

Introduction to Cryptography

Sushmita Ruj

People and Website

- Convenor: Sushmita Ruj
- Tutors: Vir Pathak, Nhi Nguyen
- Course Email: cs6453@cse.unsw.edu.au
- Course Website: <https://webcms3.cse.unsw.edu.au/COMP6453/24T2>
- Forum : Ed forum (please join in with the link on WebCMS)
- Please bookmark this page
- Consultation time: Tuesday 3-4 pm (in-person/online), by appointment

Why Study Cryptography?



- Logging in to your computer
- Online Transactions
- Secure Messaging

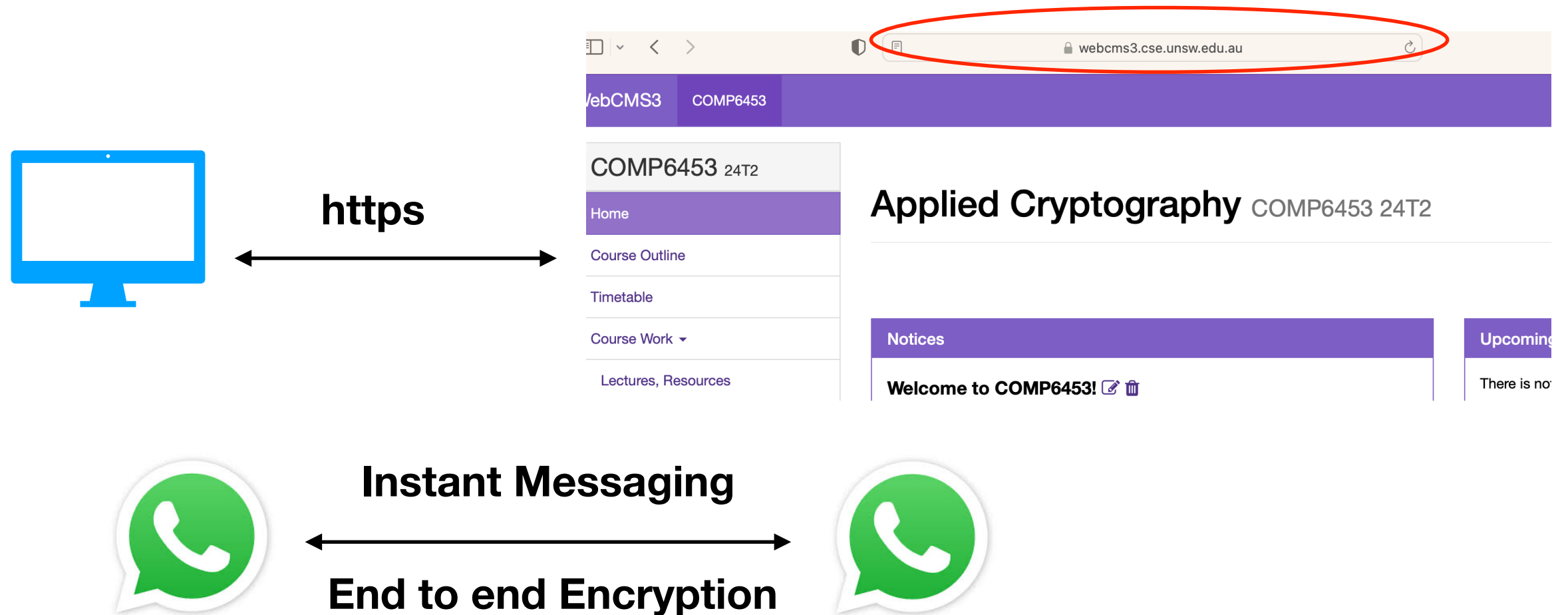
Cryptography is Everywhere

- Wifi
- Your access card
- Your online browser
- Apps on your phone
- myUNSW
- myGov Database...

Cryptology

- Crypt: Hidden
- Cryptology = Cryptography + Cryptanalysis
- Cryptography: Art of secret writing (Defender)
- Cryptanalysis: Art of revealing information from hidden messages (Attacker)

Secure Communication

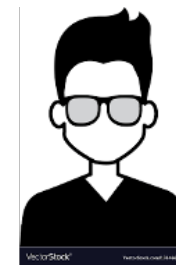
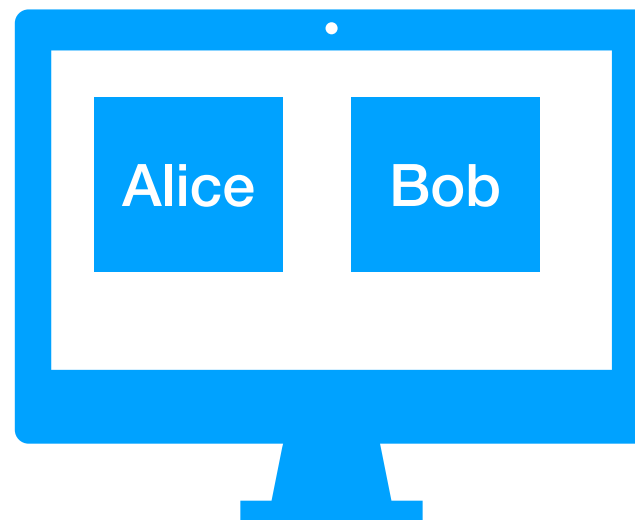


1. Eavesdropper wants to read your message (passive attacker)
2. A malicious entity can even modify your message (active attacker)

Secure Storage



Alice



Bob

Alice's files: No one apart from Alice can access her files or modify content

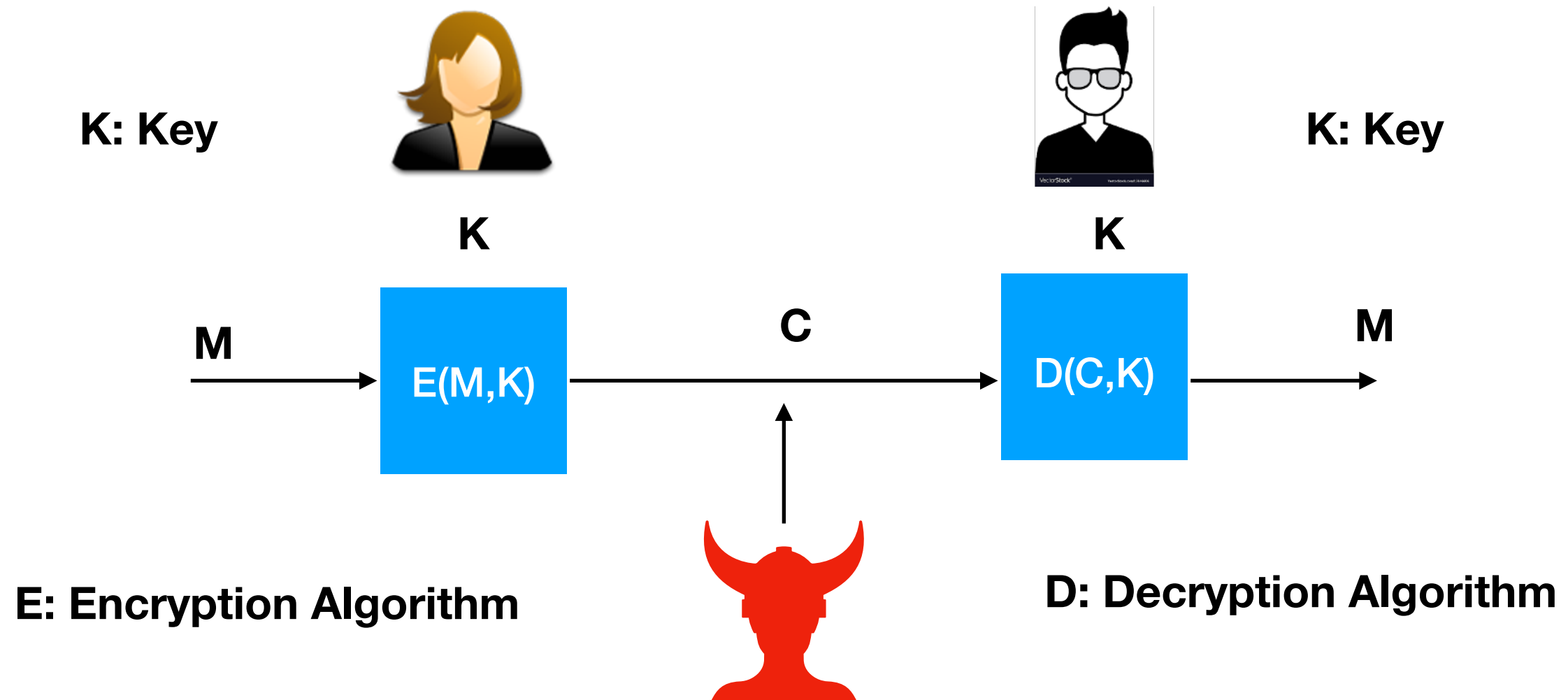
Bob's files: No one apart from Alice can access her files or modify content

Files are encrypted

What is Encryption

- Plaintext is garbled in a way that you cannot get any **meaningful information** from the garbled message
- What can I know from the Garbled Message (Ciphertext)
- Alice's student record is encrypted: Adversary can't get her DoB, but can an adversary get her address, or her phone number? **(Important questions!)**

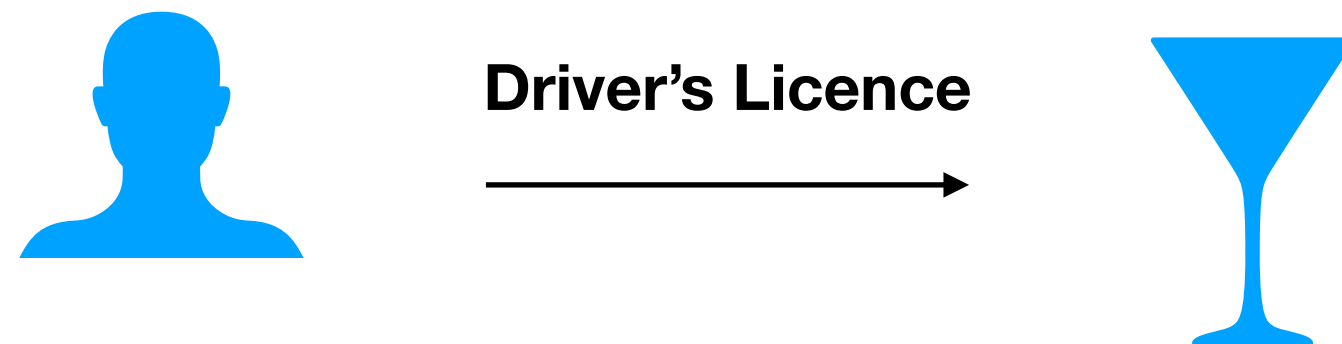
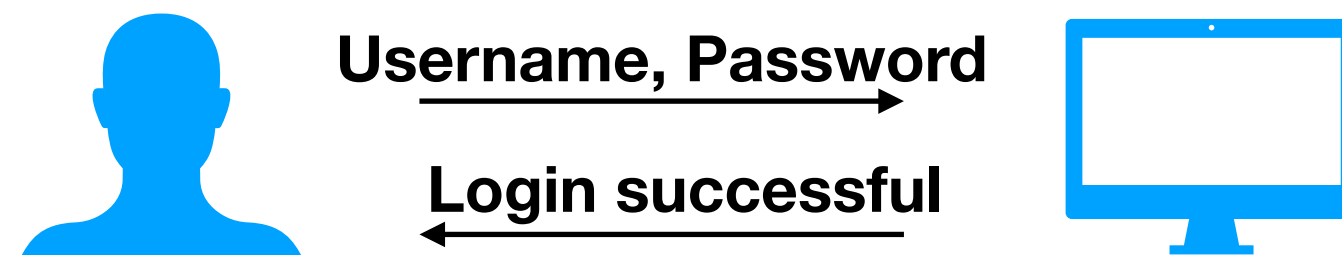
Encryption (Building Block)



Algorithms are known to Everyone (Public information)
Key is secret (known only to Alice and Bob)

Kerckhoff's Law: The security of a cryptographic system should not rely on the secrecy of the algorithm

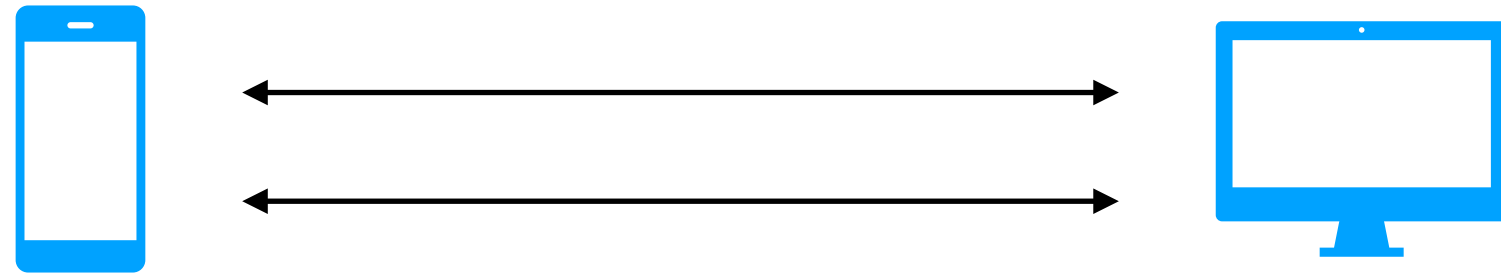
Authentication



Authentication: Verify if user is a legitimate entity

**Very important to know the
difference between
Encryption and Authentication**

Who Wants What?



- User
 - Confidentiality
 - Integrity
 - Authentication
- Attacker:
 - Passive (eavesdropper)
 - Malicious/ Active: Modify content

Protect against Attacker
Have a threat model

Cryptography is..

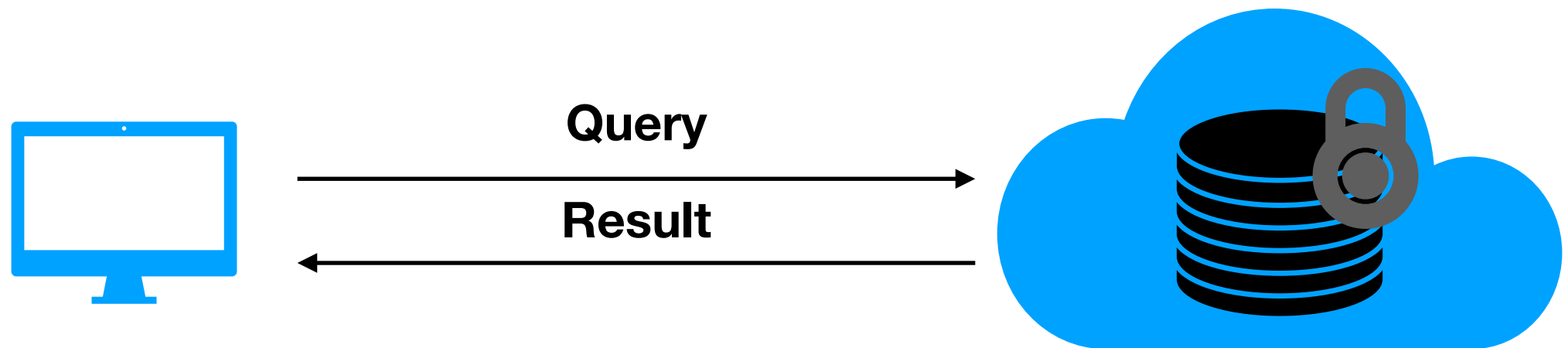
- A powerful tool to protect against attackers
- Core of many secure systems and mechanisms
- NOT
 - A solution for all security problems
 - Dangerous if not implemented properly
 - Dangerous if not used properly
 - Dangerous if not **analysed properly**

Power of Cryptography

Compute without knowing the data (Secure Computing)

- E-voting: You don't want the system to know your vote, but count your vote
- Private Auction: You want to hide the bid, and the auctioneer is still able to determine the highest bidder?

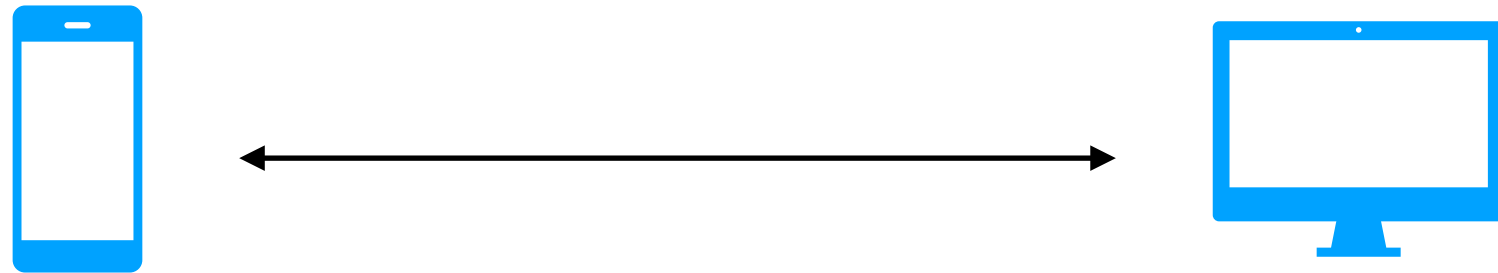
Computing on Encrypted Data



Query can be a keyword search
Complicated statistical query
Some function $f(x, y, \dots)$

Homomorphic Encryption, Searchable Encryption : Week 10

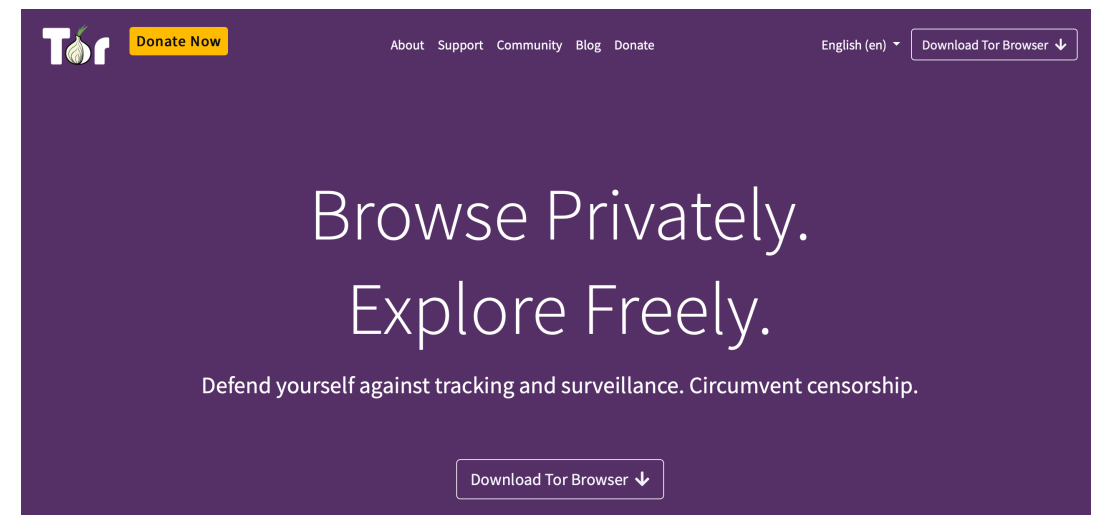
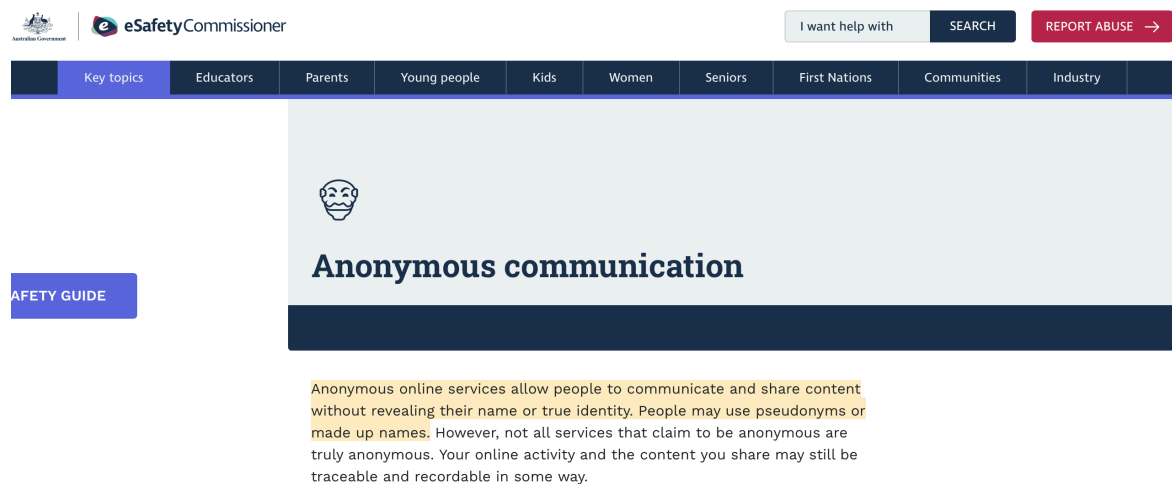
Anonymous Communication



Server does not know the IP Address

Freedom of information: Strict regime in certain countries

Anonymous Messaging: Post Without disclosing identity



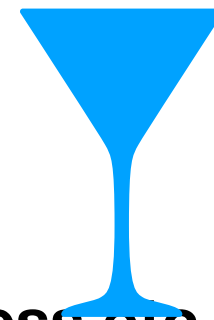
Buying on a dark web

Key exchange and digital signatures: Weeks 5 and 7

Verifiability



Driver's Licence



Is age >18

User has to reveal Date of Birth, Address etc

Verify without revealing all information: Verifiable credentials



Query



Result



Prove that the result is correct, without disclosing the answers


Prove I have enough money in my bank account to buy a car worth \$X,
without revealing my bank balance?

How do I verify a ML algorithm generates the correct models

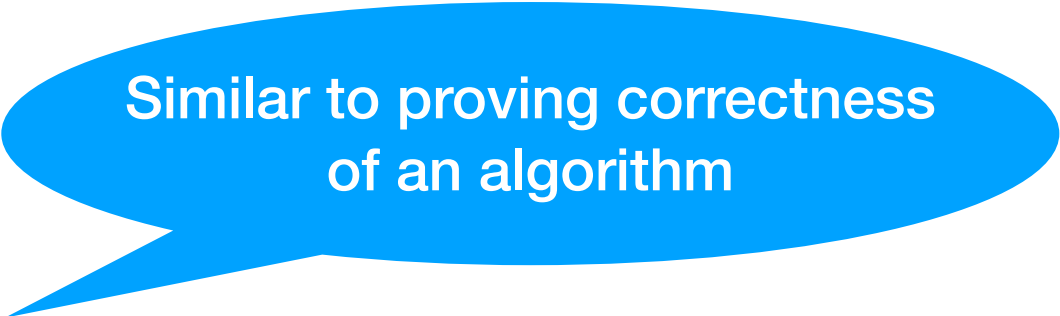
Zero-Knowledge Proofs: Week 9

Cryptography in 3 Steps

- Define the threat model precisely
- Propose a construction
- Prove that breaking the construction under the threat model is hard



Do this
iteratively, playing the devil's
advocate



Similar to proving correctness
of an algorithm

Course Objectives

- Understand cryptographic algorithms with an aim of using them to protect computer systems, networks, and data protection.
- Foundational aspects of encryption and authentication techniques with an aim to use them correctly and effectively in applications.

Course Goals

- Explain the foundations of cryptography, primitives, and protocols, including encryption and authentication.
- Perform Cryptanalysis on ciphers based on an understanding of the techniques of Cryptanalysis
- Formally analyse security of protocols based on an understanding of security considerations
- Implement cryptographic algorithms including practical encryption and authentication protocols.
- Design secure cryptographic protocols for a broad range of applications like blockchains, e-commerce and computer networks.
- Explain the implications of quantum computing on Cryptography and learn about existing quantum safe solutions.

Cryptography: Definition

- A cryptographic algorithm is a well-defined transformation, which on a given input value produces an output value, achieving certain security objectives.
- A cryptographic protocol is a distributed algorithm describing precisely the interactions between two or more entities, achieving certain security objectives.
- A cryptographic scheme is a suite of related cryptographic algorithms and cryptographic protocols, achieving certain security objectives.

What we will learn?

- Foundations
- Algorithms
- Cryptanalysis
- Cryptographic libraries
- Good and Bad implementations
- Security analysis
- Problem solving

What Jobs Require Cryptography?

- Cryptography everywhere!
- Defence: ASD, DSTG etc
- Government: State and Federal Governments
- Blockchain startups: Plethora of jobs + flexibility
- Industry: Tech jobs, Banking/finance, Telecom, Health
- Do Cryptography Research: Many many unsolved problems

Lectures/Tutorials

- Ask as many questions as you can
- Don't take anything for granted
- Build- Break-Build repeat!
- Security vs performance

Assessment

- Fortnightly assessments: Submissions on Week 3, 5, 7, 9 on Fridays 5 pm
- Term Project + Paper: Submission Week 10, Friday 5 pm
- Final Exam: Closed book in-person during exam period

Fortnightly Assessment

- Assessment released on the week before submission
- Combination of coding, short answer type questions and problem solving questions

Term Project

- Start thinking seriously about projects from day 1
- Group projects : group size 2-4
- Should be complete, a solid problem statement, algorithmic solution, implementation, security analysis
- Choose your group to have a good technical diversity (coding skills, analytical/math skills)
- Some ideas will be discussed in class.
- Abstract submission by Week 5. Should receive a good ahead from me. Earlier Submission will receive early review.
- Projects report/paper are published online in Week 10. Everyone's contribution will be documented along with the report/paper.
- Peer-reviewed. If you can find bugs in your peer's project, you get extra marks
- Your project will also be evaluated/graded by a tutor.
- This is a general practice for cryptography evaluation.

Page under construction

Marks Distribution

- ass = Fortnightly Assignments (out of 30)
- proj = mark for Project (out of 30)
- finalExam = mark for final exam (out of 40)
- $\text{mark} = \text{ass} + \text{proj} + \text{finalExam}$
- $\text{grade} = \text{HD}|\text{DN}|\text{CR}|\text{PS}$ if $\text{mark} \geq 50$
- $= \text{FL}$ if $\text{mark} < 50$ or $\text{finalExam} < 40$
- Late penalties, Special considerations on Course Outline

Resources

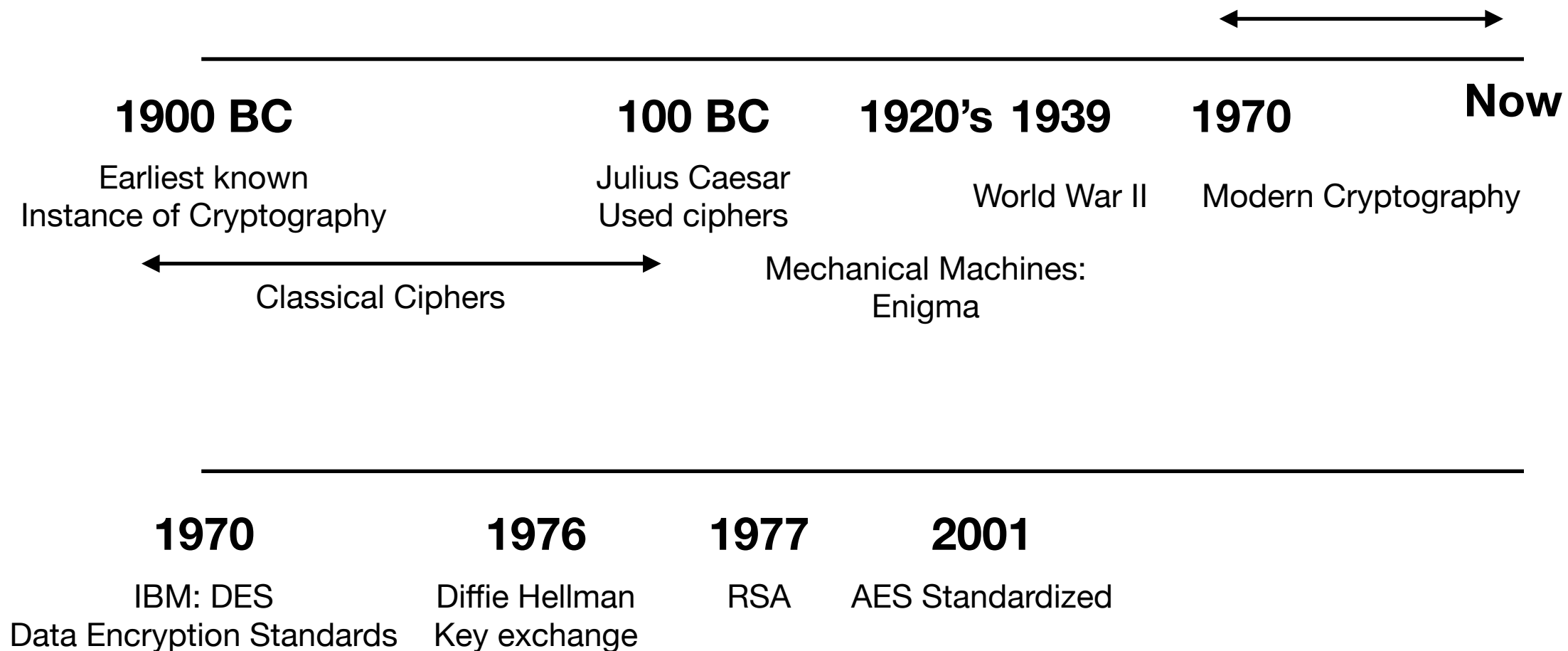
- Cryptography, Theory and Practice, (4th Edition)
by Douglas Stinson and Maura B Paterson published by Routledge.
- [https://www.ic.unicamp.br/~rdahab/cursos/mo421-mc889/Welcome_files/Stinson-Paterson_CryptographyTheoryAndPractice-CRC_Press_\(2019\).pdf](https://www.ic.unicamp.br/~rdahab/cursos/mo421-mc889/Welcome_files/Stinson-Paterson_CryptographyTheoryAndPractice-CRC_Press_(2019).pdf) (freely available)
- Introduction to Modern Cryptography (3rd Edition)
by Jonathan Katz, Yehuda Lindell, Routledge
- Handbook of Applied Cryptography (3rd Edition)
by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, CRC Press. Available online <https://cacr.uwaterloo.ca/hac/>
- A Graduate Course in Applied Cryptography (3rd Edition)
by Dan Boneh and Victor Shoup Available online <http://toc.cryptobook.us>
- Web recourse will be posted.
- The Code Book by Simon Singh. (Popular Science book.)

Ethics and Integrity

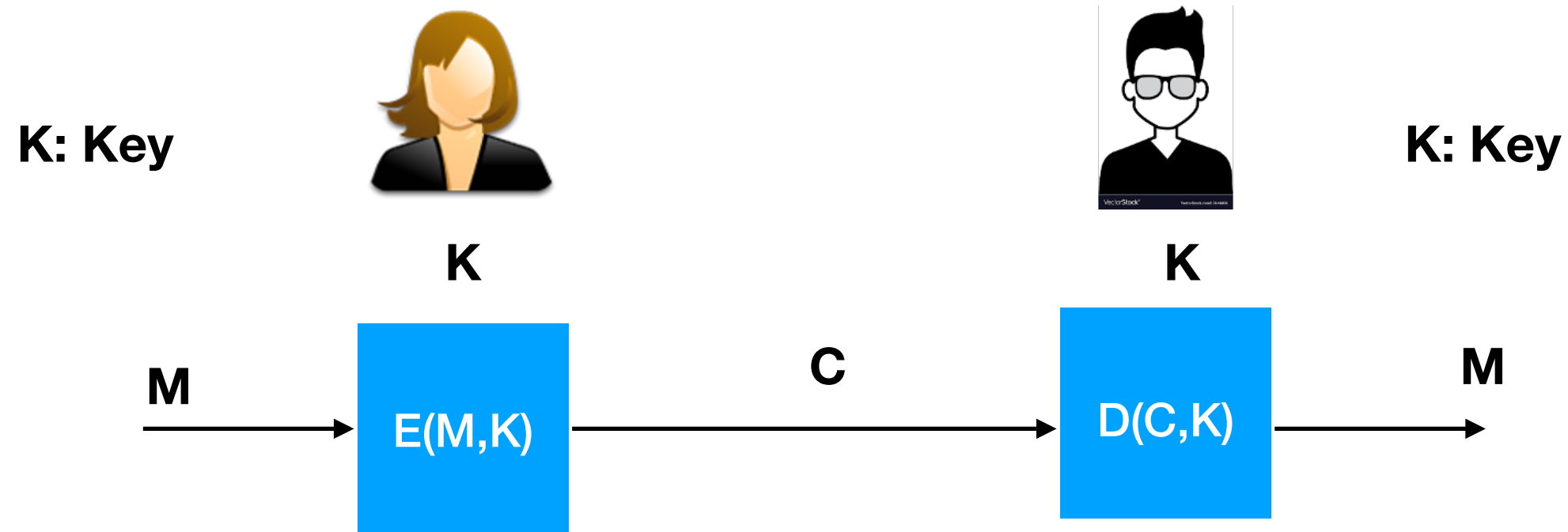
- Strict actions will be taken against plagiarism
- Acknowledge all help and resources in your assessments
- Use of AI Assisted tools in Assessments will lead to 0

Course Content

Crypto Timeline



Classical Ciphers

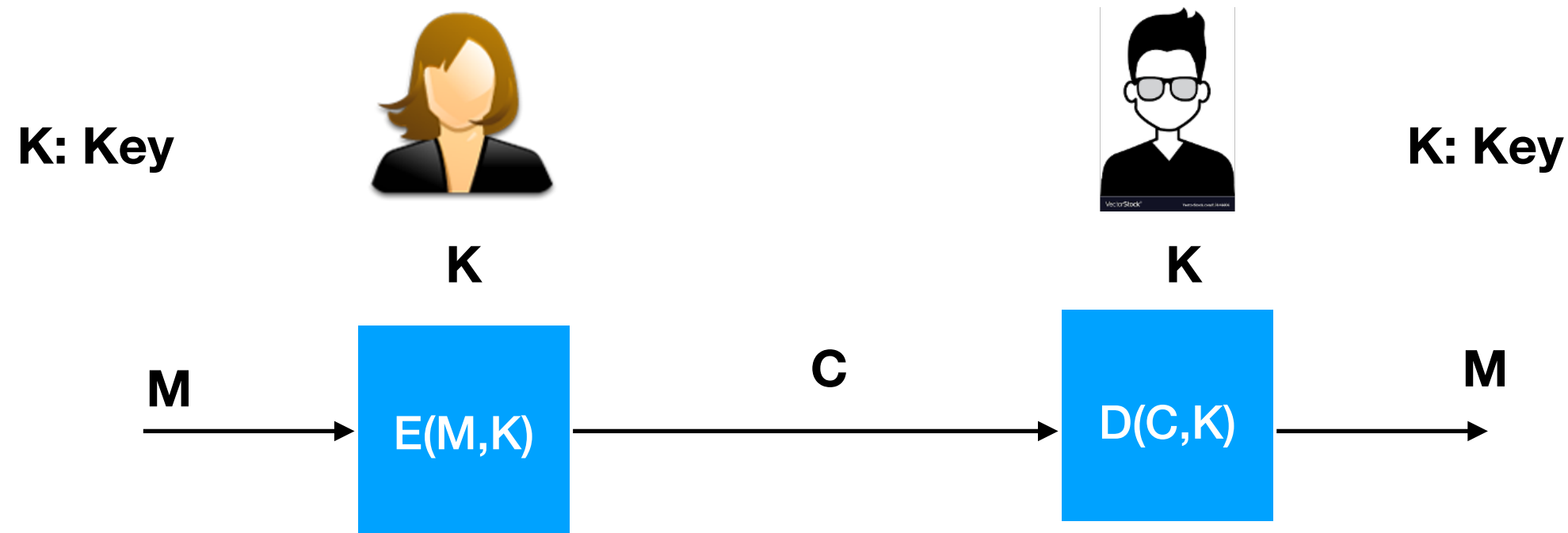


E: Encryption Algorithm

D: Decryption Algorithm

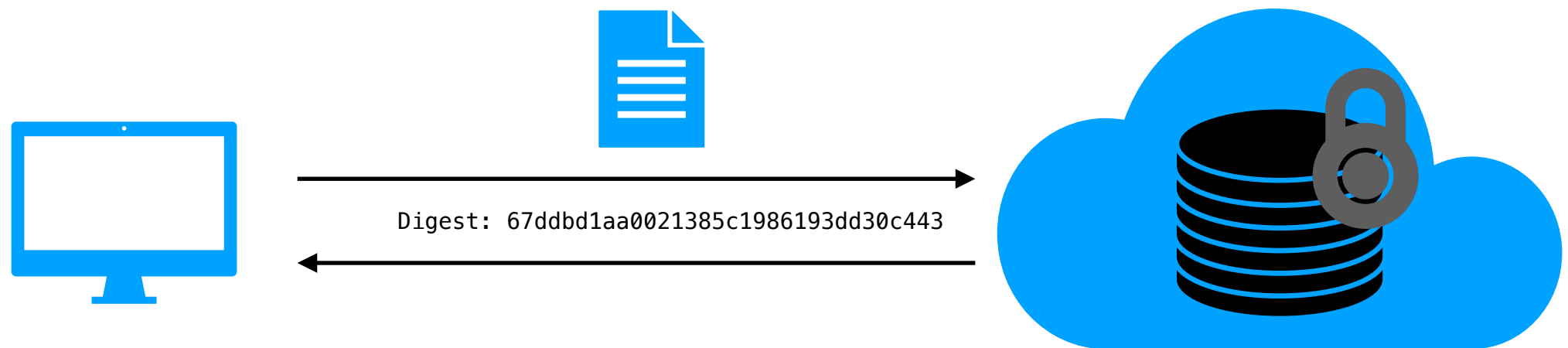
**E and D Very simple functions
Simple substitution, permutation**

Symmetric Key Encryption



- Examples of Encryption algorithms: Stream and Block ciphers [Weeks 1-2](#)
- How does Alice and Bob decide the common key?
- Key Establishment [Weeks 5](#)
- Too cumbersome in many situations
- Public key Cryptography : Part of the key is public [Weeks 4, 5](#)

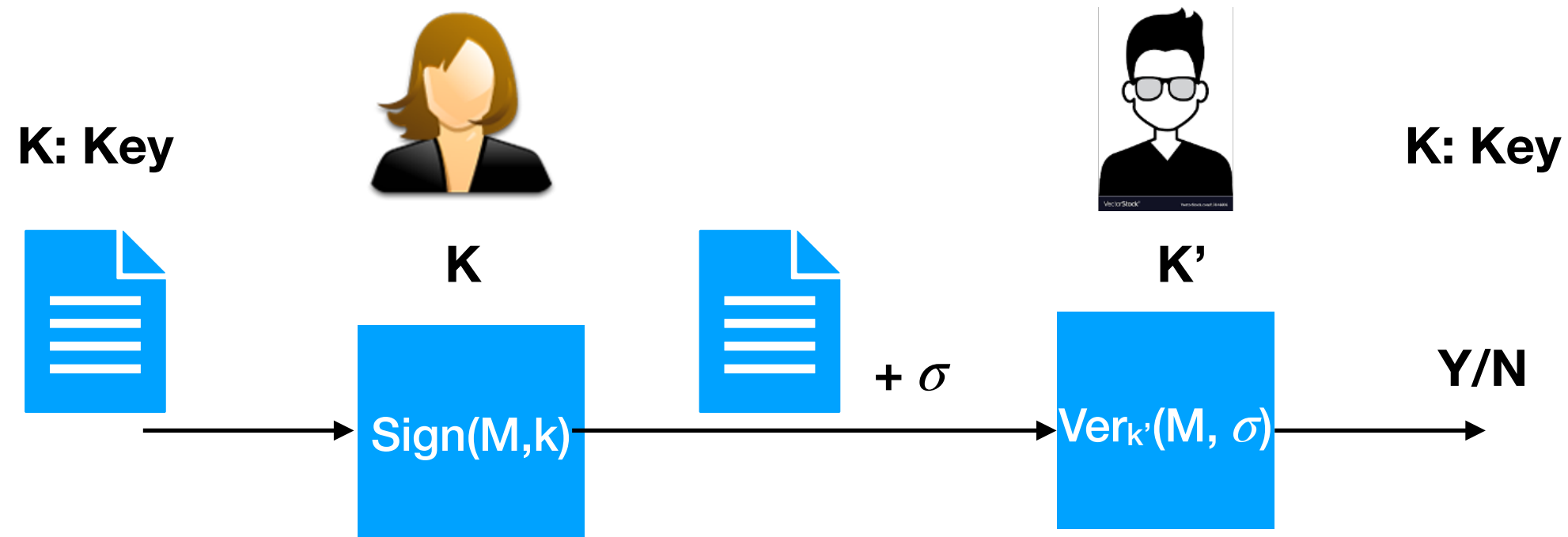
Integrity



Hash Functions : H
 $H : \{0,1\}^* \rightarrow \{0,1\}^l$

Week 3

Digital Signatures

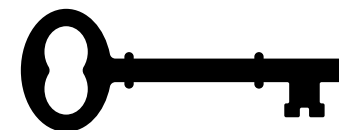


Week 7

Post Quantum Cryptography

- PKC prone to attacks by Quantum Computers
- How to design new algorithms that are resilient to quantum threats?
- Week 8

Secret Sharing



At least 2 out of 3 keys are required to open the vault
Threshold Cryptography: Threshold Signatures
Multi-sig wallets etc

Week 10

Applications

- Secret Sharing
- Secure Communication
- Secure Computation
- Blockchains
- Verifiable credentials
- E-voting

Thank you