MODULE DESCRIPTION FORM

نموذج وصف المادة الدراسية

Module Information معلومات المادة الدراسية					
Module Title	**Probability & Statistics for Cybersecurity / الاحتمالية والإحصاء للأمن السيبراني**			**Module Delivery**	
Module Type	**Core**			☒ **Theory** ☒ **Lecture** ☒ **Tutorial** ☐ **Practical** ☐ **Seminar**	
Module Code	CYBT207				
ECTS Credits	**6**				
SWL (hr/sem)	**150**				
Module Level			**Semester of Delivery**	4	
Administering Department	Department of Cybersecurity Technical Engineering		**College**	Technical Engineering College of Computer and Artificial Intelligence - Kirkuk	
Module Leader			**e-mail**		
Module Leader's Acad. Title			**Module Leader's Qualification**		
Module Tutor			**e-mail**		
Peer Reviewer Name			**e-mail**		
Scientific Committee Approval Date	2/11/2026		**Version Number**	1.0	

Relation with other Modules العلاقة مع المواد الدراسية الأخرى			
Prerequisite module	Discrete Mathematics & Calculus	**Semester**	3

Module Aims, Learning Outcomes and Indicative Contents أهداف المادة الدراسية ونتائج التعلم والمحتويات الإرشادية	
Module Aims أهداف المادة الدراسية	This module aims to provide cybersecurity students with a solid mathematical foundation in probability theory, random variables, and statistical inference tailored for security analysis and risk assessment. It focuses on probability axioms, Bayes' Theorem for threat classification, discrete and continuous distributions (modeling DDoS, malware propagation, and failure rates), hypothesis testing for Intrusion Detection Systems (IDS), Chi-square randomness testing for cryptographic PRNGs, Markov chains for state-based threat modeling, and statistical anomaly detection using Python/R.
Module Learning Outcomes مخرجات التعلم للمادة الدراسية	Understand probability fundamentals, conditional probability, and Bayes' Theorem for probabilistic threat modeling. Master discrete and continuous probability distributions to model network traffic, packet inter-arrival times, and vulnerability occurrences. Apply statistical inference, confidence intervals, and hypothesis testing to evaluate security metrics and False Positive/Negative rates. Perform randomness testing (Chi-Square) to validate cryptographic pseudo-random number generators (PRNGs). Model dynamic security states, malware behavior, and system reliability using Markov chains and stochastic processes. Implement statistical anomaly detection algorithms (Naïve Bayes, Z-score, IQR) for intrusion detection and spam filtering. Utilize programming tools (Python NumPy/SciPy/Pandas or R) for statistical data analysis, visualization, and security modeling.
Indicative Contents المحتويات الإرشادية	The module will cover the following key areas: Introduction to Probability and Statistics in Cybersecurity & Risk Analysis Sample Space, Events, Axioms of Probability, Combinatorics, and Counting Rules Conditional Probability, Independence, Bayes' Theorem, and Naïve Bayesian Threat Filtering Discrete Random Variables, PMF, Cumulative Distributions, Expectation, and Variance Key Discrete Distributions: Binomial, Poisson, Geometric, and Hypergeometric (Modeling Attacks & Packets) Continuous Random Variables, PDF, CDF, Normal/Gaussian Distribution, Exponential & Weibull Distributions Joint Probability Distributions, Covariance, Correlation, and Central Limit Theorem (CLT) Descriptive Statistics, Data Visualization, and Exploratory Security Data Analysis Statistical Inference: Parameter Estimation, Confidence Intervals, and Hypothesis Testing (Z-test, T-test, P-values) Errors in Hypothesis Testing: Type I (False Positive) and Type II (False Negative) Errors in IDS Evaluation Chi-Square Tests: Goodness-of-Fit Test and Independence Testing for Cryptographic Randomness Markov Chains & Stochastic Processes: State Transition Matrices, Stationary Distributions, and Behavioral Modeling Statistical Anomaly Detection, Quantitative Risk Assessment (ALE & Loss Event Frequency), and Security Metrics

Learning and Teaching Strategies استراتيجيات التعلم والتعليم	
Strategies	The module will employ a combination of strategies including: Lectures: To provide rigorous theoretical foundations on probability theory, statistical inference, and stochastic modeling. Group Discussions: To analyze probabilistic security models, false alarm trade-offs, and statistical attack metrics. Problem-Solving Sessions: To solve mathematical problems on probability distributions, hypothesis testing, and Bayes' theorem. Practical Lab Sessions: Hands-on statistical analysis, simulation, and anomaly detection modeling using Python (Jupyter Notebooks) or R. Tutorials: To practice complex statistical calculations, Markov state transitions, and Chi-Square randomness tests. Mid-term and final exams: To evaluate theoretical understanding and analytical problem-solving skills. Preparatory Week: To give students time to revise and clarify any difficulties before the final exam.

Student Workload (SWL) الحمل الدراسي للطالب محسوب لـ ١٥ أسبوعا			
Structured SWL (h/sem) الحمل الدراسي المنتظم للطالب خلال الفصل	63	**Structured SWL (h/w)** الحمل الدراسي المنتظم للطالب أسبوعيا	
Unstructured SWL (h/sem) الحمل الدراسي غير المنتظم للطالب خلال الفصل	87	**Unstructured SWL (h/w)** الحمل الدراسي غير المنتظم للطالب أسبوعيا	
Total SWL (h/sem) الحمل الدراسي الكلي للطالب خلال الفصل	150		

Module Evaluation تقييم المادة الدراسية					
		Time/Number	**Weight (Marks)**	**Week Due**	**Relevant Learning Outcome**
Formative assessment	**Quizzes**	2	5% (5)	5, 10	LO #1, 3 and 5
	Assignments	2	5% (5)	2, 12	LO #2, 4 and 6
	Projects / Lab.	1	10% (10)	Continuous	LO #7

	Report	1	10% (10)	13	LO #3, 5 and 7
Summative assessment	**Midterm Exam**	2 hr	20% (20)	8	LO #1 - 4
	Final Exam	2hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus) المنهاج الاسبوعي النظري	
	Material Covered
Week 1	Introduction to Probability and Statistics in Cybersecurity: Role in Risk Analysis, Anomaly Detection, and Cryptography.
Week 2	Probability Foundations: Sample Spaces, Events, Probability Axioms, Addition and Multiplication Rules.
Week 3	Conditional Probability, Total Probability Theorem, Independence of Events.
Week 4	Bayes' Theorem: Concept, Mathematical Derivation, and Application in Bayesian Spam & Threat Filtering.
Week 5	Discrete Random Variables: Probability Mass Function (PMF), Cumulative Distribution Function (CDF), Expectation, and Variance.
Week 6	Discrete Distributions in Security: Binomial Distribution (Attack Success), Poisson Distribution (DDoS Packet Rates).
Week 7	Geometric & Hypergeometric Distributions: Vulnerability Discovery Rates and System Failure Modeling.
Week 8	Mid-term Exam (الفصل منتصف اختبار) & Continuous Random Variables: Probability Density Functions (PDF) and CDF.
Week 9	Continuous Distributions: Normal/Gaussian Distribution, Standard Normal Curves, and Exponential Distribution (Inter-arrival Times).
Week 10	Joint Distributions, Covariance, Correlation Analysis, and Central Limit Theorem (CLT) Applications.
Week 11	Descriptive Statistics & Data Visualization: Mean, Median, Variance, Standard Deviation, IQR, Boxplots in Security Data.
Week 12	Statistical Inference: Sampling Distributions, Point Estimation, and Confidence Interval Calculations.
Week 13	Hypothesis Testing Foundations: Null vs. Alternative Hypotheses, Test Statistics, Z-Test, T-Test, and P-Values.

Week 14	Evaluating Security Systems: Type I Error (False Positive) vs Type II Error (False Negative) Trade-offs in IDS/IPS.
Week 15	Chi-Square Tests: Goodness-of-Fit and Testing Randomness in Cryptographic Pseudo-Random Number Generators (PRNGs).
Week 16	**Markov Chains & Stochastic Modeling: State Transitions, Threat Modeling / Final Examination.**

Learning and Teaching Resources
مصادر التعلم والتدريس

	Text	Available in the Library?
Required Texts	Ross, S. M. (2020). "Introduction to Probability and Statistics for Engineers and Scientists" (6th ed.). Academic Press.	Yes
Recommended Texts	Devore, J. L. (2016). "Probability and Statistics for Engineering and the Sciences" (9th ed.). Cengage Learning.	Yes
Websites	Yes	

Grading Scheme
مخطط الدرجات

Group	Grade	التقدير	Marks (%)	Definition
Success Group (50 - 100)	**A** - Excellent	امتياز	90 - 100	Outstanding Performance
	B - Very Good	جيد جدا	80 - 89	Above average with some errors
	C - Good	جيد	70 - 79	Sound work with notable errors
	D - Satisfactory	متوسط	60 - 69	Fair but with major shortcomings
	E - Sufficient	مقبول	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	**FX** – Fail	راسب (قيد المعالجة)	(45-49)	More work required but credit awarded
	F – Fail	راسب	(0-44)	Considerable amount of work required

Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.