Cryptography

Lecture 1 : Introduction and Recap

Dr. Muhammad Hataba

Muhammad.Hataba@giu-uni.de

References and Legalities

These slides are in part based on:

- Understanding Cryptography, Christof Paar and Jan Pelzl, Lec 1
- Cryptography and Network Security Course, Swansea University, Lec 1 and 2
- Information Security Course, German International University, Amr ElMougy - Lec 1

The IT Security Major

Information Security

(4th Semester)

5th	**Cryptography**	Software and Mobile Devices Security	Digital Forensics
6th	Security and Risk Management	Pentesting	Business Continuity Management

Why Cryptography?

Cryptography in everyday life

Real Attack Incidents

WannaCry attack (2018)

18 days of NHS downtime

More than 200,000 computers in at least 100 countries

https://www.infosecurity-magazine.com/news/cyberattacks-caused-18-days-of-nhs/ https://www.bbc.co.uk/news/health-43795001

Real Attack Incidents

https://www.cyberscoop.com/vulnerability-iot-software-opened-door-thousands-internet-connected-devices/
http://blog.senr.io/blog/devils-ivy-flaw-in-widely-used-third-party-code-impacts-millions
https://www.arxan.com/wp-content/uploads/2017/01/2017_Security_IoT_Mobile_Study.pdf

Course Learning Outcomes (CLOs)

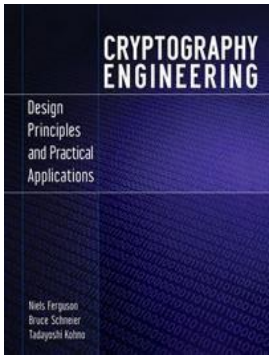
- Understand the difference between classical and modern cryptography
- Get familiar with modern cryptography approaches for collaboration, secure cloud storage, computing on encrypted data, and providing connections
- Understand the current research trends in cryptography
- Apply the theoretical concepts in a practical setup
- Learn how to critically examine case studies you hear about or read about

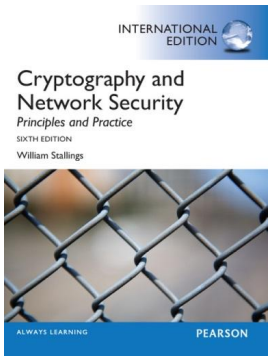
Course Outline

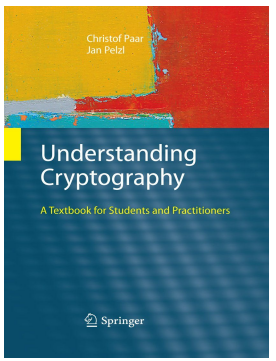
Week	Lectures
1	Intro + Recap
2	Mathematics Basics
3	Advanced Encryption Standard
4	Elliptic Curve I
5	Elliptic Curve II
6	Zero Knowledge Proofs
7	Threshold Crypto + Secret Sharing
8	Secure Multiparty Computation I
9	Homomorphic Encryption I
10	Homomorphic Encryption II
11	Functional Encryption
12	Quantum and Post-Quantum Crypto

Course Resources

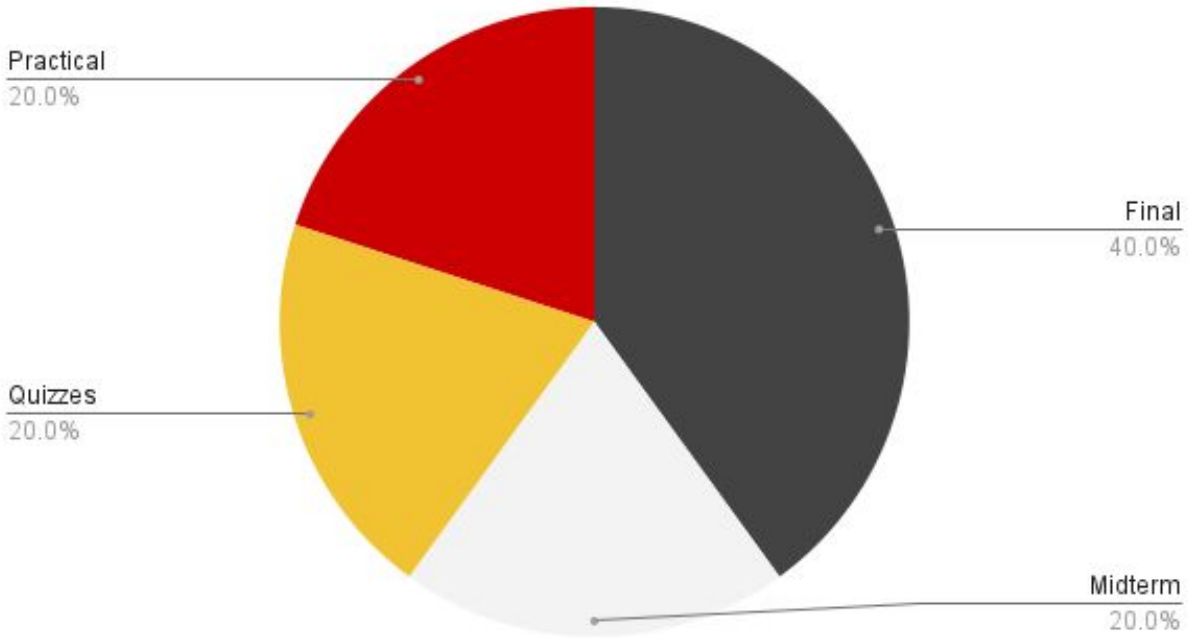
- Paar, Christof, and Jan Pelzl. Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media, 2009.
- Ferguson, Niels, Bruce Schneier, and Tadayoshi Kohno. Cryptography engineering: design principles and practical applications. John Wiley & Sons, 2011.
- Stallings, William. Cryptography and network security, 8th Edition. Pearson Education India, 2020.
- Software (excellent demonstration of many ancient and modern ciphers): Cryptool, http://www.cryptool.de







Course Evaluation



Outline of Today's Lecture

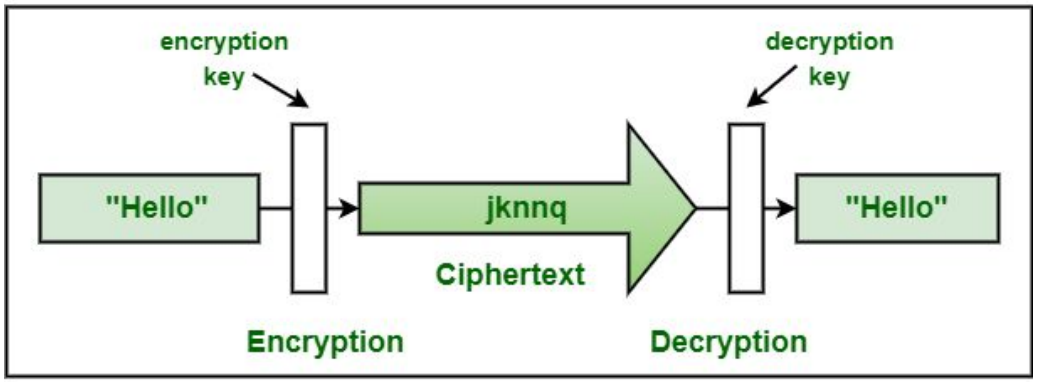
- Recap of key concepts of Cryptography
- Classification of Cryptology and Cryptography
- The different types of attacks

Introduction

What is Cryptography?

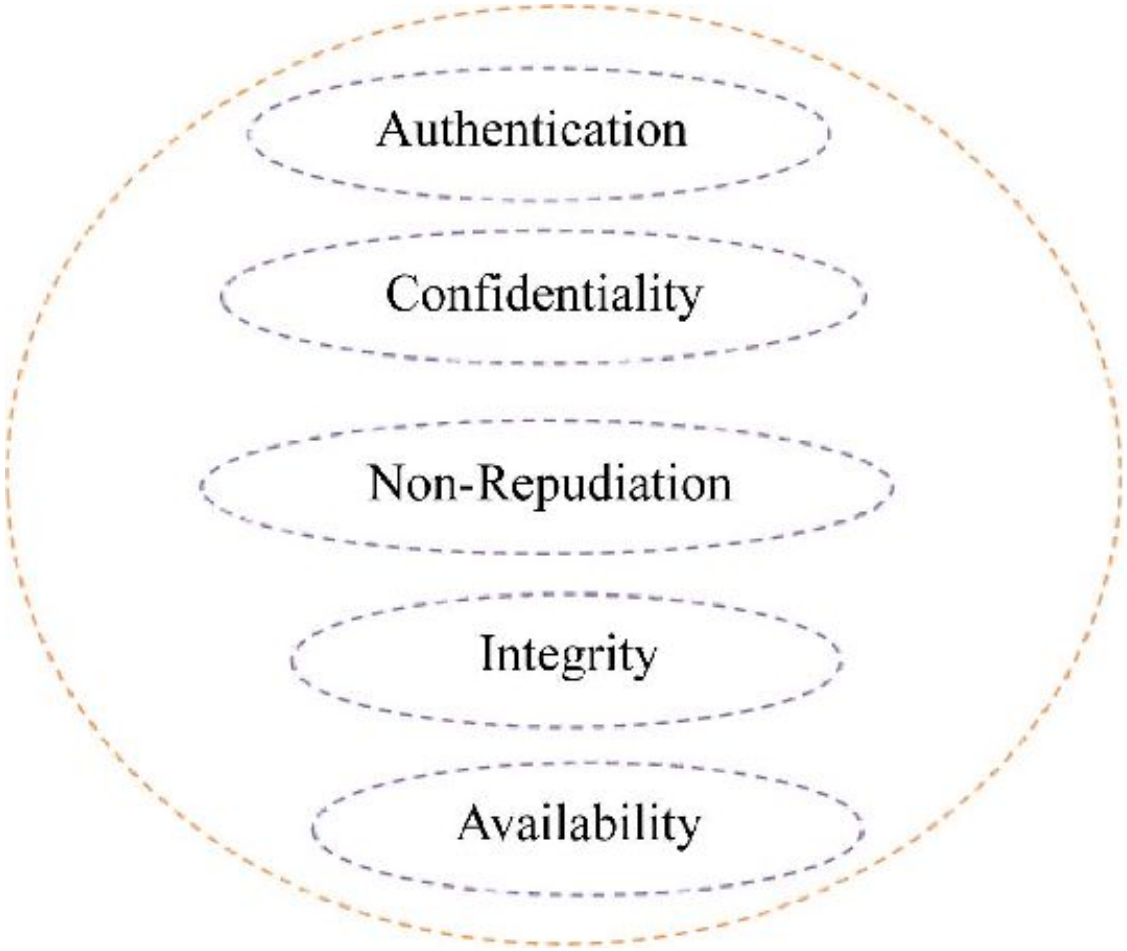
What is Cryptography?

Cryptography is the practice and study of techniques for secure communication in the presence of adversarial behavior.



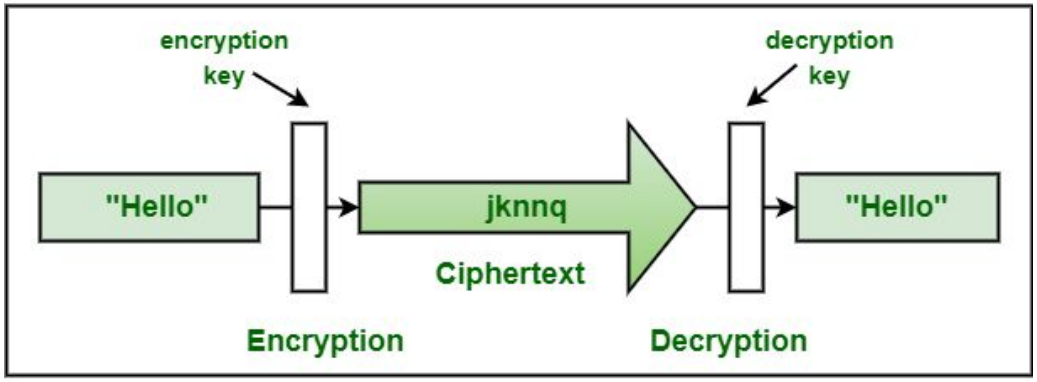
Cryptography

Key Security Concepts



What is Cryptography?

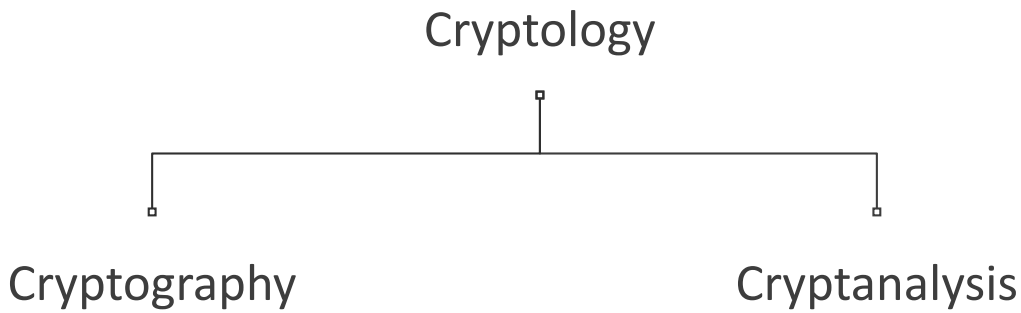
Cryptography is the practice and study of techniques for secure communication in the presence of adversarial behavior.



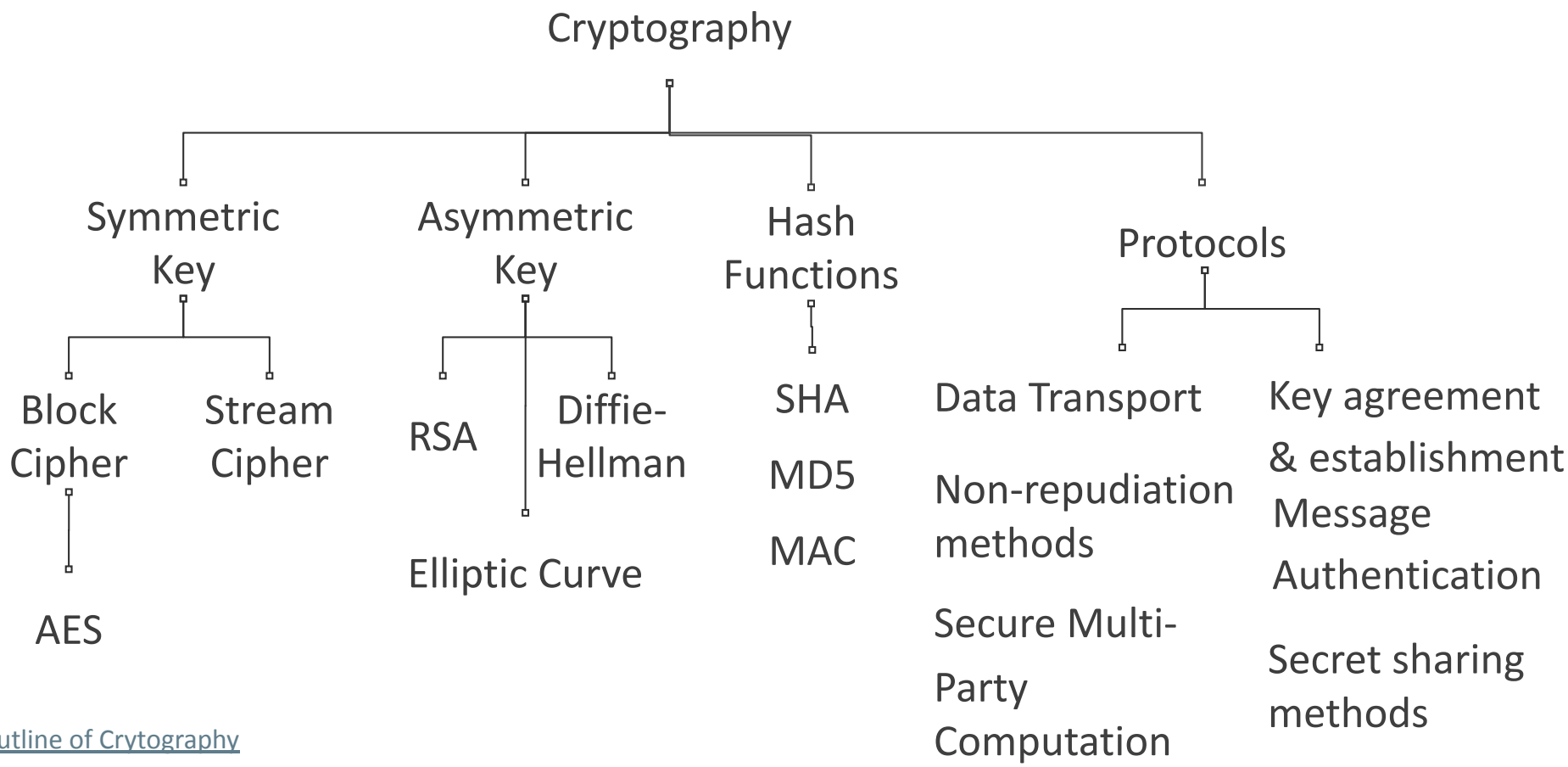
Cryptography

In practice: How to fulfil all the key concepts of security?

Classification of Cryptology



Classification of Cryptography



Outline of Crytography

Course Outline

	Week	Lectures
Crypto 1.0	1	Intro + Recap
	2	Mathematics Basics I
	3	Mathematics Basics II
	4	Advanced Encryption Standard
	5	Elliptic Curve I
	6	Elliptic Curve II
Crypto 2.0	7	Zero Knowledge Proofs
	8	Secret Sharing
	9	Secure Multiparty Computation I
	10	Homomorphic Encryption I
	11	Homomorphic Encryption II
	12	Quantum and Post-Quantum Crypto

Recap

What you learned so far?

Recap - Basic Facts

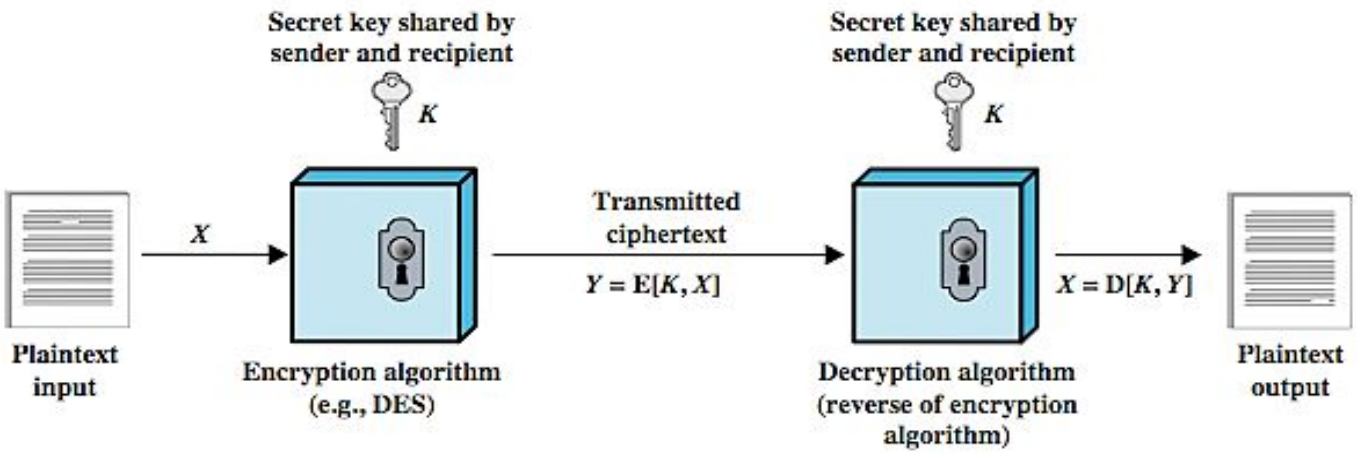
- Ancient Crypto: Early signs of encryption in Egypt in ca. 2000 B.C.
- Letter-based encryption schemes (e.g., Caesar cipher) popular ever since.
- Symmetric ciphers: All encryption schemes from ancient times until 1976 were symmetric ones.
- Asymmetric ciphers: In 1976 public-key (or asymmetric) cryptography was openly proposed by Diffie, Hellman and Merkle.
- Hybrid Schemes: The majority of today‘s protocols are hybrid schemes, i.e., the use both
  - symmetric ciphers (e.g., for encryption and message authentication) and
  - asymmetric ciphers (e.g., for key exchange and digital signature).

Nice article

Notation and Setup

- m represents the original *plaintext* message.
- c represents the *ciphertext*, i.e. *encrypted* version of the message.
- E *represents encryption*: is the process of converting plaintext into ciphertext, especially to prevent unauthorized access.
- D *represents decryption*: is the reverse process, converting ciphertext back into the original plaintext.
- k *represents key*: is the key used by the encryption, decryption function
- $|k|$ *represents keyspace*: is the number of possible keys

Symmetric Encryption



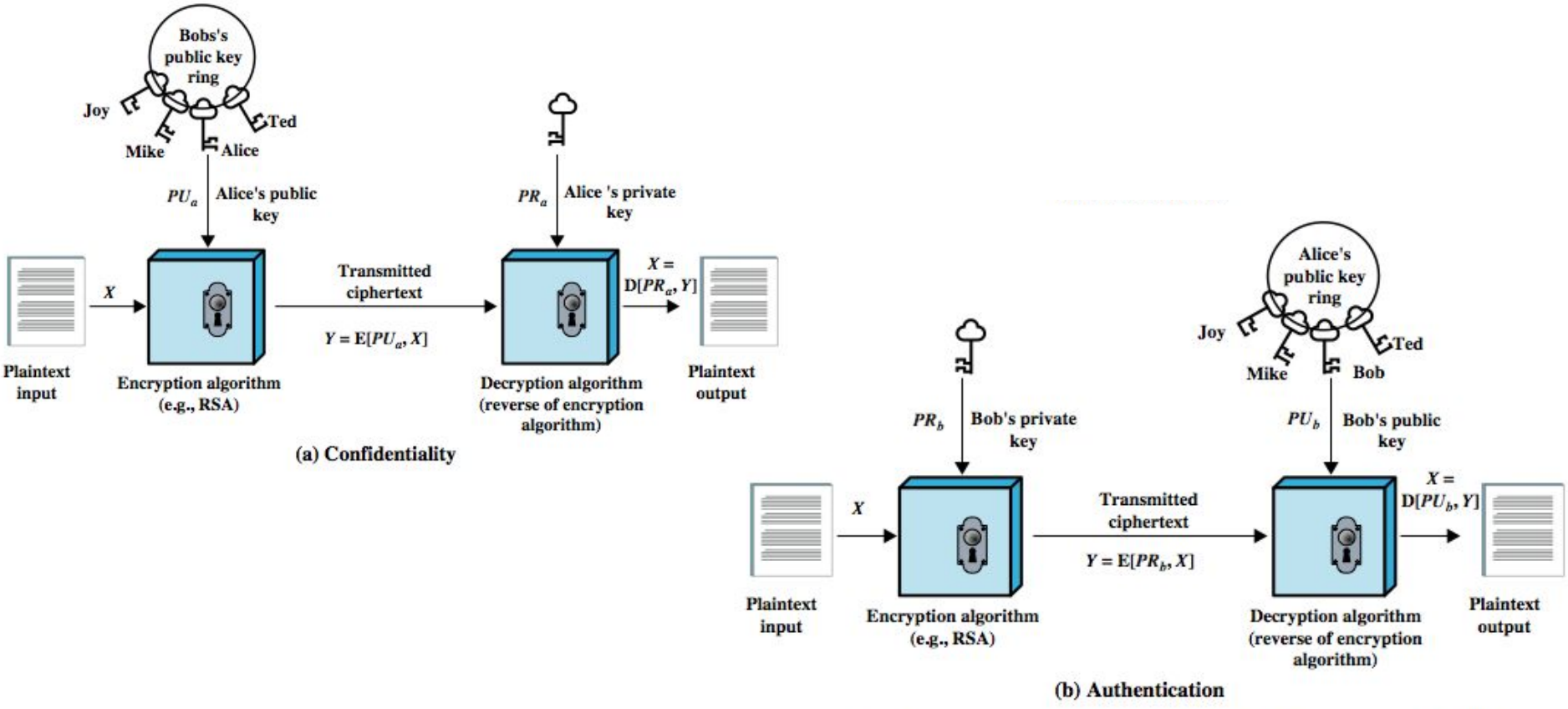
- Conventional / private-key / single-key
- Sender and recipient share a common key
- All classical encryption algorithms are private-key
- Was only type prior to invention of public-key in 1970's, and by far most widely used

GIU GERMAN INTERNATIONAL UNIVERSITY

Requirements

- Two requirements for secure use of symmetric encryption:
  - a strong encryption algorithm
  - a secret key known only to sender / receiver
- Mathematically have:
  - $Y = E_K(X)$
  - $X = D_K(Y)$
- Assume encryption algorithm is known
- Implies a secure channel to distribute key

Public Key Encryption



GIU GERMAN INTERNATIONAL UNIVERSITY

Kerckhoff's Principle (1883)

To decrypt the message Bob needs to know:

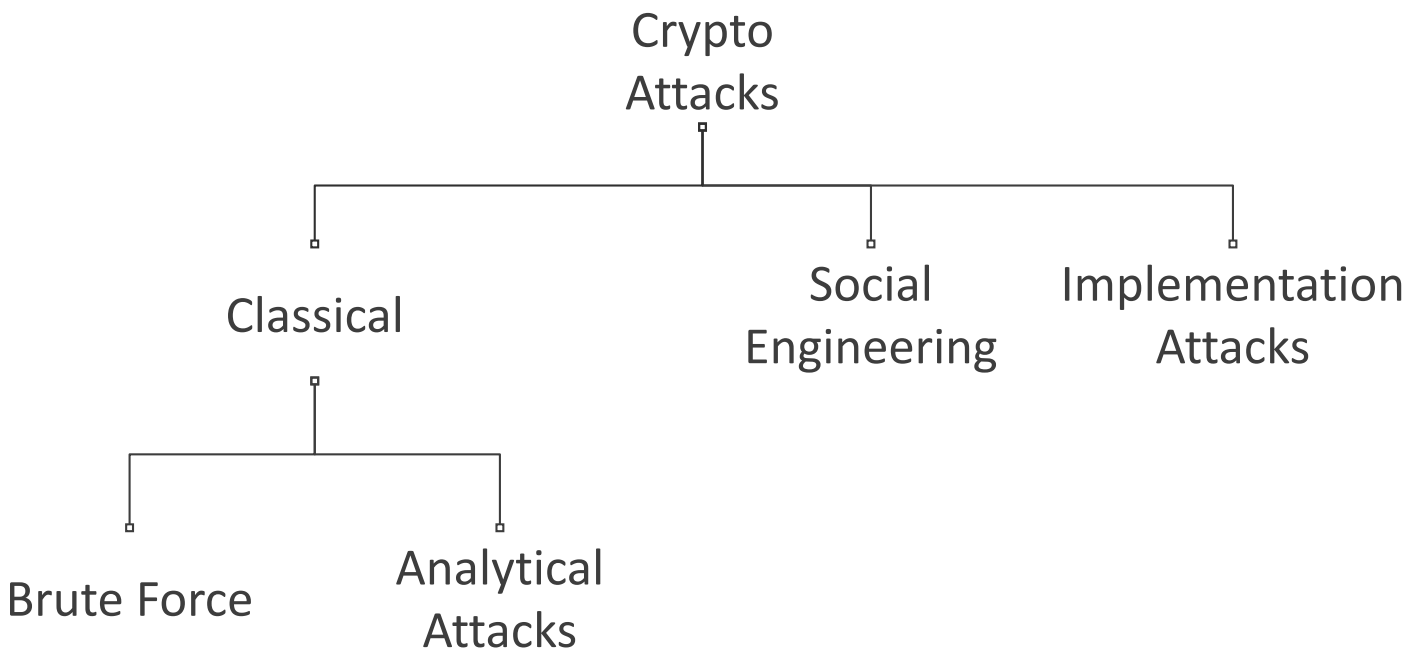
- the decryption algorithm $\mathcal{D}$, and
- the key K_e

The Principle states:

> "the security of the encryption scheme must depend only on the secret of the key and not the algorithm"

There are many reasons to follow this rule -- we will see throughout the course (hard to change algorithm, easy to change key, better to have many people check the algorithm, etc).

Classification of Crypto Attacks



An adversary only needs to succeed with **one** attack. Thus, a long keyspace does not help if other attacks (e.g., social engineering) are possible ⇒ **interdisciplinary field**

Interdisciplinary Approach in Security

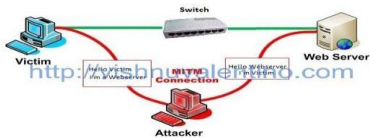
- Mathematics
- Computer Science
- Modern Computer Networks
- Security Engineering
- Electronics & Communication
- Ubiquitous Technology
- Human Computer Interaction
- Many more

Weakest Link Principle

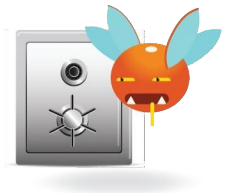
Cryptography is different due to the Weakest Link Property

"A security system is only as strong as its weakest link"

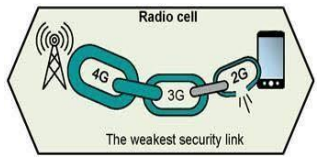
Human



Network

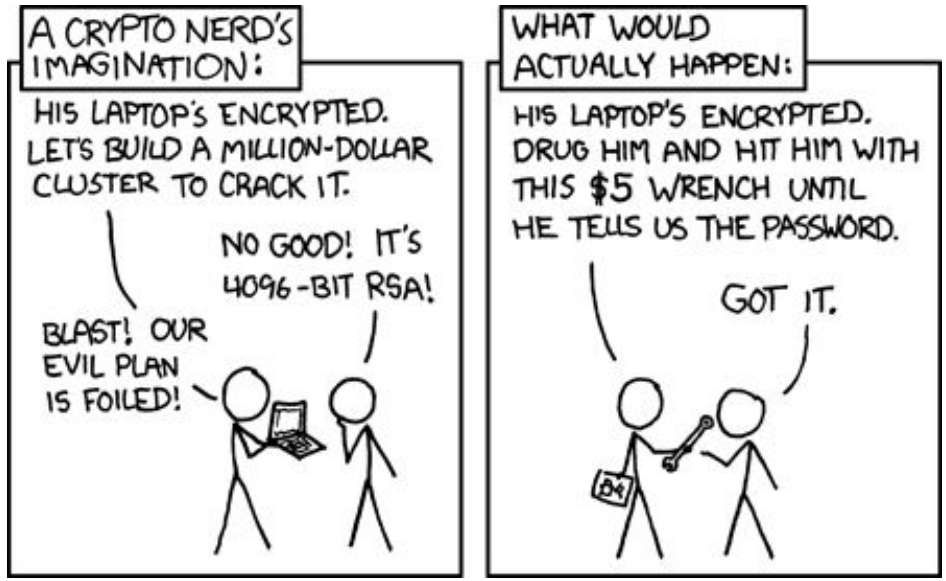


System



Communication

Examples


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Cryptography as a Whole

Is Cryptography an absolute solution?

- Cryptography (the art and science of secure communication) is often considered a solution to security.
- It is not absolute! Believe me!!
- It can often form part of the solution, but in itself it is not a full solution to a problem.
- It can make security of systems stronger but also *weaker* if weak crypto solutions are being implemented.

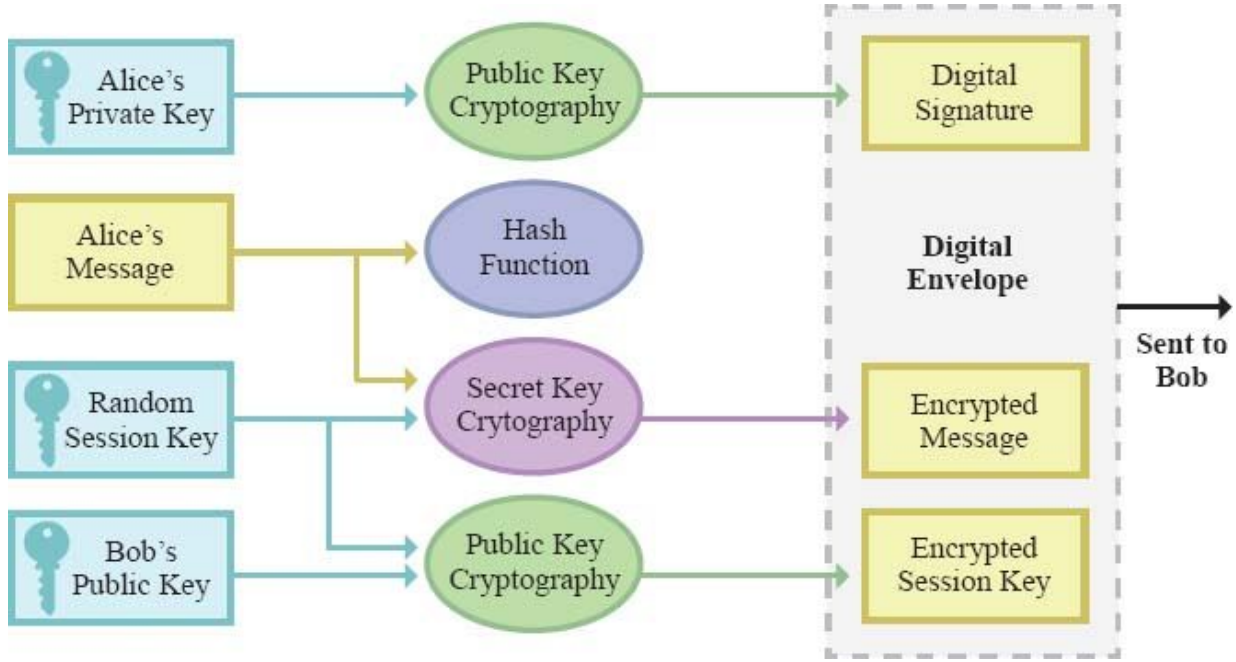
Cryptography is Hard!

Never trust a cryptographic system that has not been analysed by experts (and still then there is likely to be flaws!)

⇒ Cryptography Protocols and Services

Cryptographic Services and Protocols

- Encryption
- Authentication
- Key Management
- Signage



Each of them have their different approaches, parameters, pros, and cons.

Thank you