Welcome to ICT2205/ICT2213 Applied Cryptography

Module Description:

- This module covers the fundamental cryptographic primitives that are deployed in secure systems today, including one-way hash functions, symmetric key cryptography, public key cryptography, and digital signatures. It also addresses common cryptographic failures and weak designs, and discusses practical deployment issues, such as key generation, distribution, and storage. In addition to the theoretical background, students will also implement several cryptographic protocols using well-known cryptographic libraries.

Learning Outcomes:

- Explain the main concepts and properties of hash functions, message authentication codes, symmetric key cryptography, public key cryptography, and digital signatures.
- Explain the core design concepts, key applications, and problems (common failures, weak designs and incorrect project approaches) of using cryptography, and correctly implement real world

solutions, such as in deployments of key generation, distribution and storage.
- Correctly apply cryptography to achieve confidentiality, integrity, and authenticity in real world applications; implement cryptographic protections in applications using open source cryptographic libraries.

Instructor:

- A/Prof Spiros Bakiras **spiridon.bakiras@singaporetech.edu.sg**

Assumed Knowledge:

- Python programming
- Basic algebra
- Discrete math

Topics Covered:

- Topic 1: Foundations, Classical Cryptography
  - Introduction to applied cryptography
  - Mono-alphabetic ciphers
  - Poly-alphabetic ciphers
- Topic 2: Symmetric Key Cryptography
  - AES cipher
  - Block cipher modes
- Topic 3: Public Key Cryptography
  - Number theory
  - RSA and ElGamal cryptosystems
  - Elliptic curve cryptography
- Topic 4: One-way Hash Functions
  - One-way hash functions

    - Message authentication codes
- Topic 5: Digital Signatures
    - RSA signatures
    - Elliptic curve digital signature algorithm (ECDSA)
- Topic 6: Key Management
    - Key distribution
    - Key storage
- Topic 7: Confidentiality, Integrity, Message Authentication
    - Using symmetric key cryptography correctly
    - Using public key cryptography correctly
- Topic 8: User Authentication
    - Password-based authentication
    - Password storage
    - Key-based authentication
- Topic 9: Authenticated Key Establishment
    - Authentication and key establishment
    - Perfect forward secrecy
    - A study of TLS
    - A study of WiFi security

Assessment Information:

	Assessment Mode	Weightage
1.	Weekly lab quizzes (Weeks 2, 3, 5, 9, 11)	5%
2.	Lab Quiz 1 + 2	30%
3.	CTF 1 + 2	40%
4.	Team project (with peer feedback multiplier)	25%

Schedule:

Week	Date	Lab
1	9 Jan	Lab 1 (foundations, classical cryptography)
2	16 Jan	Lab 2 (symmetric-key cryptography)
3	23 Jan	Lab 3 (public-key cryptography)
4	30 Jan	CNY
5	6 Feb	Lab 4 (hash functions, message authentication codes)
6	13 Feb	Lab 5 (digital signatures) Lab Quiz 1
7	20 Feb	Recess week
8	27 Feb	Lab CTF 1
9	6 Mar	Lab 6 (key management)
10	13 Mar	Lab 7 (confidentiality, integrity, message authentication) Project demo
11	20 Mar	Lab 8 (user authentication)
12	27 Mar	Lab 9 (authenticated key establishment) Lab Quiz 2
13	3 Apr	Lab CTF 2