

Course Title	Course Number	Credits
General Education Courses**		**36**
Mathematics of Data Science	MAP 2192	**3**
AI Core Courses		
Course Title	**Course Number**	**Credits**
Applications of Artificial Intelligence	CAP 2603	3
Introduction to AI	CAP 4630	3
Introduction to Data Science and Analytics	CAP 4773	3
Introduction to Software Design	CEN 3062C	3
Introduction to Programming in Python	COP 3035C	3
Data Structures and Algorithm Analysis with Python	COP 3410C	3
Analysis of Algorithms	COT 4400	3
Foundations of Computing	COT 2000C	3
Total AI Core Credits		***24***
AI Electives ***		
Select 5 courses totaling 15 credits		
Introduction to Web Programming	COP 3834	3
Introduction to Database Structures	COP 3540	3
Introduction to Natural Language Processing	CAI 4304	3
Trustworthy Artificial Intelligence	CAP 4623	3
Introduction to Deep Learning	CAP 4613	3
Python Programming	COP 4045	3
Introduction to Data Mining and Machine Learning	CAP 4770	3
Introduction to Large Language Models	CAI 4223	3
Applied Database Systems	COP 4703	3
Total AI Elective Credits		***15***



Cybersecurity Core Courses		
Foundations of Cybersecurity	CNT 4403	3
Artificial Intelligence for Cybersecurity	CAI 4802	3
Communication Networks	CNT 4007	3



Systems Programming with C++	COP 3275C	3
Introduction to Web Programming	COP 3834	3
Trustworthy Artificial Intelligence	CAP 4623	3
Network and Data Security	CNT 4411	3
Applied Cryptography and Security	CIS 4634	3
Total Cybersecurity Core Credits		**24**