Cryptography & Network Security
Introduction

Chester Rebeiro

IIT Madras

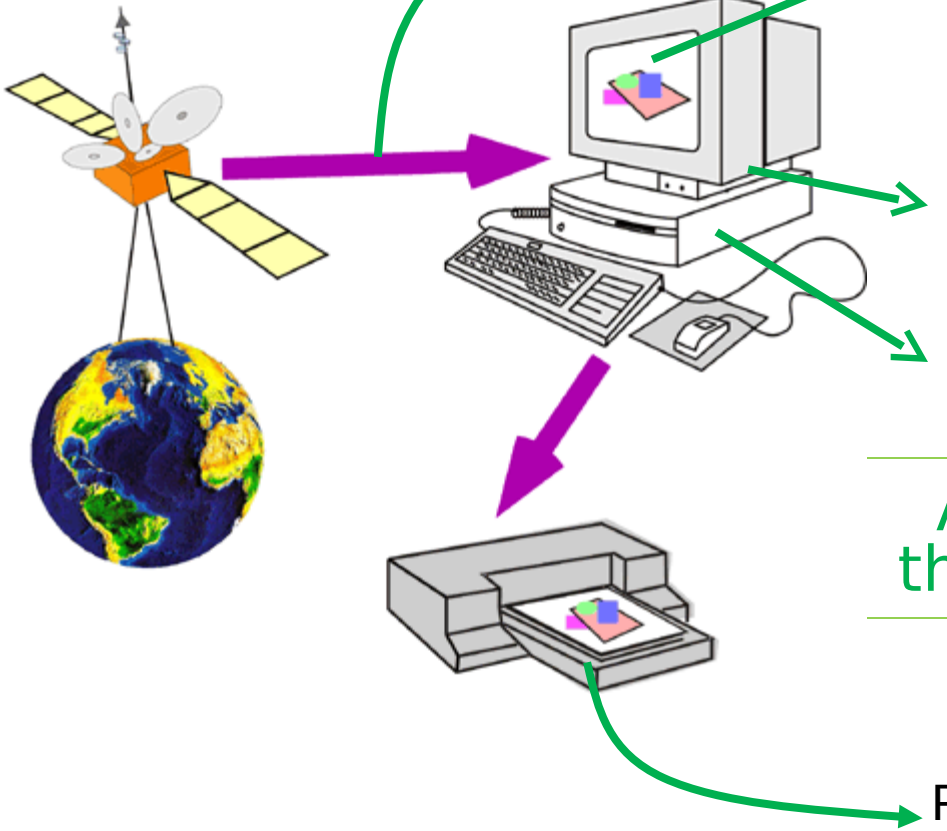
The Connected World

Increased Security Breaches

81% more in 2015

http://www.pwc.co.uk/assets/pdf/2015-isbs-executive-

Security Threats (why difficult to prevent?)



Networks / Communication links

Hardware

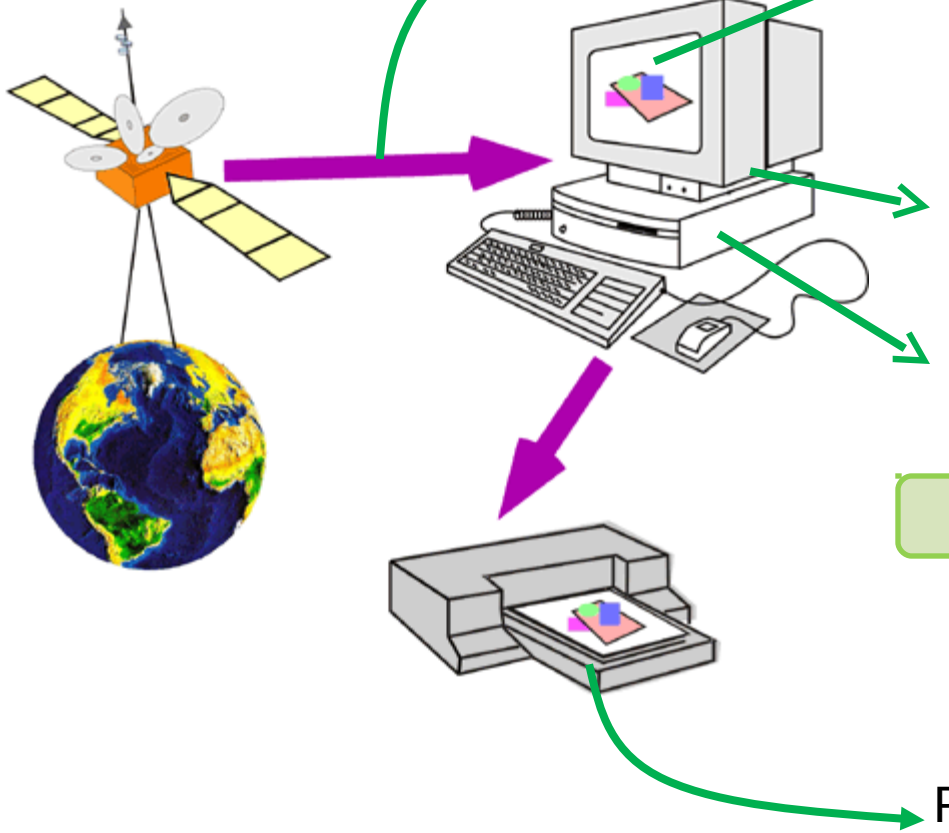
System Software
(Operating Systems / Hypervisor)

Applications

Attackers need to target the weakest link in the chain

Peripherals

Security Studies (Research) (an ocean)



Networks / Communication links

Network Security

Hardware

Hardware Security

System Softw

System Security

(Operating Systems / Hypervisor)

OS Security

Applications

Cloud Security

Web Security

Cryptography

DBMS Security

Peripheral

Embedded Security

Cryptography

- A crucial component in all security systems
- Fundamental compor ve
  - **Confidentiality**

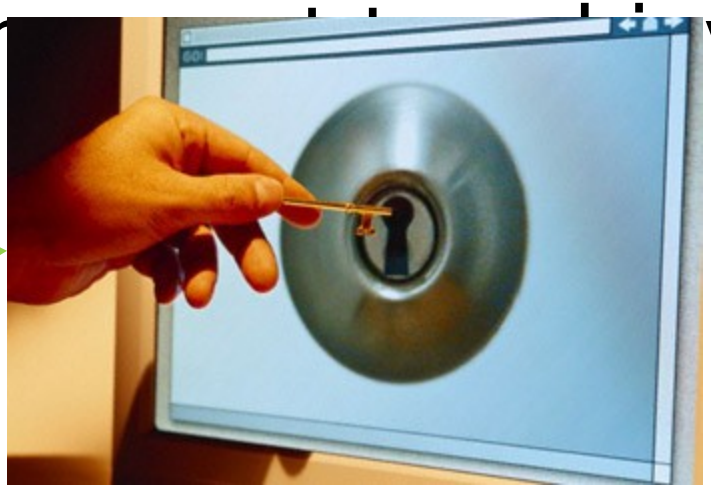
Allows only authorized users access t

Cryptography (its use)

- A crucial component in all security systems
- Fundamental component to achieve
  - Confidentiality
  - **Data Integrity**
    - Cryptography can be used to ensure that only authorized users can make modifications (for instance to a bank account number)

Cryptography (its use)

- A crucial component in all security systems
- Fundamental com ve
  - Confidentiality
  - Data Integrity
  - **Authentication**



Cryptography helps prove identities

Cryptography (its use)

- A crucial component in all security systems
- Fundamental compo[illegible]chieve
  - Confidentiality
  - Data Integrity
  - Authentication
  - **Non-repudiation**

The sender of a message cannot claim that she did not send it

Scheme for Confidentiality

Alice

Bob

untrusted communication link

message
Attack at Dawn!!

Mallory

Problem : Alice wants to send a message to Bob (and only to Bob) through an untrusted communication link

Encryption

Alice

message
"Attack at Dawn!!"

K_E

E

encryption

untrusted
communication link

#*%AR3X!34^$
(ciphertext)

K_D

D

decryption

Bob

"Attack at Dawn!"

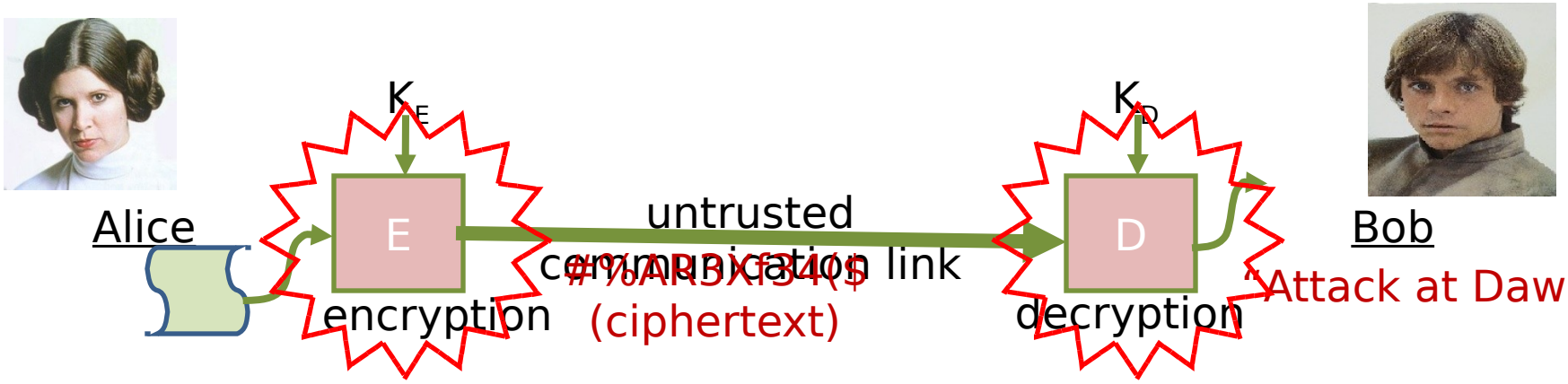
Secrets

- Only Alice knows the encryption key K_E
- Only Bob knows the decryption key K_D

Mallory

Only sees ciphertext.
cannot get the plaintext message
because she does not know the keys

Encryption Algorithms



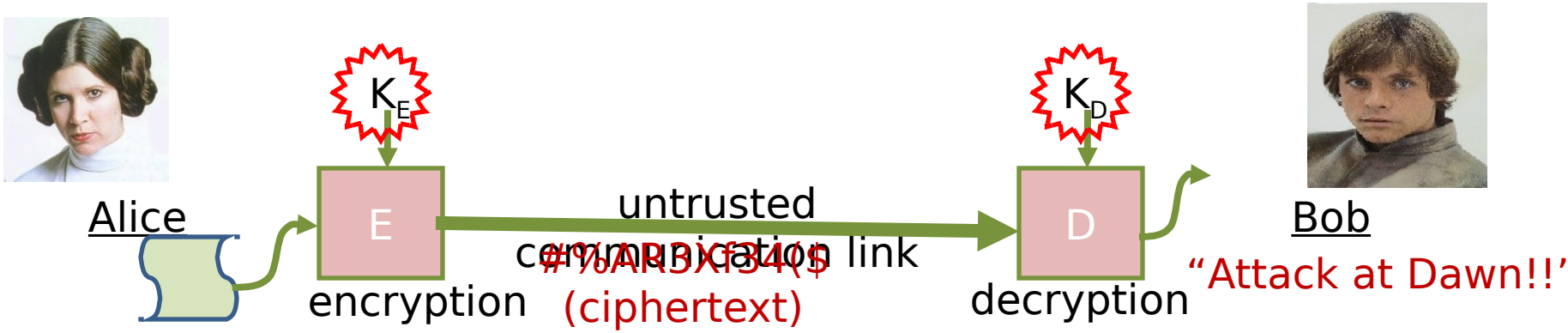
- Should be **easy to compute** for Alice / Bob (who **know the key**)
- Should be **difficult to compute** for Mallory (who **does not know the key**)
- What is **'difficult'**?
  - **Ideal case :** Prove that the probability of Mallory determining the encryption / decryption key is ***no better than a random guess***
  - **Computationally :** Show that it is ***difficult*** for Mallory to determine the keys even if she has massive computational

Algorithmic Attacks

- Can Mallory use tricks to break the algorithm

- There by reducing the ‘difficulty’ of getting the key.

Encryption Keys



- How are keys managed
  - How does Alice & Bob select the keys?
  - Need algorithms for key exchange

Ciphers

- Symmetric Algorithms
  - Encryption and Decryption use the same key
  - i.e. $K_E = K_D$
  - Examples:
    - Block Ciphers : DES, AES, PRESENT, etc.
    - Stream Ciphers : A5, Grain, etc.
- Asymmetric Algorithms
  - Encryption and Decryption keys are different
  - $K_E \neq K_D$
  - Examples:
    - RSA
    - ECC

Cipher Implementations

Cryptography is always an overhead !!

- For security, the algorithms need to be computation intensive.
  - Often require large numbers, complex mathematical operations.
- Design Challenges: Performance, Size, Power.
  - Algorithms to achieve this

Encryption Devices

Side Channels
Eg. Power consumption / radiation of device, execution time, etc.

Mallory
Gets information about the keys by mo
Side channels of the device

Side Channel Analysis

Alice

00111

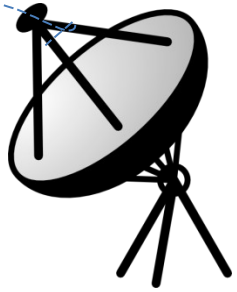
E

encryption

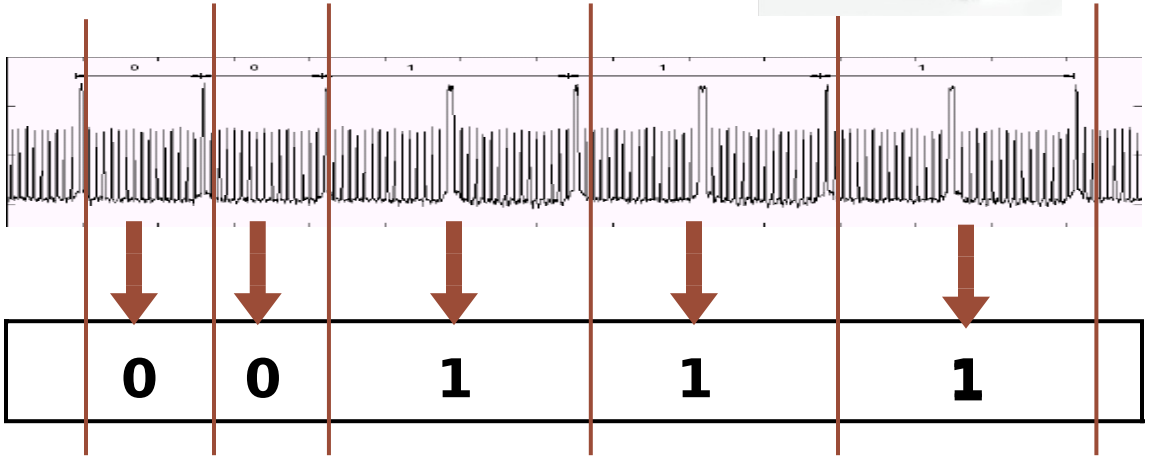
message

"Attack at Dawn!!"

electro-magnetic radiation



Radiation from Device



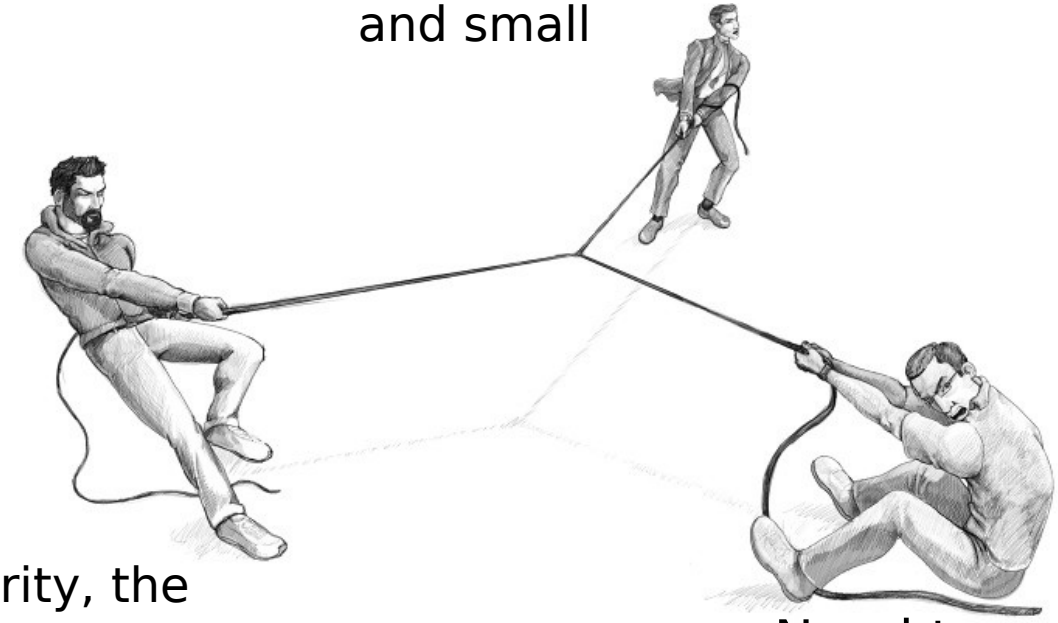
Secret information

0	0	1	1	1

Ciphers Design Challenges

Tradeoffs between Security , Speed, Side-Channel Attack

We want crypto algorithms to be fast and small

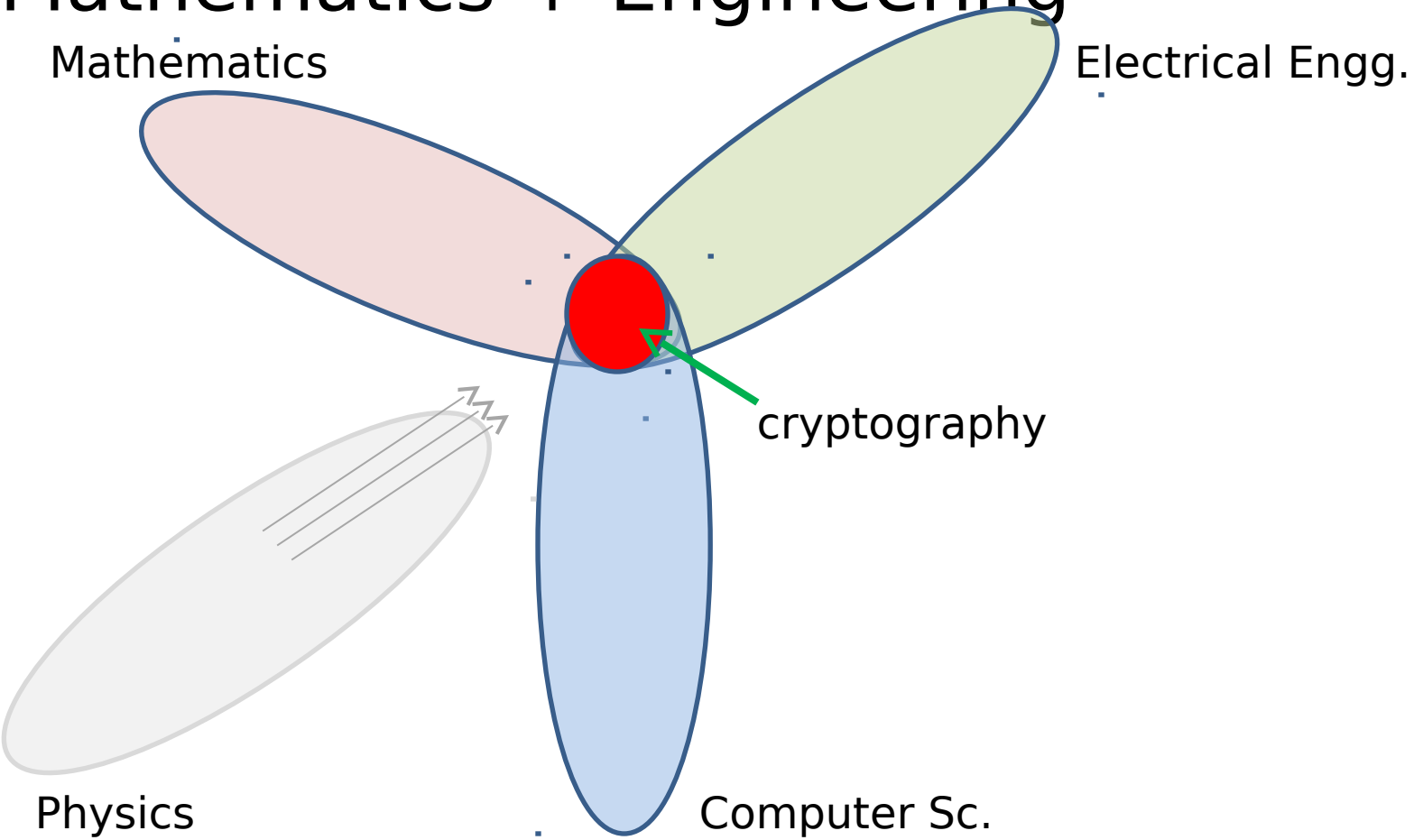


For security, the algorithms are computationally intensive. Typically use large numbers, complex operations

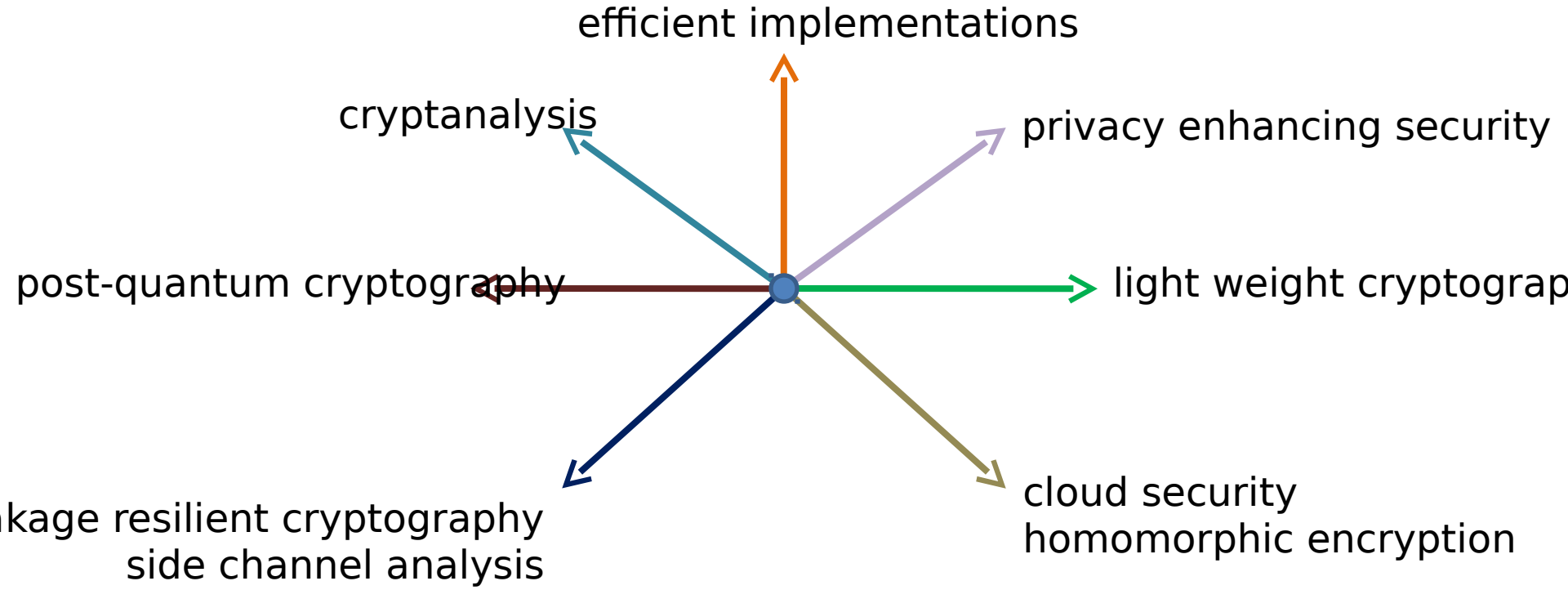
Need to protect against side channel attacks.

Cryptography Study

- Mathematics + Engineering



Some Hot Research Trends

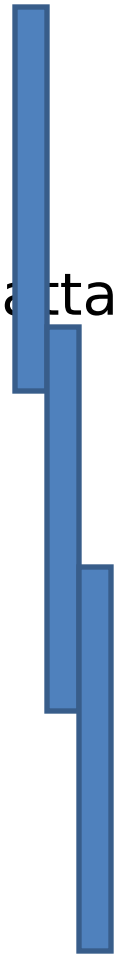


The Plan Ahead

- **How are ciphers designed?**
  - Ideal security vs Computational security
  - Block ciphers / Stream ciphers
  - Asymmetric key ciphers
  - Trade offs between security and implementation
- **Attacks**
  - Algorithmic / Side Channel Analysis
- **Applications**
  - How are they used to achieve confidentiality, integrity, authentication, non-repudiation
- **Case Studies**
  - Network security aspects, Bitcoins

Course Structure

- Classical Cryptography
- Shannon's Theory
- Block Ciphers
  - DES, AES, their implementations and their attacks
- Stream Ciphers
- Digital Signatures and Authentication
  - Hash functions
- Public key ciphers
  - RSA, implementations, and attacks
- Side channel analysis
- Network Security aspects
- Case Studies : Bitcoins



Expected Learning Outcomes

- What you would learn by the end of the course
  - Distinguish between cipher algorithms
    - Where to use what algorithm?
  - Evaluate ciphers and their implementations for security
    - Mathematical cryptanalysis of some algorithms
    - Side channel based attacks on cipher implementations
  - Apply algorithms to solve security problems in networks and real-world systems

Books / References

Textbooks

(STINSON) "Cryptography: Theory and Practice", Third Edition, by Douglas R. Stinson, CRC Press, Taylor and Francis Group

References

(STALLINGS) "Cryptography and Network Security: Principles and Practices", Sixth Edition, by William Stallings

(HANDBOOK) "Handbook of Applied Cryptography", Fifth Printing, by Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, CRC Press

(HARDSEC) "Hardware Security : Design, Threats, and Safeguards", by Debdeep Mukhopadhyay and Rajat Subhra Chakraborty, CRC Press, Taylor and Francis Group

Grading

- Quiz 1 : 20%
- Quiz 2 : 20%
- End semester : 40%
- Assignments : 20%
  - Surprise tests / Tutorials / Programming assignments / minute papers / etc.

Self Study vs Attending Classes

- Same tutorials / assignments / quizzes / etc.
- Grading policy is different

Course Webpages

- For PPTs etc.

  http://www.cse.iitm.ac.in/~chester/courses/16e_cns/index.html

- For discussions / announcements / submissions

  CSE Moodle

  Google Groups (cnsiitm_2016)

Logistics

- Room CS26
- Time:
  - ~~Tuesdays : 11:00 - 11:~~50 AM
  - Wednesdays : 10:00 - 10:50 AM
  - Thursdays : 8:00 - 8:50 AM
  - Fridays : 2:00 – **3:45 PM?**