An Introduction to Applied Cryptography

Chester Rebeiro

IIT Madras

CR

Cryptography

- A crucial component in all security systems
- Fundamental component to achieve
  - **Confidentiality**

Allows only authorized users access to data

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)

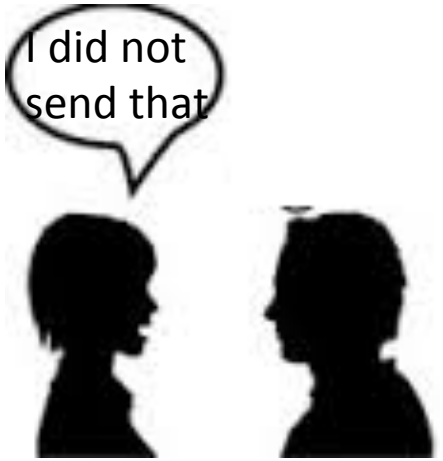
Cryptography (its use)

- A crucial component in all security systems
- Fundamental component to achieve
  - Confidentiality
  - Data Integrity
  - **Authentication**

Cryptography helps prove identities

Cryptography (its use)

- A crucial component in all security systems
- Fundamental component to achieve
  - Confidentiality
  - Data Integrity
  - Authentication
  - **Non-repudiation**



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

Scheme for Confidentiality

Alice

message

Attack at Dawn!!

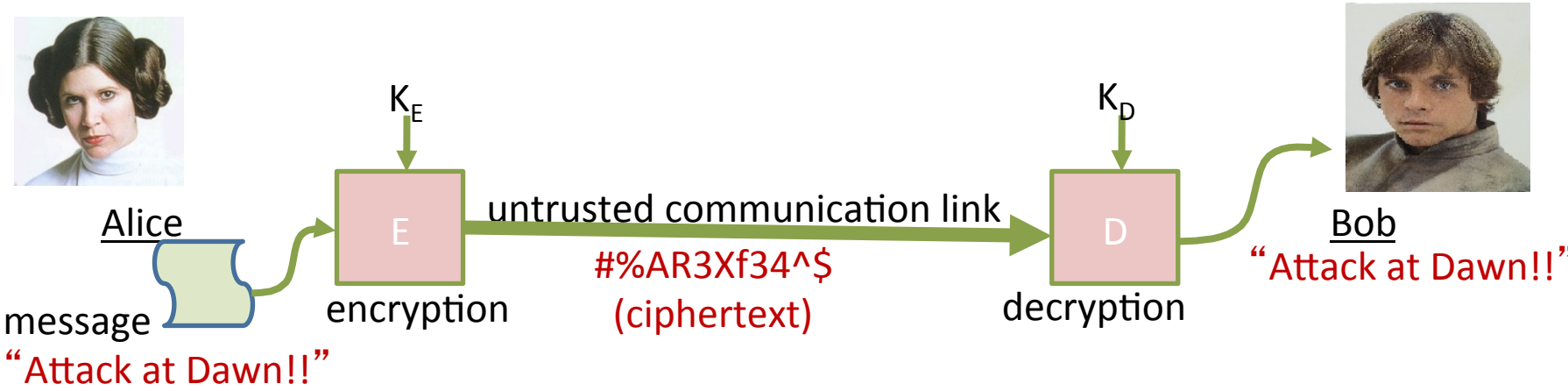
untrusted communication link

Bob

Mallory

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

Encryption



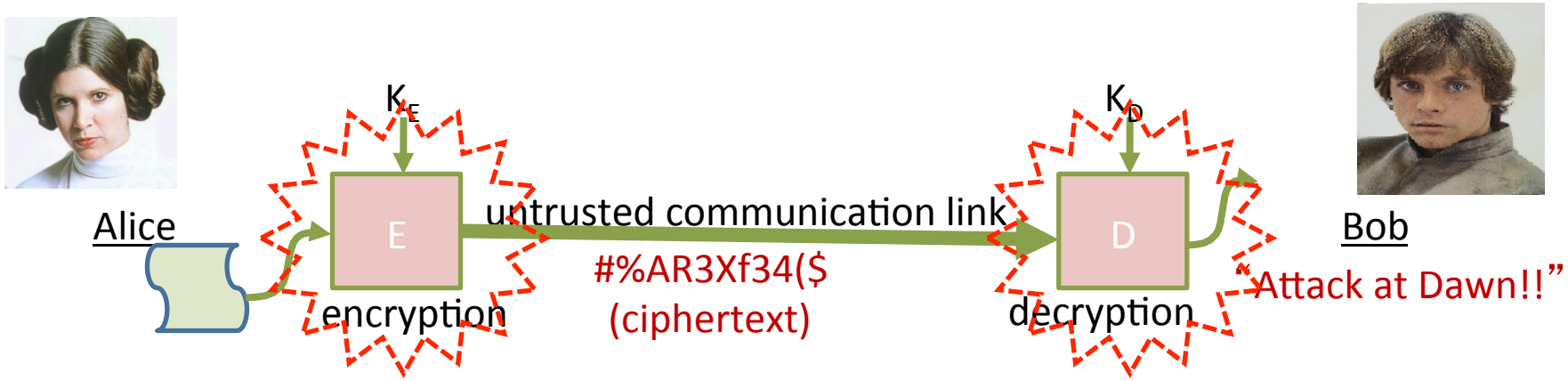
Secrets

- 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



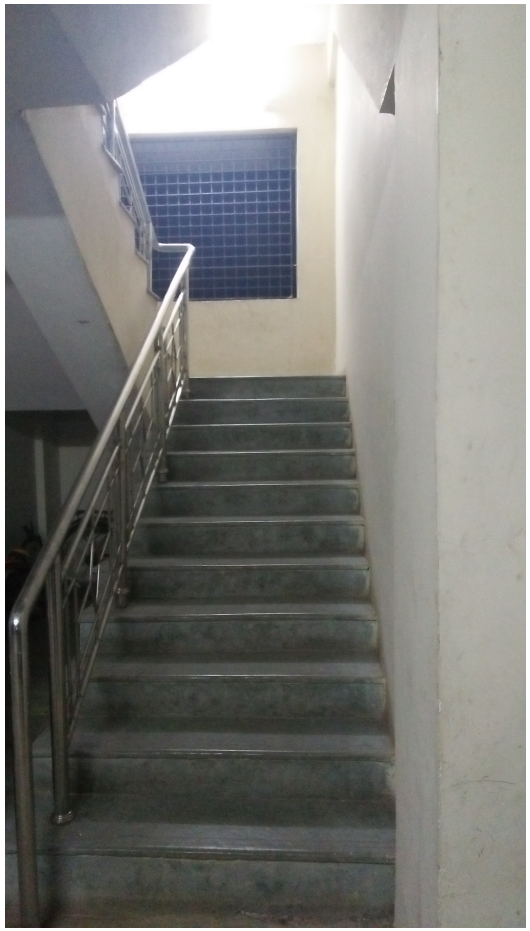
- Should be **easy to compute** for Alice / Bob (who **know the key**)
- Should be **difficult to compute** for Mallory (who **does not know the key**)
- What is '**difficult**'?
  - **Ideal case :** Prove that the probability of Mallory determining the encryption / decryption key is ***no better than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

Algorithmic Attacks

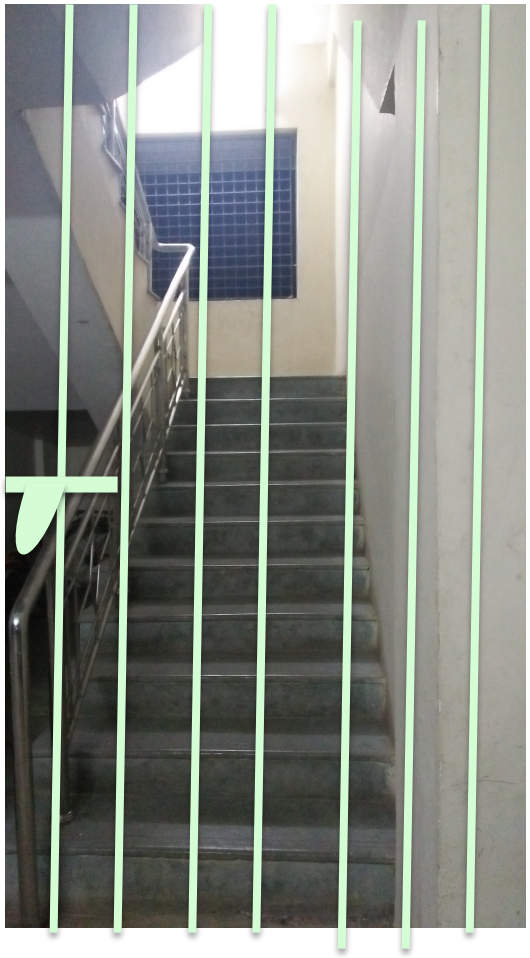
- Can Mallory use tricks to break the algorithm

- There by reducing the `difficulty' of getting the key.
- Modern crypto-systems are considerably robust against algorithmic attacks

Theory vs Practice



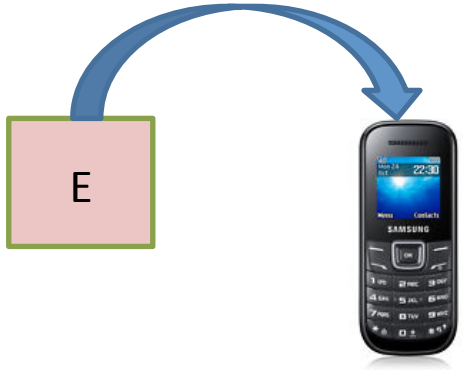
In theory



In practice

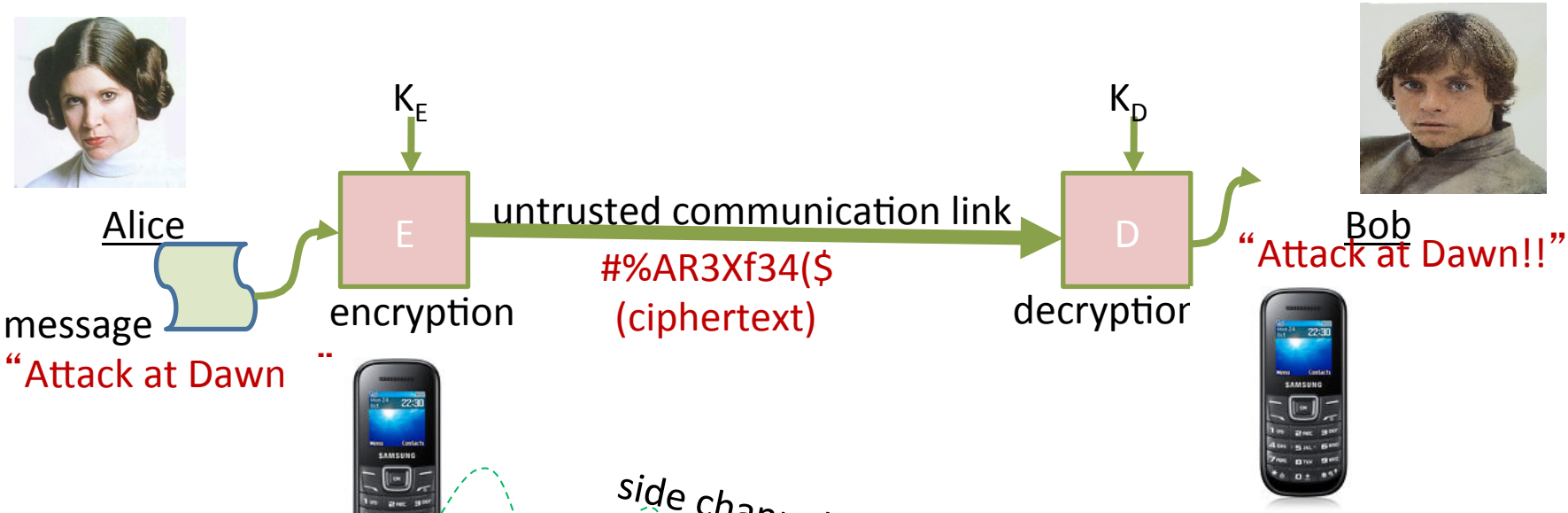
Cipher Implementations

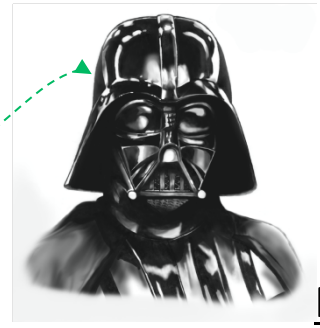
Cryptography is always an overhead !!



- 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

Implementation Attacks
(Side Channel Analysis)



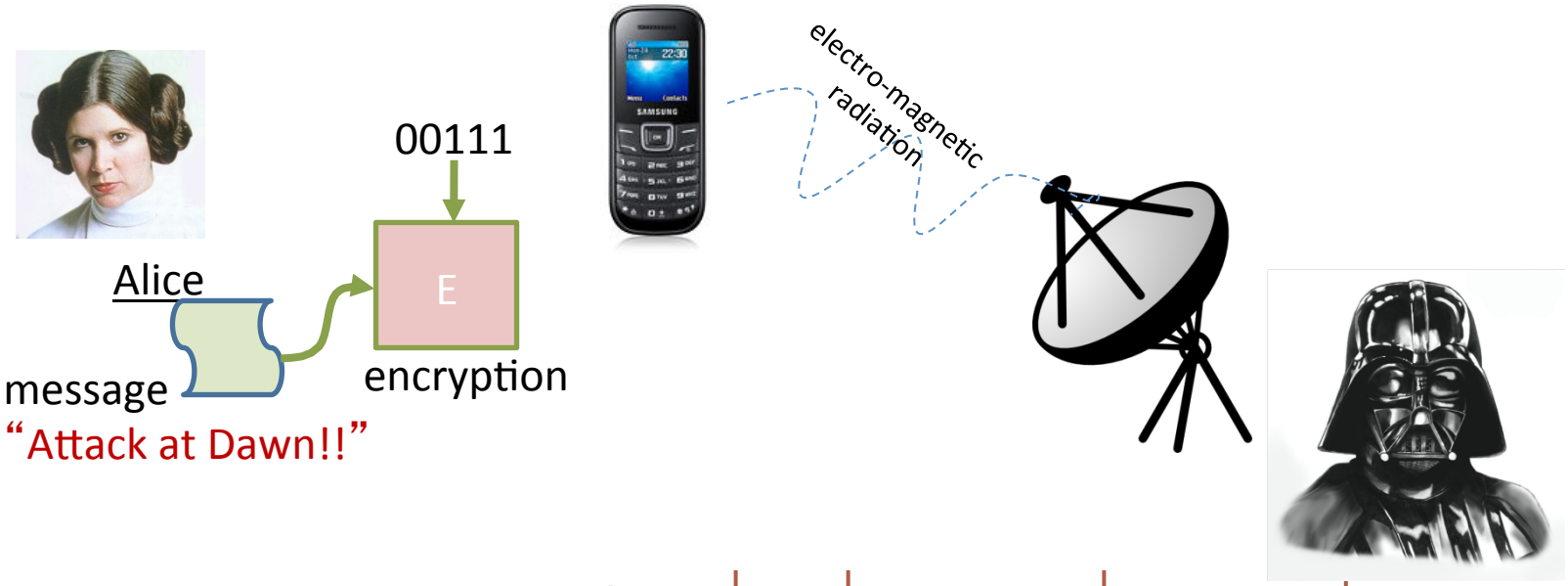


Mallory

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

Gets information about the keys by monitoring Side channels of the device

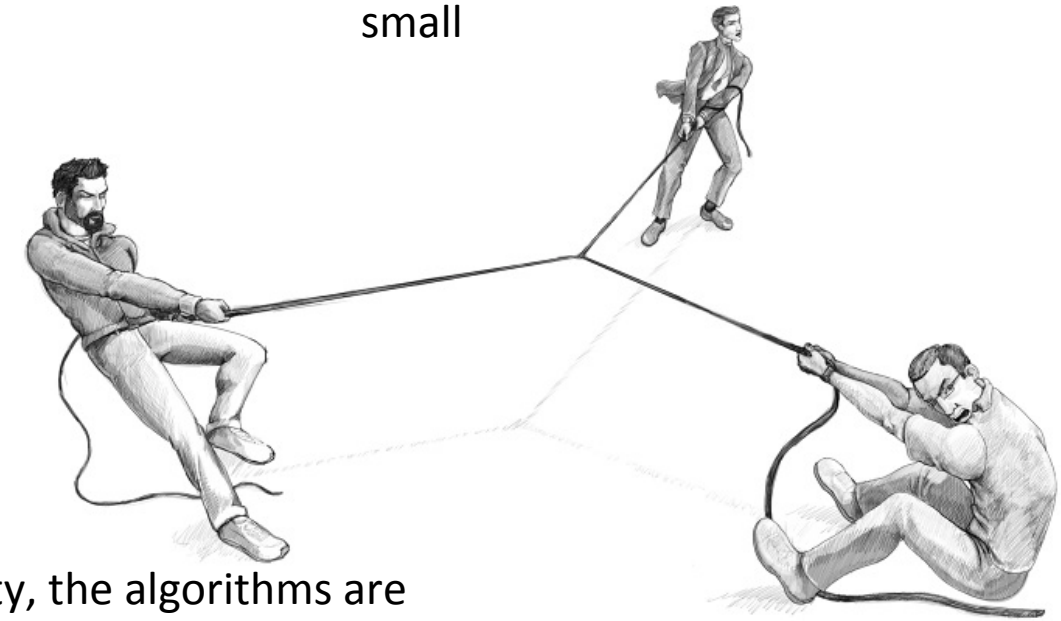
Side Channel Analysis



Ciphers Design Challenges

Tradeoffs between Security , Speed, Side-Channel Attacks

We want crypto algorithms to be fast and small

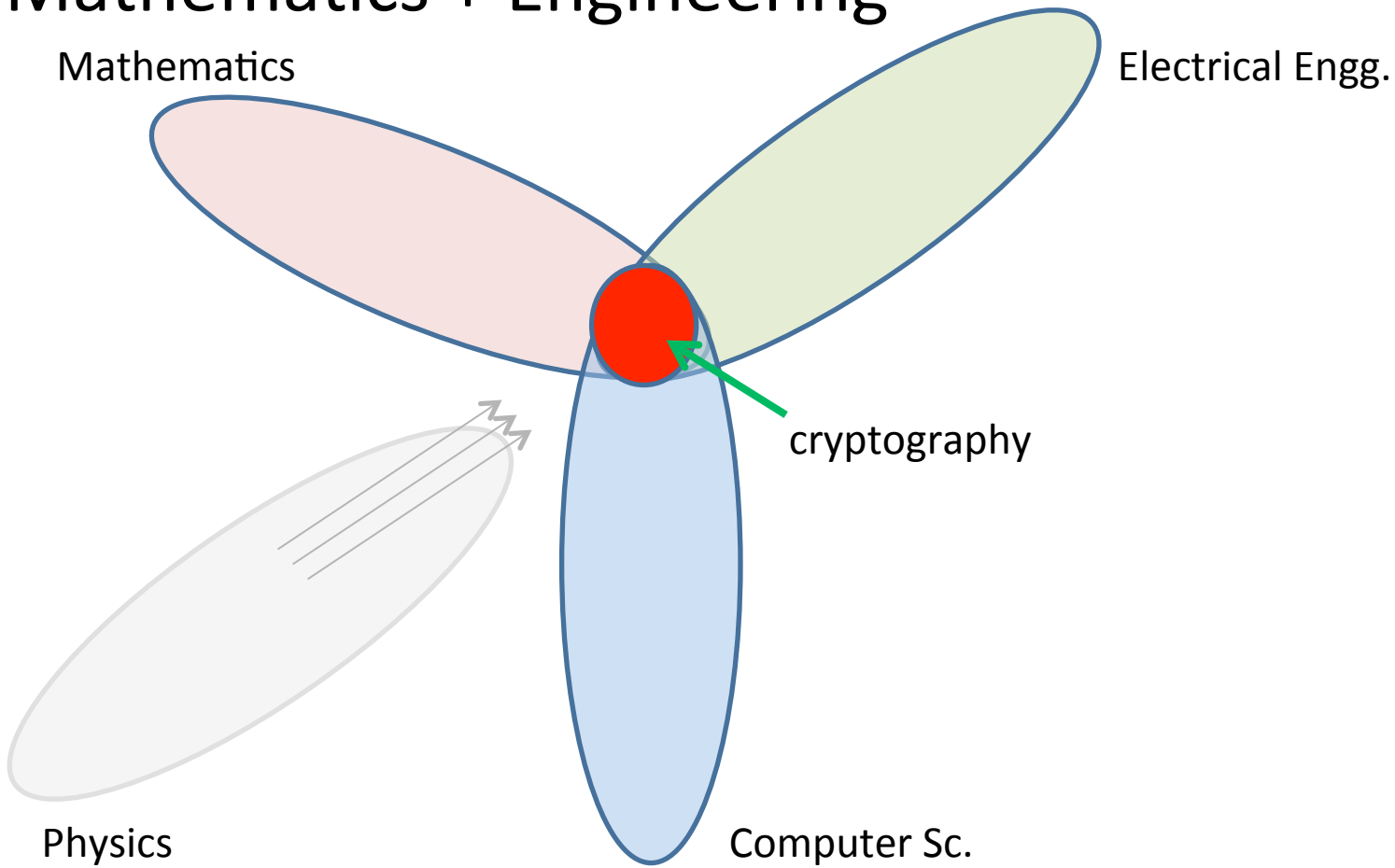


For security, the algorithms are computationally intensive. Typically use large numbers, complex operations

Need to protect against side channel attacks.

Cryptography Study

- Mathematics + Engineering



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 / Implementation based Attacks
- **Applications**
  - How are they used to achieve confidentiality, integrity, authentication, non-repudiation
- **Case Studies**
  - Key Establishments, Digital Signatures, Bitcoins

Course Structure

- Classical Cryptography
- Shannon's Theory
- Block Ciphers
  - DES, AES, their implementations and their attacks
- Digital Signatures and Authentication
  - Hash functions
- Public key ciphers
  - RSA, implementations, and attacks
  - PQC
- Side channel analysis
- 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 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

Grading

- Quiz 1 : 20%
- Quiz 2 : 20%
- End semester : 20%
- Assignments : 20%
- Tutorials : 20%

Syllabus for Quiz 1 , Quiz 2, and End Semester will be (almost) exclusive!

Course Webpages

- For slides / syllabus / schedule etc.

  http://www.cse.iitm.ac.in/~chester/courses/18e_ac/index.html

- For discussions / announcements / submissions

  CSE Moodle

  Google Groups (aciitm_2018)

Logistics

- Location : CS26
- Slot : F

Tuesday's afternoon slot will be used for tutorials occassionally