Basic Cryptography

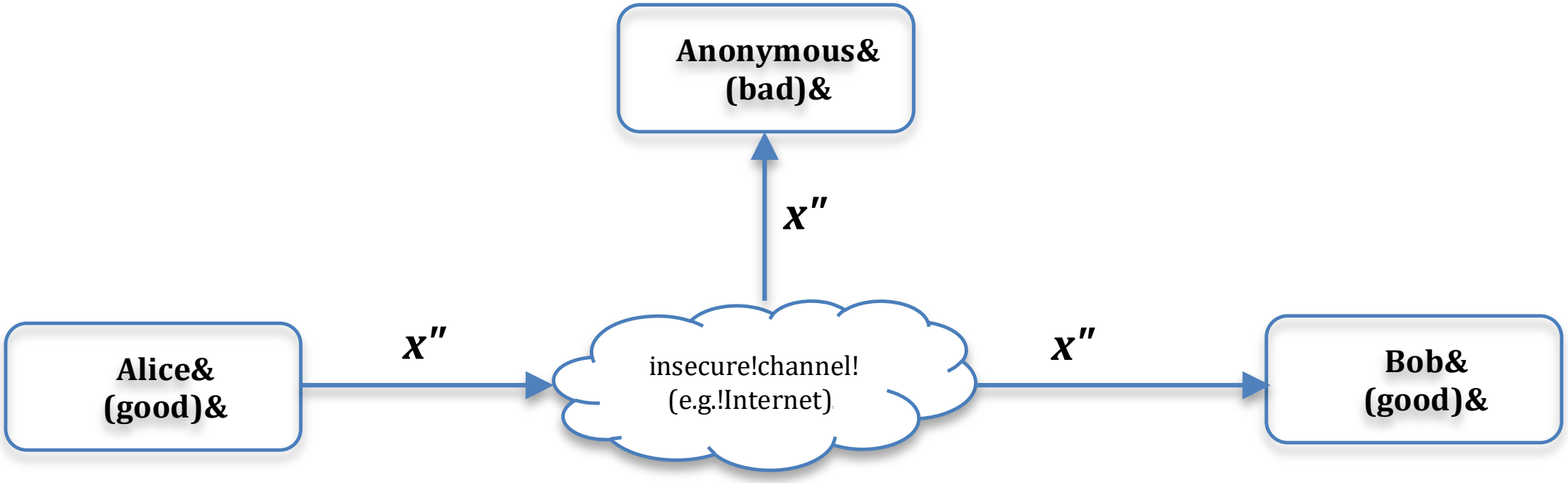
DAT159

Tosin Daniel Oyetoyan

Asset

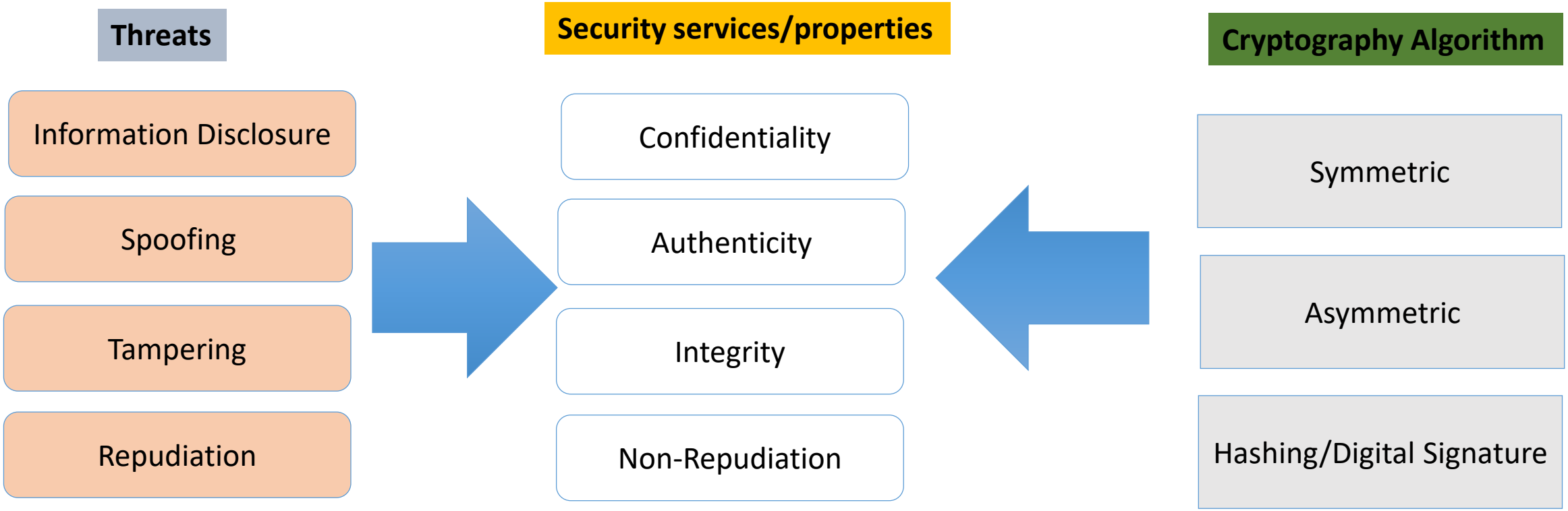
- Something of value
  - To be protected/maintain secrecy
    - Critical information (e.g. Military/Government communications)
    - Patient information
    - Credit card
    - Online transactions
    - …
- Transit, at rest, in use
  - Stored in database, transferred during transactions, under processing (calculations)

Confidentiality



Communication over an insecure channel

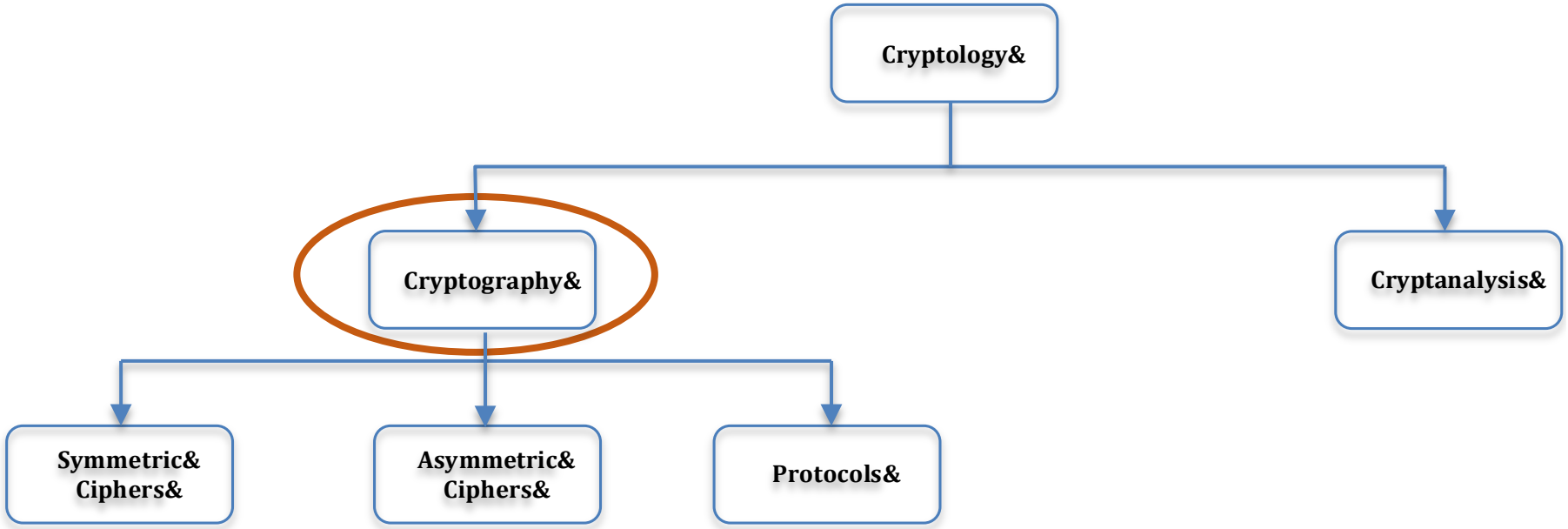
Overview


Threats
Information Disclosure
Spoofing
Tampering
Repudiation
Security services/properties
Confidentiality
Authenticity
Integrity
Non-Repudiation
Cryptography Algorithm
Symmetric
Asymmetric
Hashing/Digital Signature

Algorithms

Symmetric Algorithms (Private/Shared secret)	• RC4 • AES • DES • 3DES • BlowFish
Asymmetric Algorithms (Private/Public)	• RSA • Diffie-Hellman • ECC • El Gamal
Hashing/Digital Signature Algorithms (Message Digest, Fingerprint)	•MD4, MD5 •SHA-Family •RIPEMD- •MAC (Hash + Symmetric encryption) •DSA (Hash + Asymmetric encryption) •ECDSA (Hash + Asymmetric encryption) •Merkle Signature scheme •Schnorr/zero knowledge proofs

Overview of Crypt(-ology, -ography, -analysis)



- Cryptography: The science of and art of designing ciphers
- Cryptanalysis: The science and art of breaking ciphers
- Cryptology: The study of Cryptography and Cryptanalysis

Course Overview

- Classical cryptography
- Symmetric vs. Asymmetric cryptography
- Public Key Infrastructure (PKI)
- Cryptography in Blockchain Technology
- 2 Laboratories

Lab1 – Implementing Crypto algorithms

- We shall use:
  - A Client/Server Java application
- Main task:
  - Implement symmetric and asymmetric key algorithms

Lab2 – Intercepting & decrypting client/server messages

- We shall use
  - Wireshark and additional online resources