An Introduction to Applied Cryptography

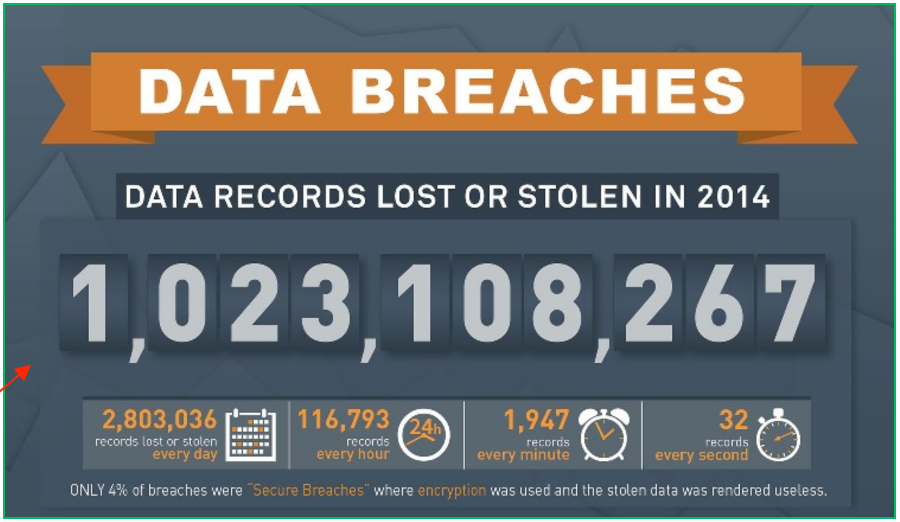
Chester Rebeiro
IIT Madras

Connected and Stored

Everything is connected!

Everything is stored!

Increased Security Breaches



DATA BREACHES

DATA RECORDS LOST OR STOLEN IN 2014

1,023,108,267

2,803,036 records lost or stolen every day

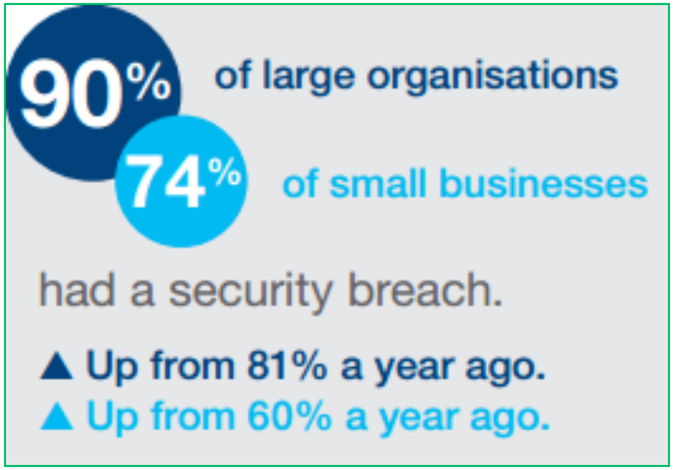
116,793 records every hour

1,947 records every minute

32 records every second

ONLY 4% of breaches were "Secure Breaches" where encryption was used and the stolen data was rendered useless.

81% more in 2015



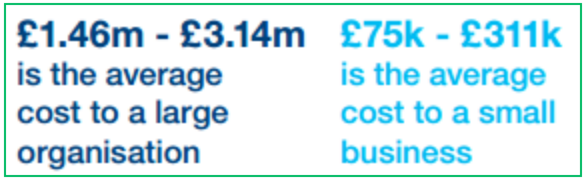
90% of large organisations

74% of small businesses

had a security breach.

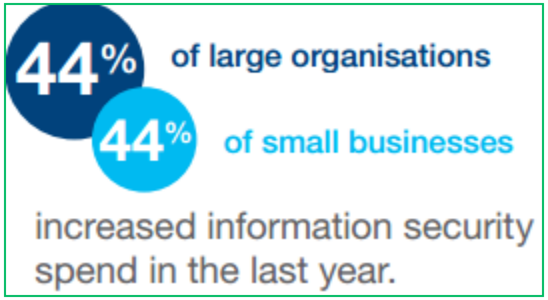
▲ Up from 81% a year ago.

▲ Up from 60% a year ago.



£1.46m - £3.14m is the average cost to a large organisation

£75k - £311k is the average cost to a small business



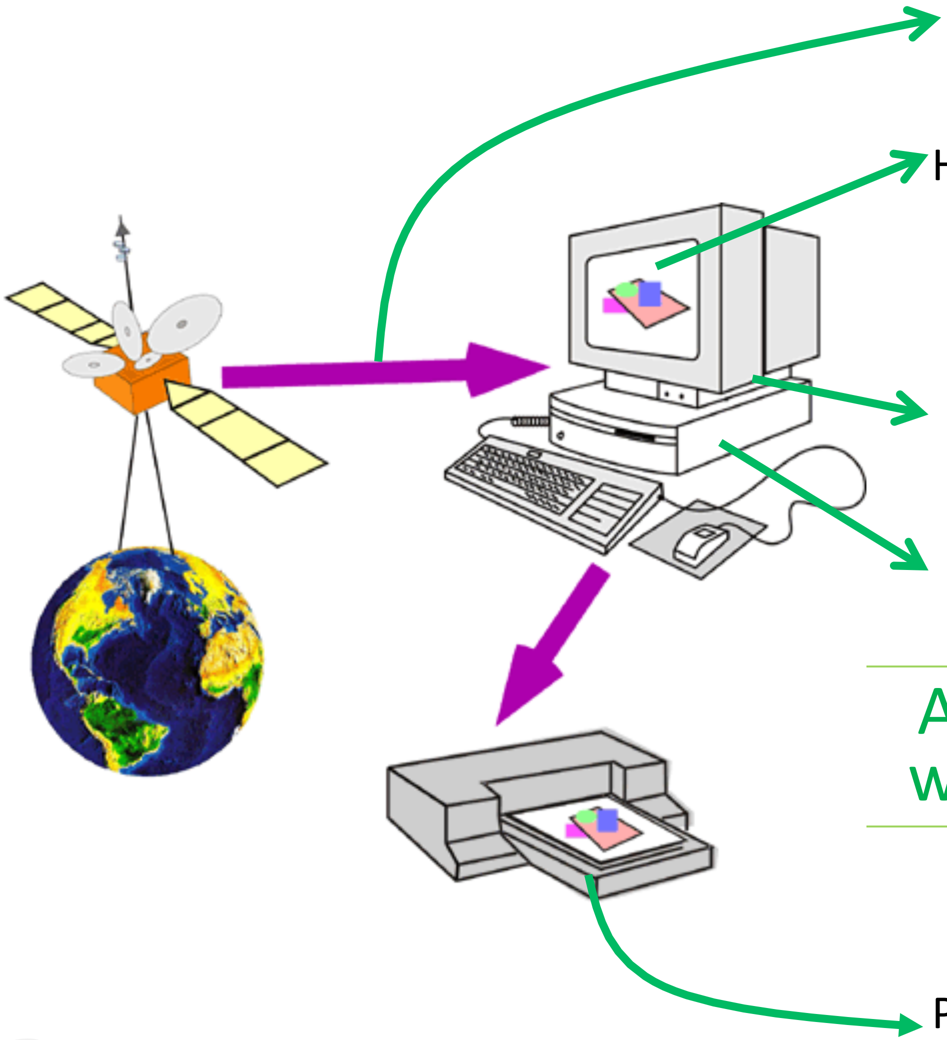
44% of large organisations

44% of small businesses

increased information security spend in the last year.

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

Security Threats
(why difficult to prevent?)



Networks / Communication links

Hardware

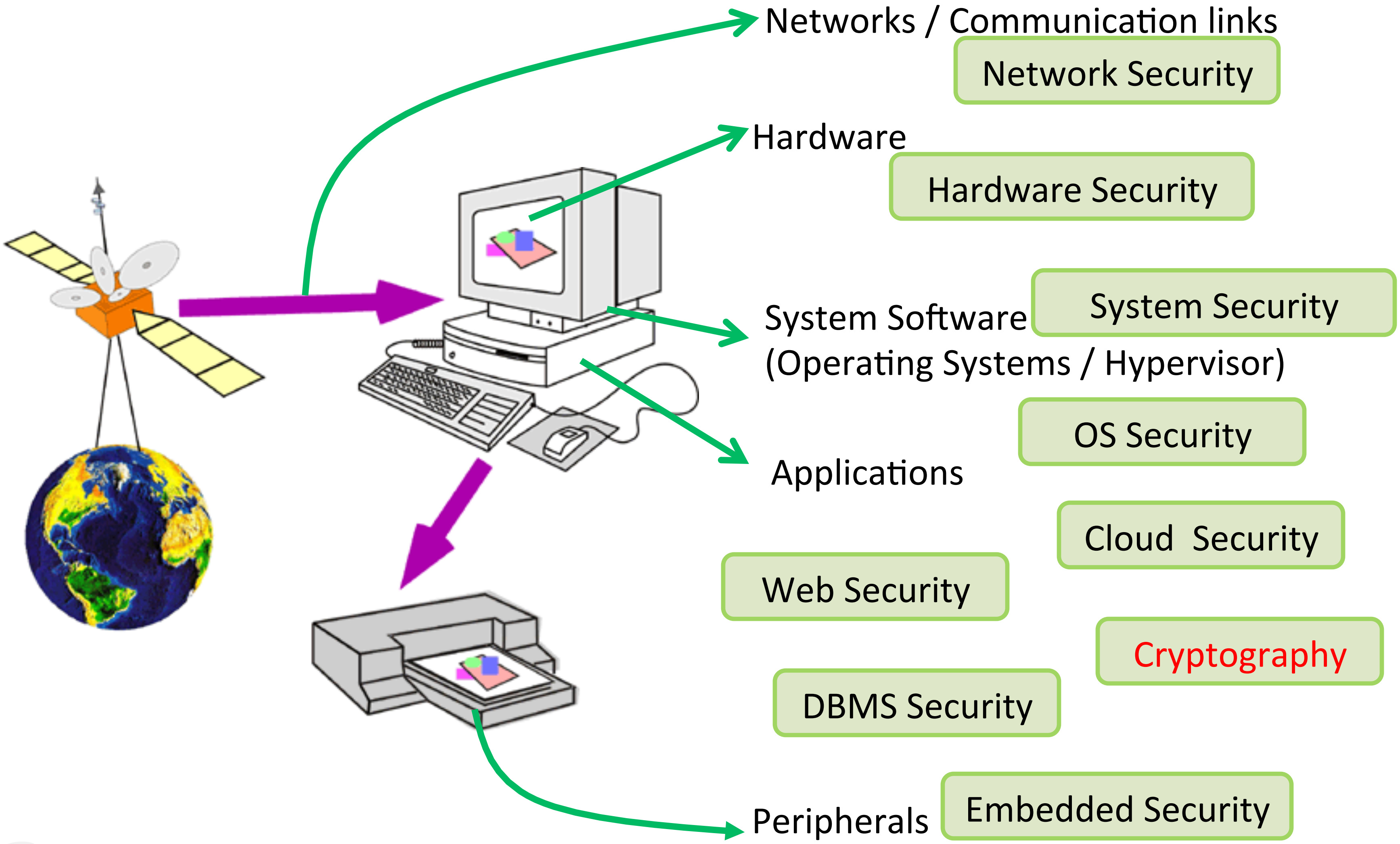
System Software
(Operating Systems / Hypervisor)

Applications

Peripherals

Attackers need to target the weakest link in the chain

Security Studies (Research)



Networks / Communication links

Network Security

Hardware

Hardware Security

System Software
(Operating Systems / Hypervisor)

System Security

OS Security

Applications

Cloud Security

Web Security

Cryptography

DBMS Security

Peripherals

Embedded Security

Cryptography

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

Allows only authorized users access to data

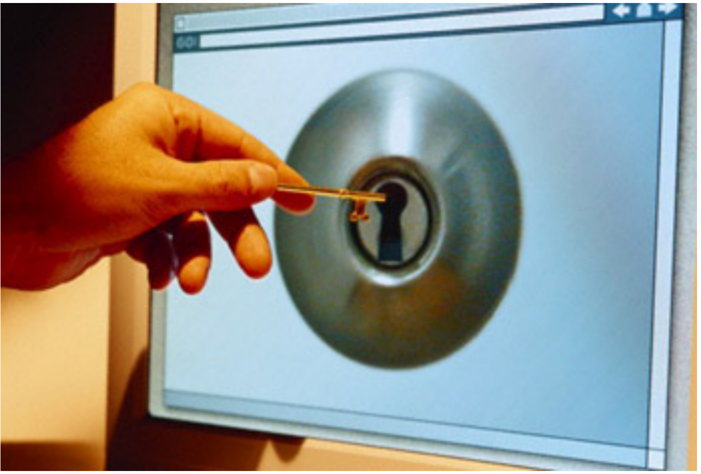
Cryptography (its use)

- 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)

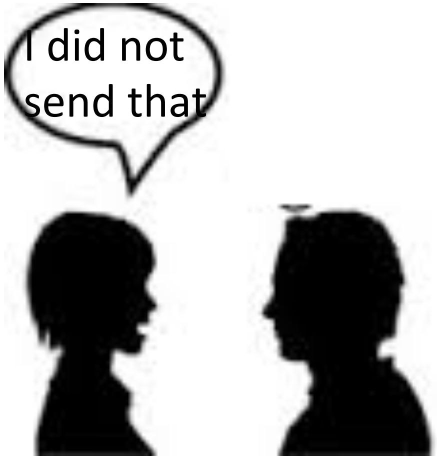
- A crucial component in all security systems
- Fundamental component to achieve
  - Confidentiality
  - Data Integrity
  - **Authentication**



Cryptography helps prove identities

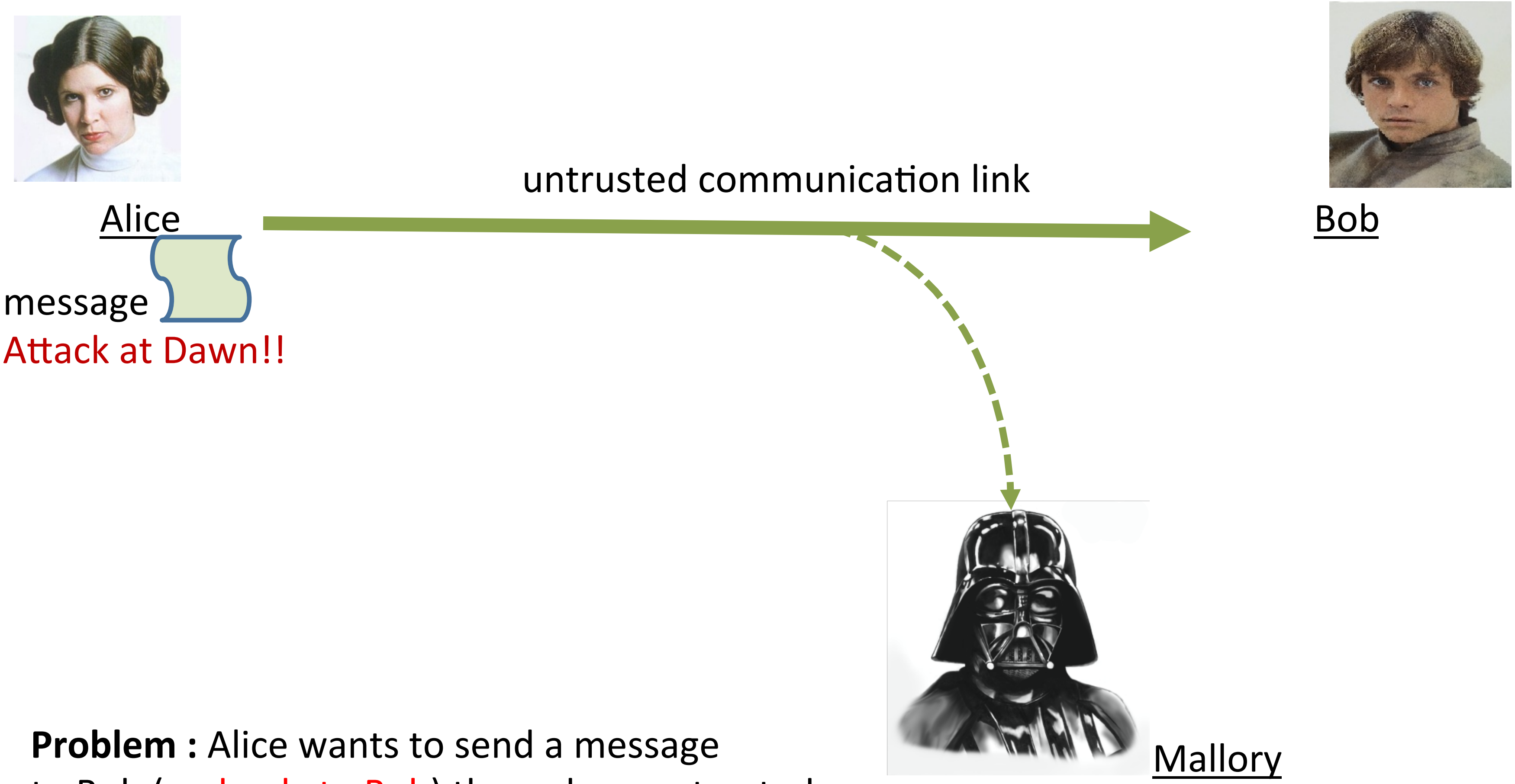
Cryptography (its use)

- 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



untrusted communication link

Alice

Bob

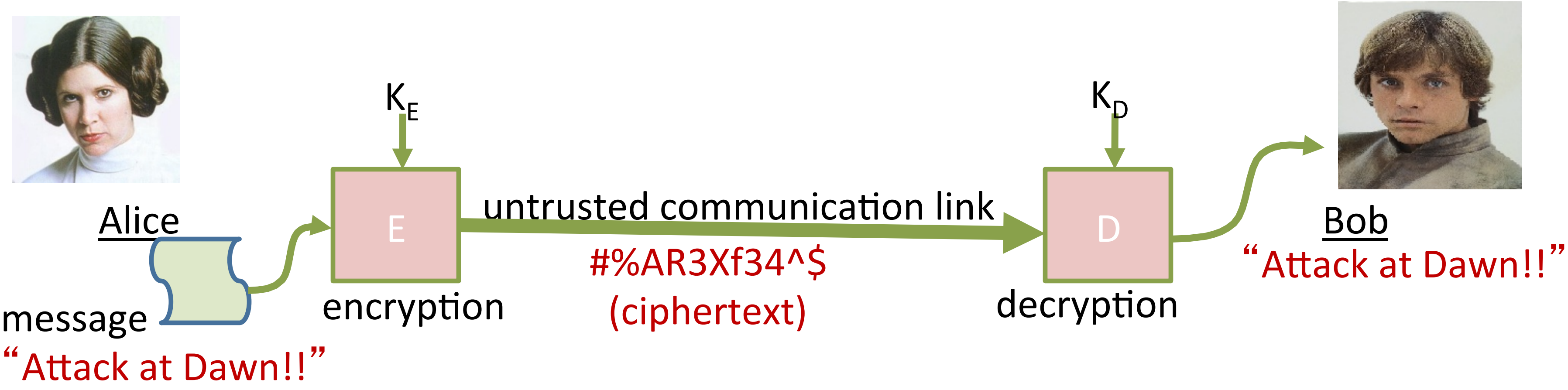
message

Attack at Dawn!!

Mallory

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

Encryption



K_E

K_D

Alice

E

untrusted communication link

D

Bob

"Attack at Dawn!!"

message

"Attack at Dawn!!"

encryption

#%AR3Xf34^$
(ciphertext)

decryption

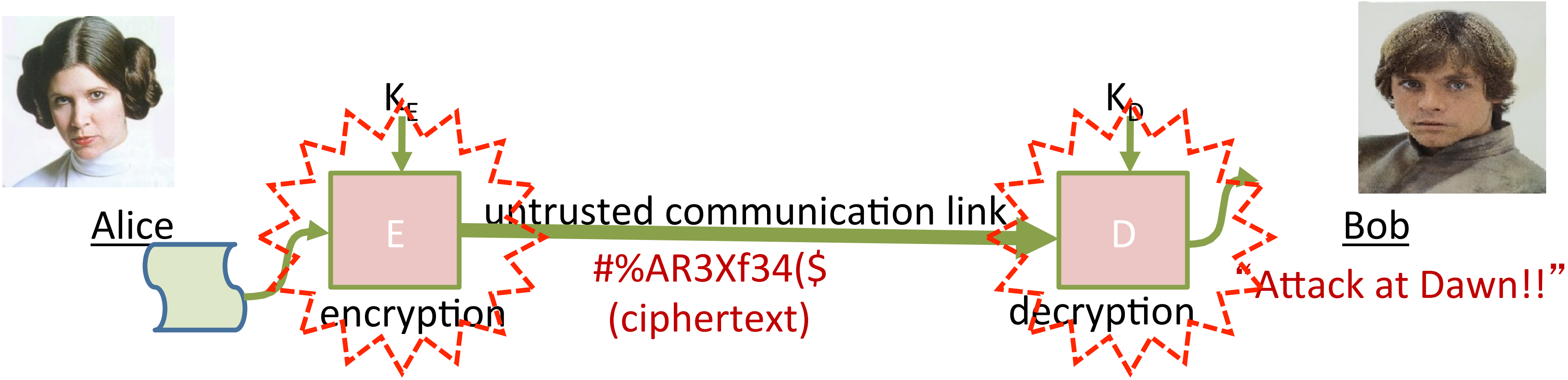
Mallory

Secrets

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

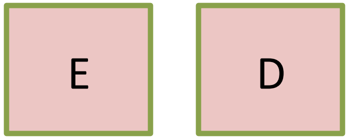
Only sees ciphertext.
cannot get the plaintext message
because she does not know the keys

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

Ciphers

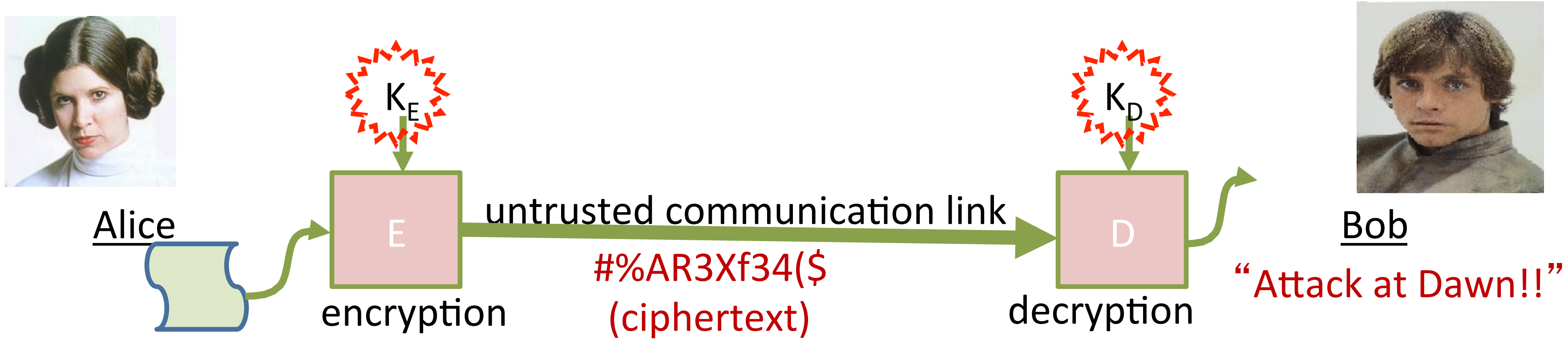


E

D

- 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

Encryption Keys



Alice

K_E

E

encryption

untrusted communication link

#%AR3Xf34($

(ciphertext)

K_D

D

decryption

Bob

"Attack at Dawn!!"

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

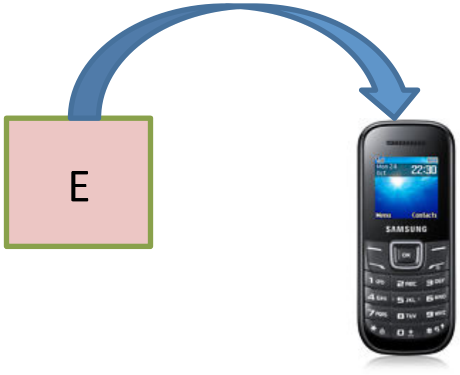
Algorithmic Attacks

- Can Mallory use tricks to break the algorithm

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

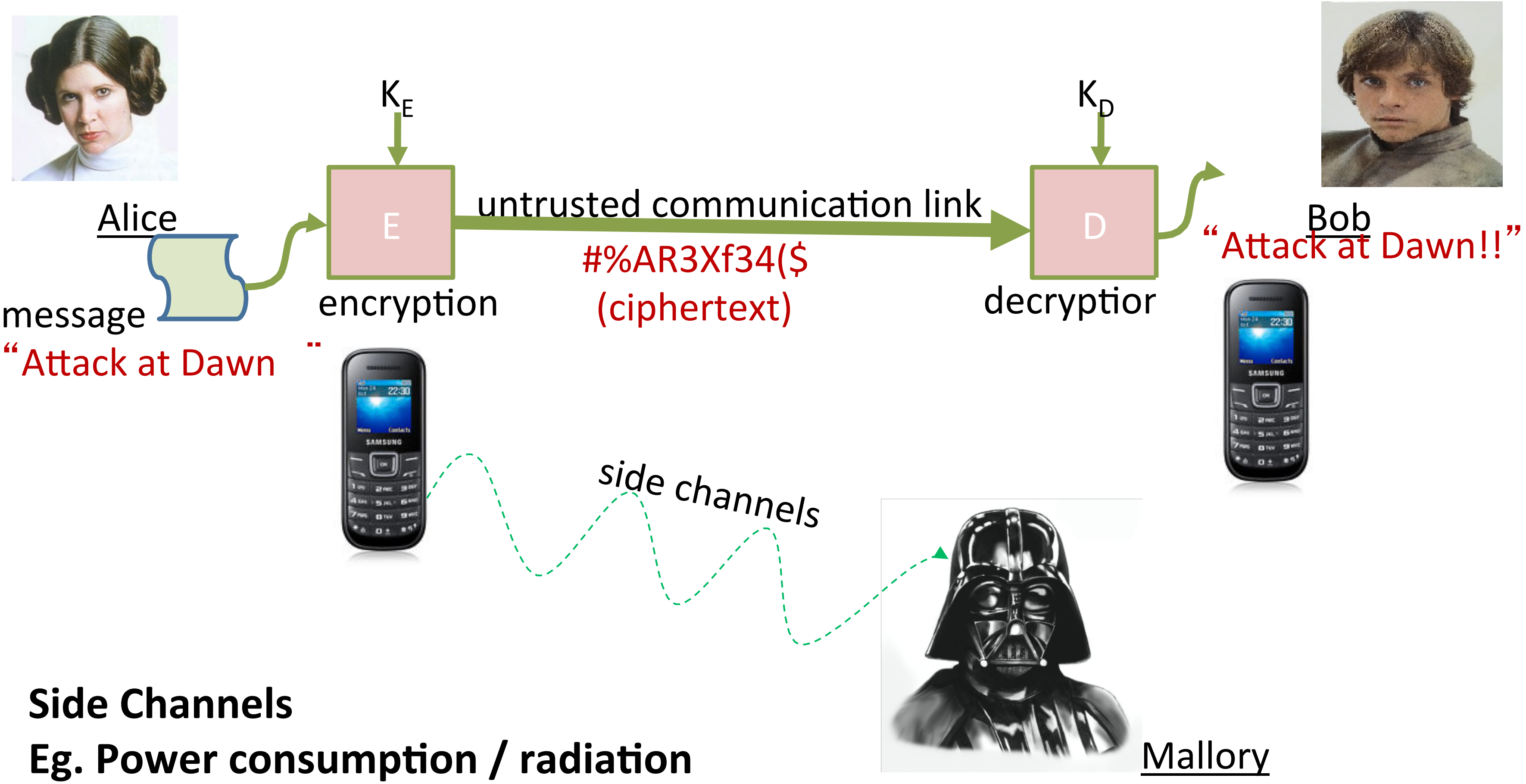
Cipher Implementations

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)



K_E

K_D

Alice

message

“Attack at Dawn ”

E

encryption

untrusted communication link

#%AR3Xf34($

(ciphertext)

D

decryptior

Bob

“Attack at Dawn!!”

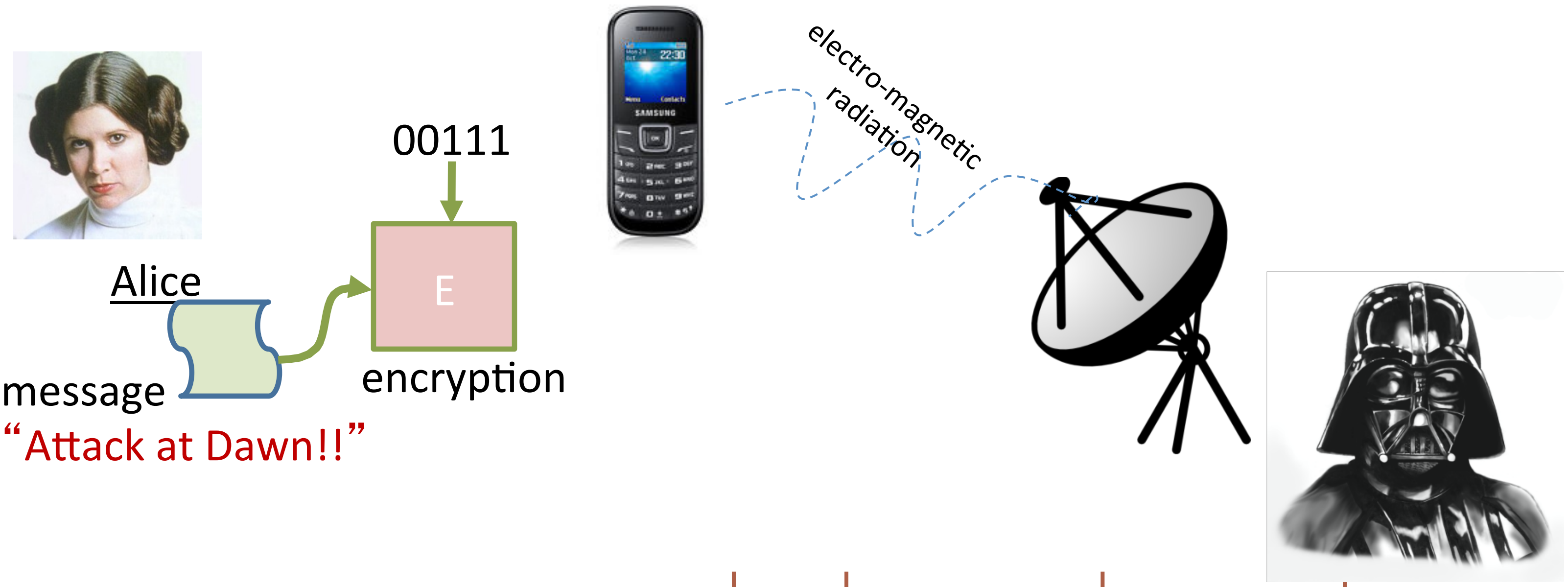
side channels

Mallory

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

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

Side Channel Analysis



Alice

message

"Attack at Dawn!!"

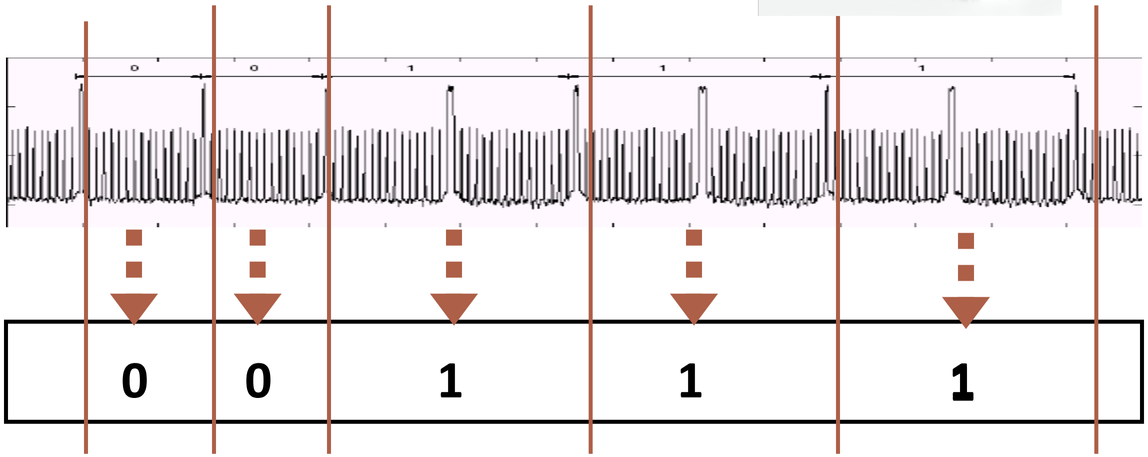
00111

E

encryption

electro-magnetic radiation

Radiation from Device

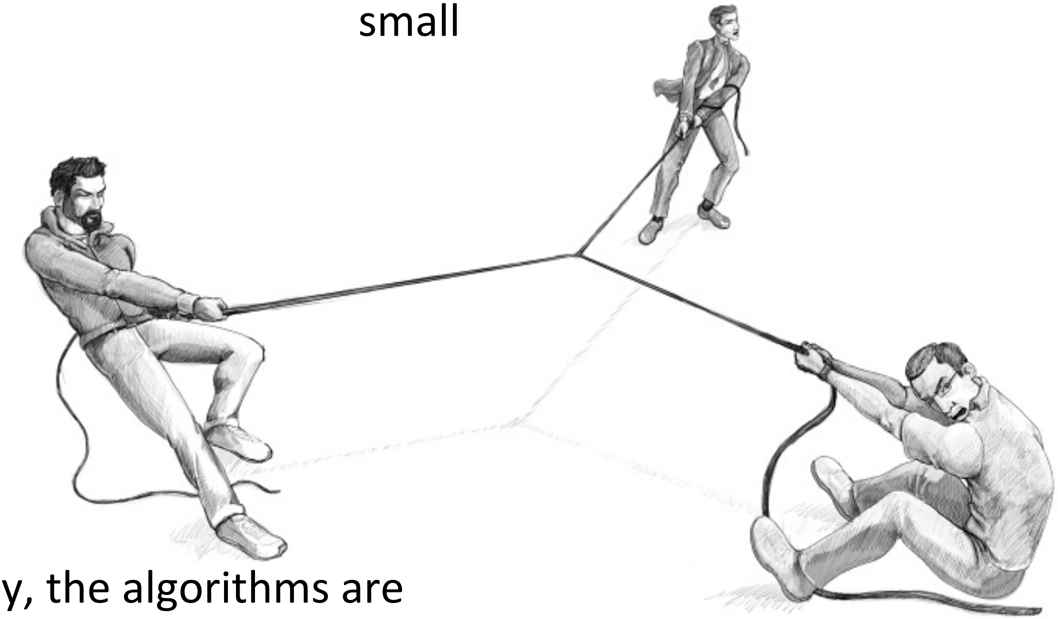


Secret information

0 0 1 1 1

Ciphers Design Challenges

Tradeoffs between Security , Speed, Side-Channel Attacks



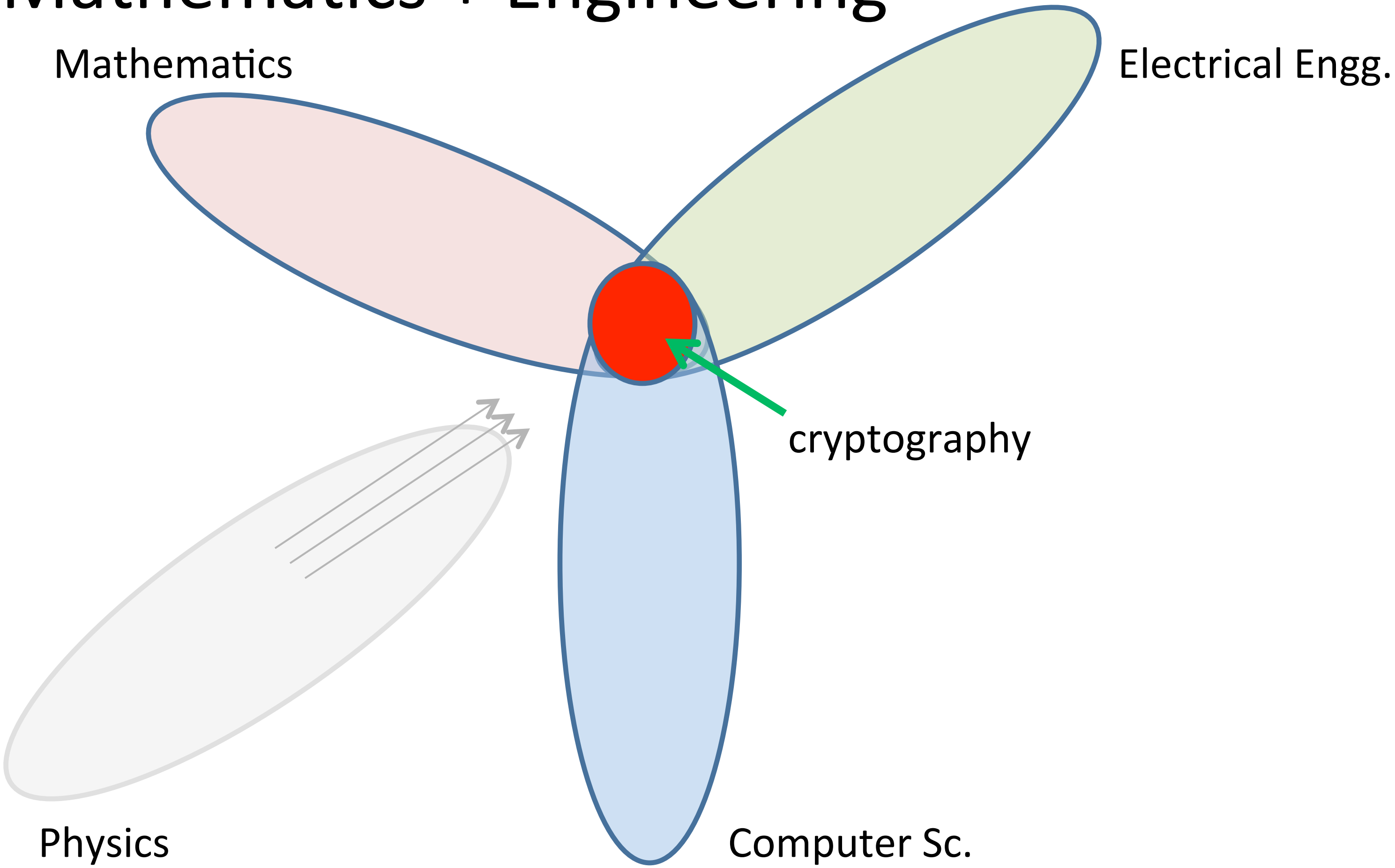
We want crypto algorithms to be fast and small

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

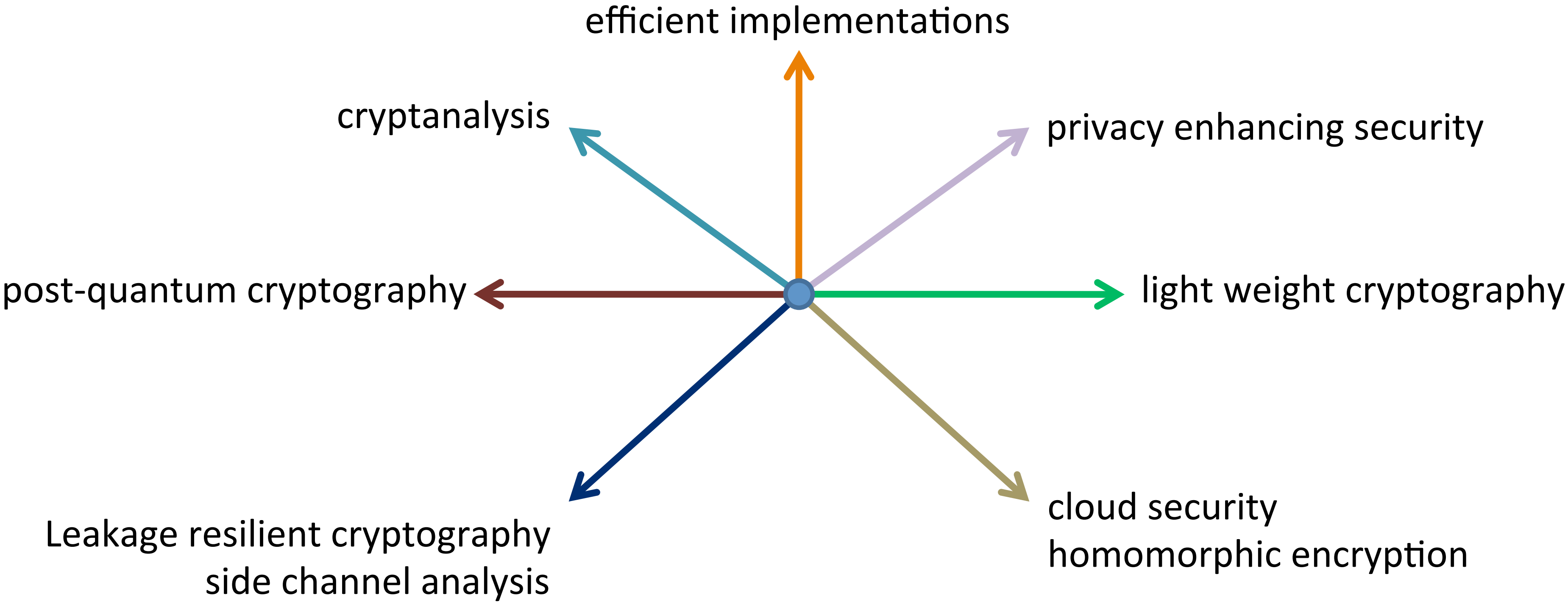
Need to protect against side channel attacks.

Cryptography Study

- Mathematics + Engineering



Some Hot Research Trends



efficient implementations

cryptanalysis

privacy enhancing security

post-quantum cryptography

light weight cryptography

Leakage resilient cryptography
side channel analysis

cloud security
homomorphic encryption

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
- Stream Ciphers
- Digital Signatures and Authentication
  - Hash functions
- Public key ciphers
  - RSA, implementations, and attacks
  - ECC
- 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% on (18/2/2016)
- Quiz 2 : 20% on (25/3/2016)
- End semester : 30% on (28/4/2016)
- Assignments : 15%
- Tutorials : 15%

Course Webpages

- For slides / syllabus / schedule etc.

  http://www.cse.iitm.ac.in/~chester/courses/17e_ac/index.html

- For discussions / announcements / submissions

  CSE Moodle

  Google Groups (aciitm_2017)

Logistics

- CS36
- Time:
  - Tuesdays : 11:00 - 11:50 AM
  - Wednesdays : 10:00 - 10:50 AM
  - Thursdays : 8:00 - 8:50 AM
  - Fridays : 4:50 – 5:40 PM