Syllabus of COMP 6712 (tentative)

For details: https://haiyangxc.github.io/hyxue/teaching/comp6712

Date	Topics\slides	Outline
Week 1: Jan 10	Course Overview	course plan, reading materials, grading, brief introduction to every topic
Week 2: Jan 17	Basic Cryptography 1: Symmetric cryptography	symmetric encryption, one-time pad, blockcipher, hash function, MAC, authenticated encryption.
Week 3: Jan 31	Basic Cryptography 2: Public key cryptography	RSA, Diffie-Hellman, public key encryption, Digital signature
Week 4: Feb 7	Network Security Principles	access control, password, authentication, PKI, and certification authorities
Week 5: Feb 14	Network Security in Practice	secure sockets layer (SSL), internet protocol security (IPSec), internet key exchange (IKE), virtual private network (VPN)
Week 6: Feb 21	Authentication	Access control, password authentication, biometric authentication
Week 7: Feb 28	Privacy-Enhancing technologies 1	post-quantum cryptography: encryption and signatures against quantum-empowered adversary; Fully-homomorphic encryption and applications
Week 8: Mar 7	Privacy-Enhancing technologies 2	commitment, zero-knowledge proofs
Week 9: Mar 14	Privacy-Enhancing technologies 3	secure multiparty computation
Week 10: Mar 21	Security and Privacy in Practice 1	security and privacy in Blockchain
Week 11: Mar 28	Security and Privacy in Practice 2	security and privacy for machine learning
Week 12: Apr 4	Final presentation 1	papers from S&P, CCS, USENIX, NDSS, CRYPTO, or EUROCRYPT
Week 13: Apr 11	Final presentation 2	papers from S&P, CCS, USENIX, NDSS, CRYPTO, or EUROCRYPT