Week 1	What is cryptography?, keys, symmetric & asymmetric cryptography, Hash vs MAC vs Digital signatures, security, SSL, cryptography attacks, Useful data types and conversions, XORing, rotating ciphers
Week 2	Common information security targets, definitions, security engineering and principles, access control, security issues, threat modelling, security policies and documents, hashing & collisions
Week 3	Access controls (identification, authorisation, authentication), password attacks, salting shadow passwords, biometrics, Types of access controls policies, AES-ECB, AES-CTR, padding
Week 4	OSI model, TCP/IP model, firewalls, ipv6, AH & ESP protocol, traffic engineering, MPLS, asymmetric cryptography, RSA, Diffie-hellman key exchange
Week 5	Operating system, security & threats, trusted platform module, trusted systems, trusted computing base, (processes, threads, memory leaks), technical attacks, Boolean Satisfiability (SAT) Problem, SAT solvers, Conjunctive Normal Form, C Bounded Model Checker (control flow simplification, loop unwinding, loop-free programs into equations, bit blasting, graph colouring problem
Week 6	Cyberattacks, threats & agents, quantitative and qualitative assessments, risk assessments, security controls, residual risk, incident management, Arithmetic Mean, Median, mode, IQ range, variance, sets (sub/super/empty), complements, Venn diagrams, de Morgan's law, events and axioms of probability, conditional probability, independence, Bayes theorem
Week 7	Threat assessment, time period, intelligence funnel, F3EAD, discrete and continuous random variables, Density and Distribution Function, variance,

standard deviation, expected values, independence of RV, joint CRV, poisson, Pareto, normal and log-normal, PERT (& modified PERT)

Week 8

Security and goods, the price of a good, price of information, business models, lock-in, information asymmetry, system reliability, software market, digital rights management (DRM), sampling (random, stratified, systematic, clustered, monto-carlo, linear programming, linear regression

Week 9

Federated learning, edge caching, security and challenges, robust-by-design, learning-based detection, similarity-based model aggression, (metrics for performance, system, security), CVSS, base metrics —> exploitability and impact metrics, environmental and temporal metrics, weighting average, ASM, attack surfaces