Introduction to Cryptography

Sushmita Ruj

People and Website

- Convenor: Sushmita Ruj
- Tutors: Nhi Nguyen (Admin), James Liu, Alex Vong
- Course Email: cs6453@cse.unsw.edu.au
- Course Website: https://webcms3.cse.unsw.edu.au/COMP6453/25T2
- Forum : On Discourse, Please bookmark this page
- Consultation time: Thursday 4-5 pm (in-person/online), by appointment

Why Study Cryptography?

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

Cryptography is Everywhere

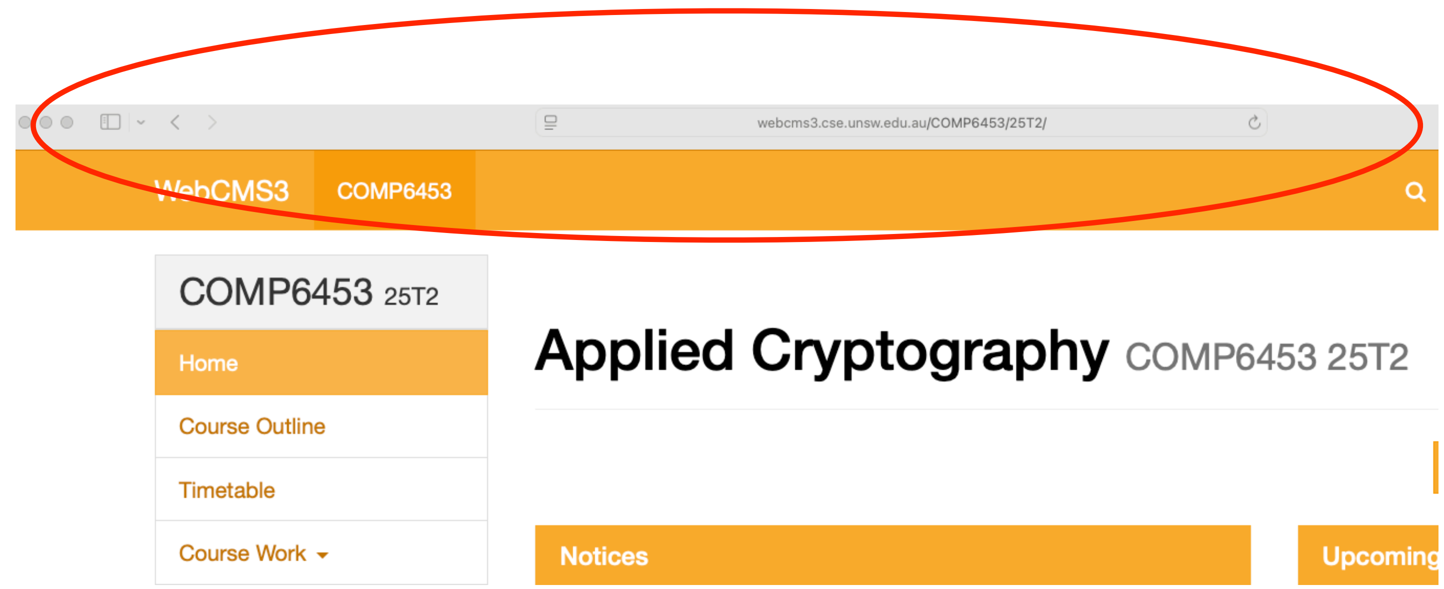
- Wifi
- Your access card
- Your online browser
- Apps on your phone
- myUNSW
- myGov Database…

Cryptology

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

Secure Communication

https

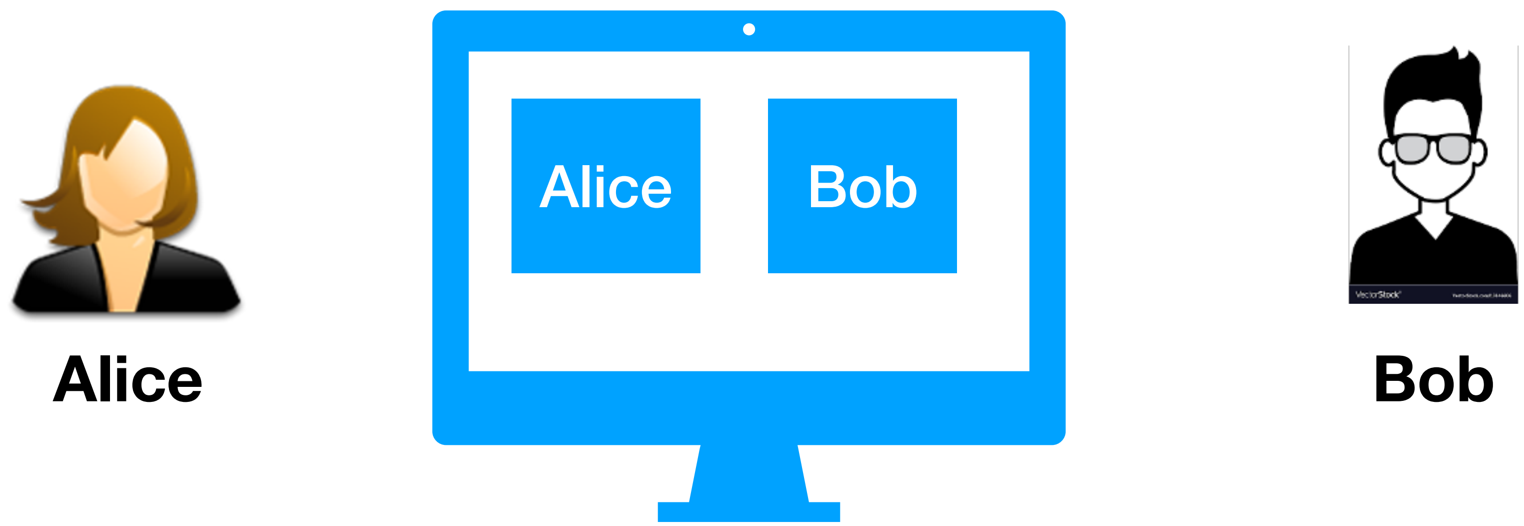


Instant Messaging

End to end Encryption

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

Secure Storage



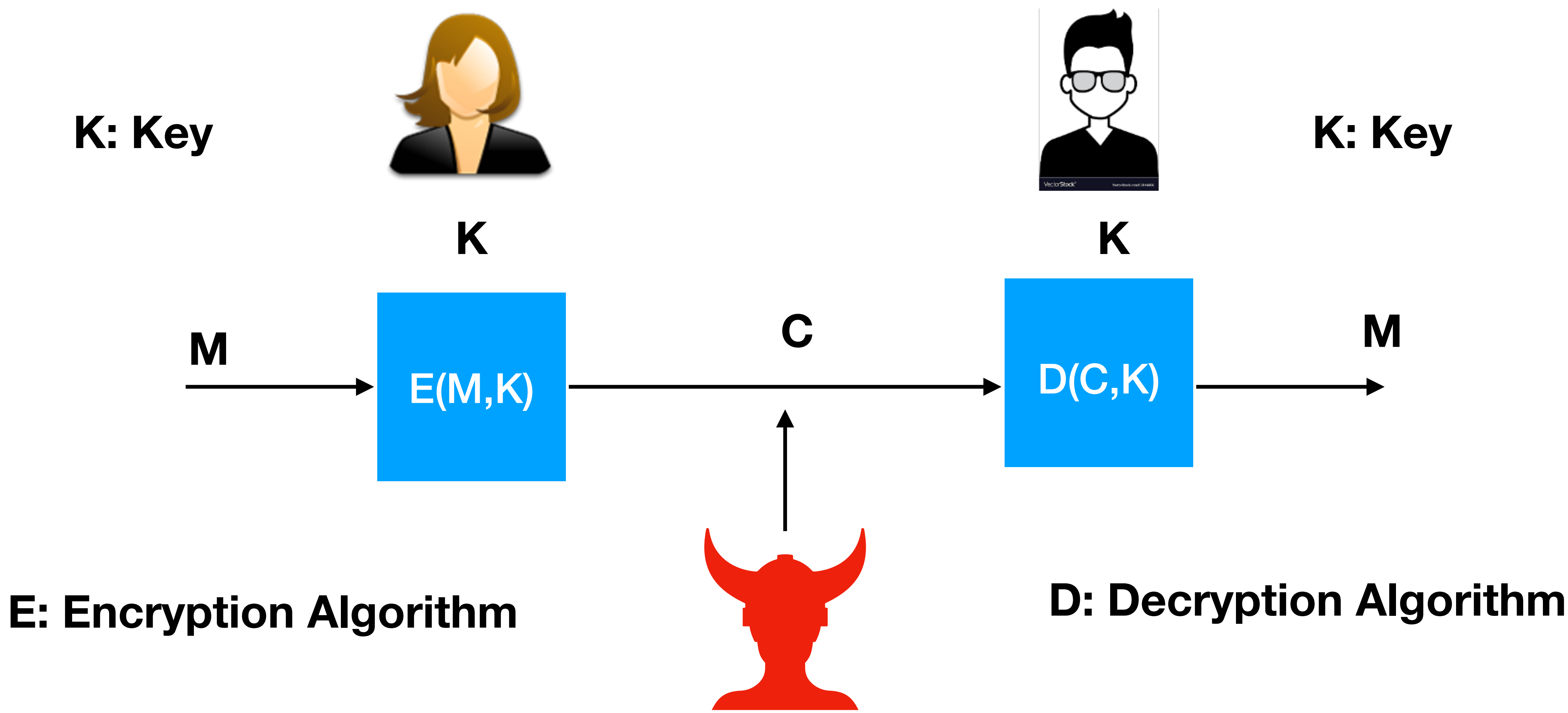
Alice’s files: No one apart from Alice can access her files or modify content
Bob’s files: No one apart from Alice can access her files or modify content

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!)

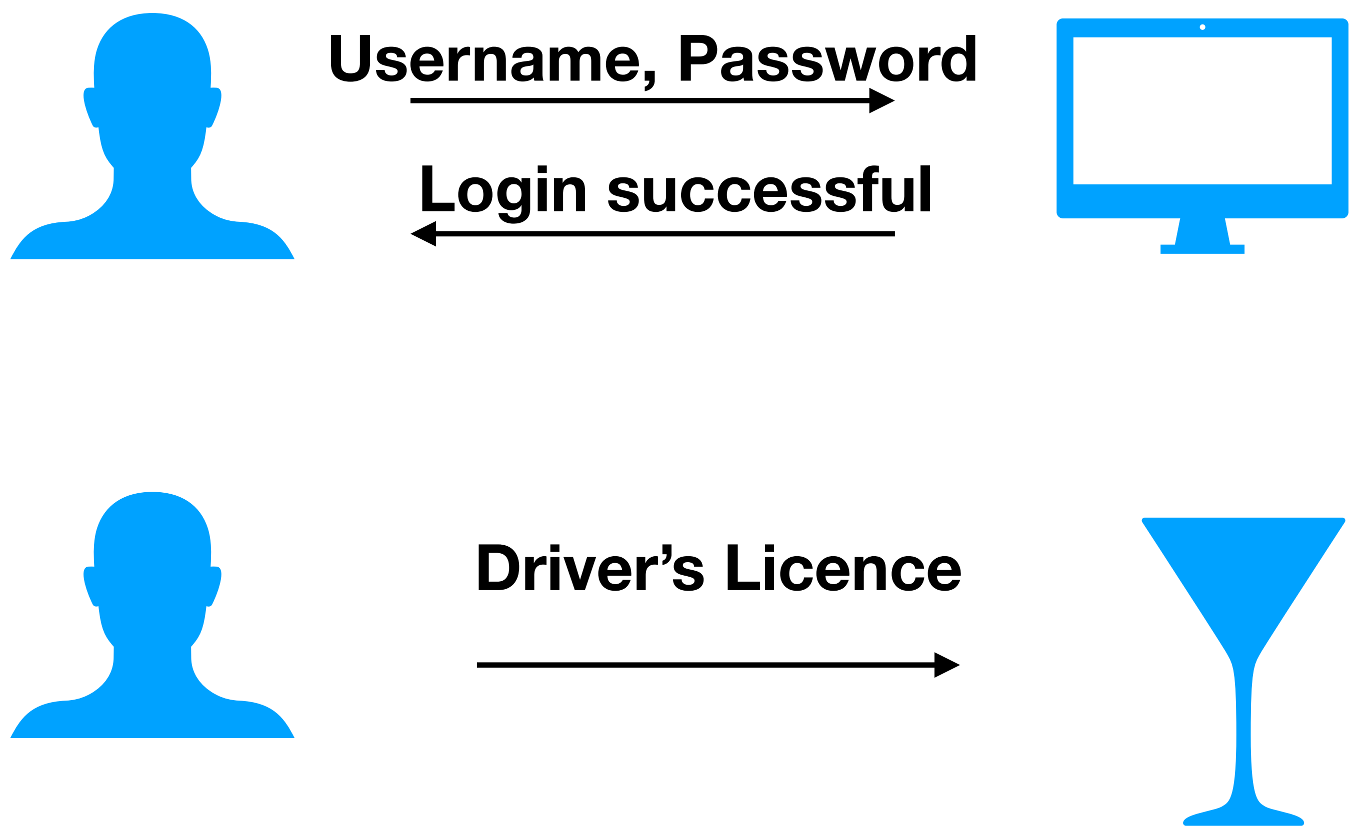
Encryption (Building Block)



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

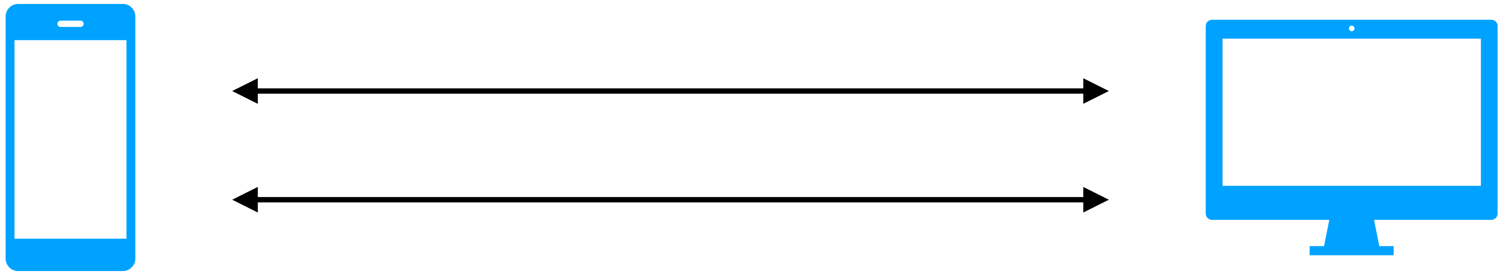
Authentication



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

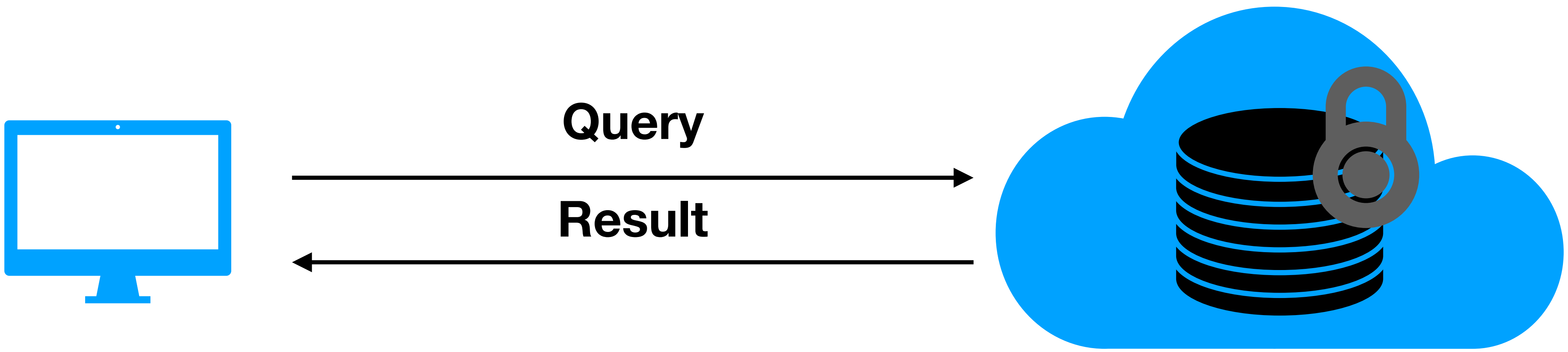
Power of Cryptography

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?

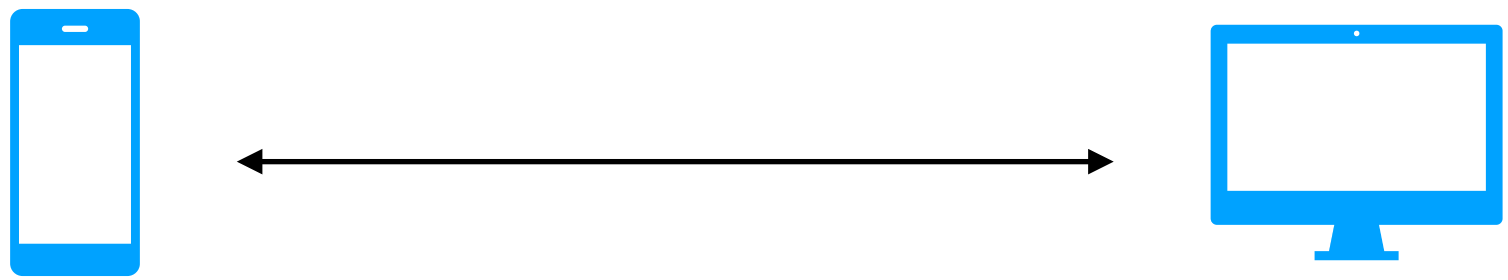
Computing on Encrypted Data



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

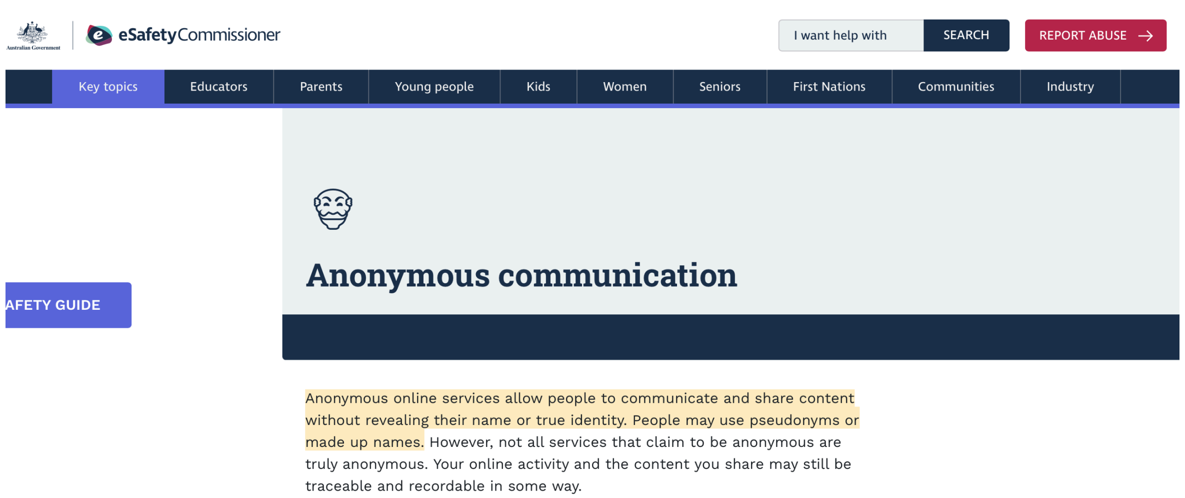
Homomorphic Encryption, Searchable Encryption : Week 10

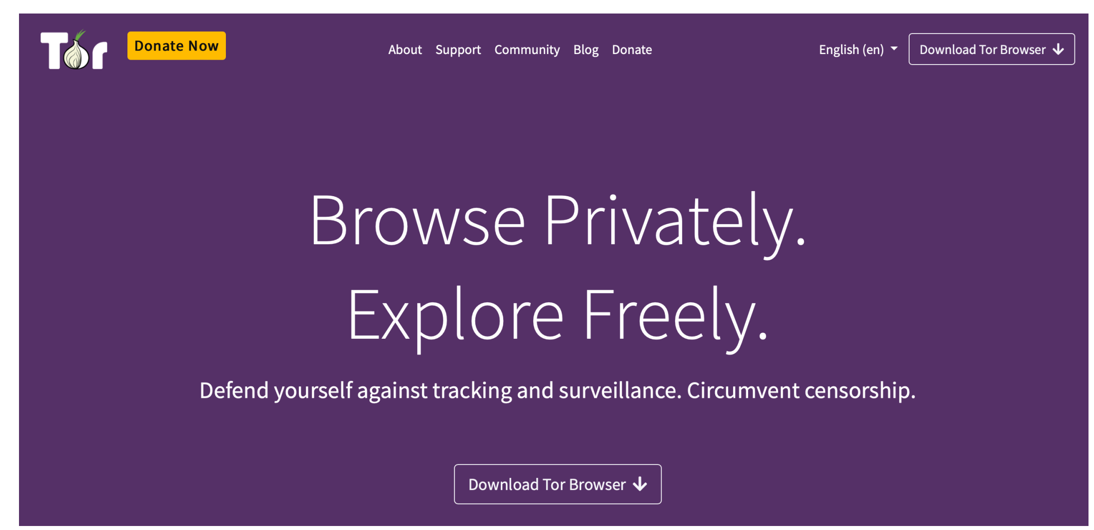
Anonymous Communication



Server does not know the IP Address

Freedom of information: Strict regime in certain countries
Anonymous Messaging: Post Without disclosing identity

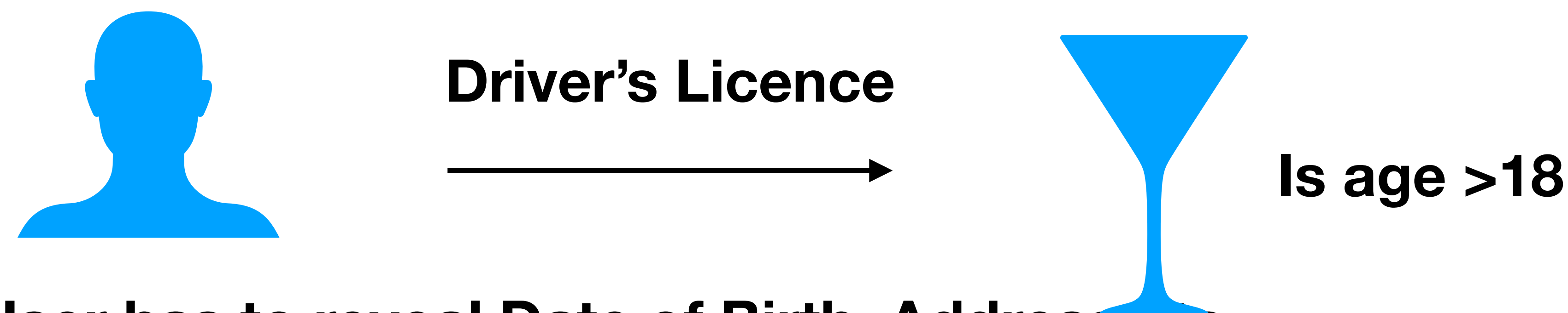




Buying on a dark web

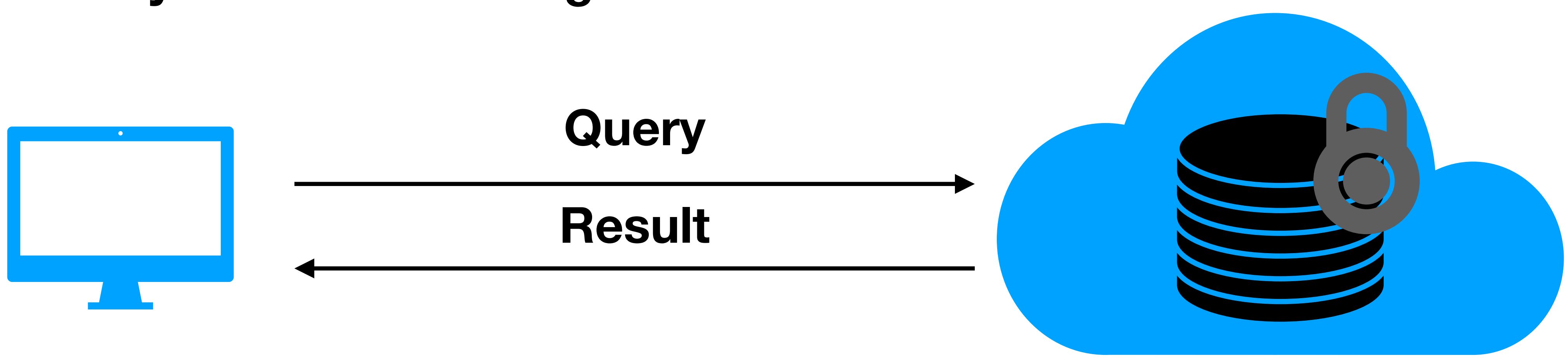
Key exchange and digital signatures: Weeks 5 and 7

Verifiability



User has to reveal Date of Birth, Address etc

Verify without revealing all information: Verifiable credentials



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

- Assigment: Submissions on Week 5 and 8
- Term Project: Submission Week 10, Friday 5 pm
- Final Exam: Closed book in-person during exam period

Assessment

- Assignment 1 and 2 released two weeks before submission
- Combination of coding and problem solving questions

Term Project

- Group projects : group size 3-5
- Should be complete, code with documentation and a report
- 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 3. 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)
- mark = ass + proj + finalExam
- grade = HD|DN|CR|PS if mark >= 50
- = FL if mark < 50 or 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 (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 Bones 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

1900 BC
Earliest known
Instance of Cryptography

100 BC
Julius Caesar
Used ciphers

Classical Ciphers

1920's **1939**
World War II

Mechanical Machines:
Enigma

1970
Modern Cryptography

Now

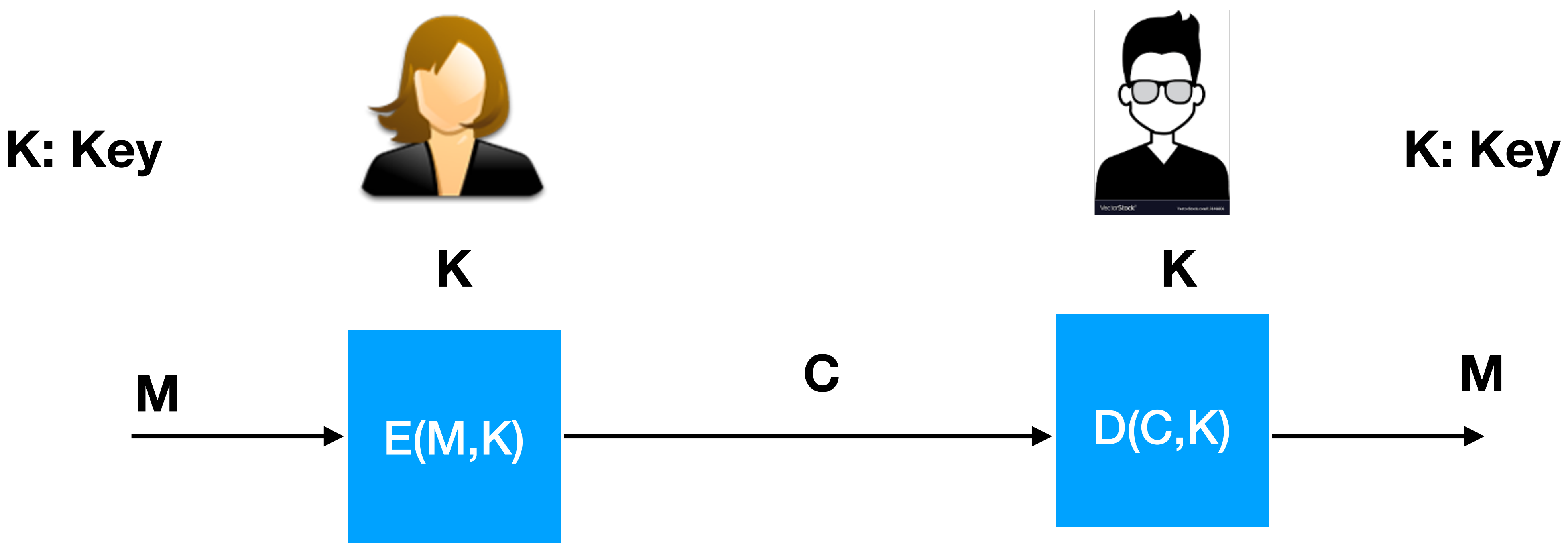
1970
IBM: DES
Data Encryption Standards

1976
Diffie Hellman
Key exchange

1977
RSA

2001
AES Standardized

Classical Ciphers

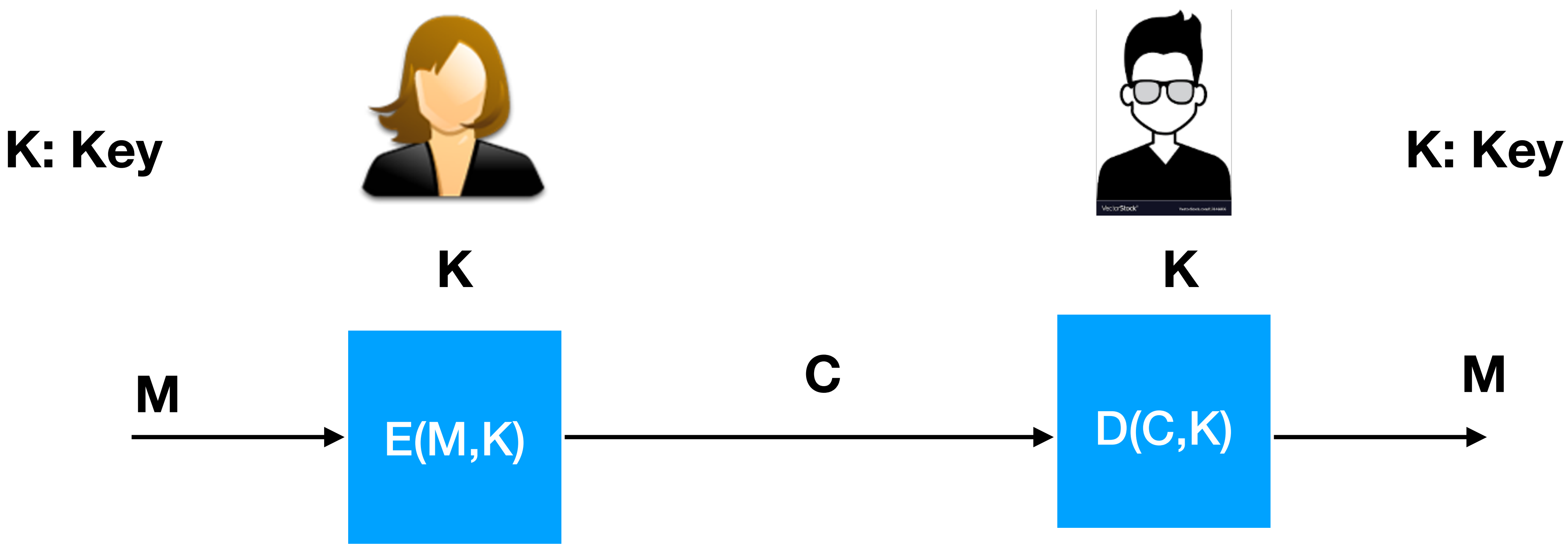


E: Encryption Algorithm

D: Decryption Algorithm

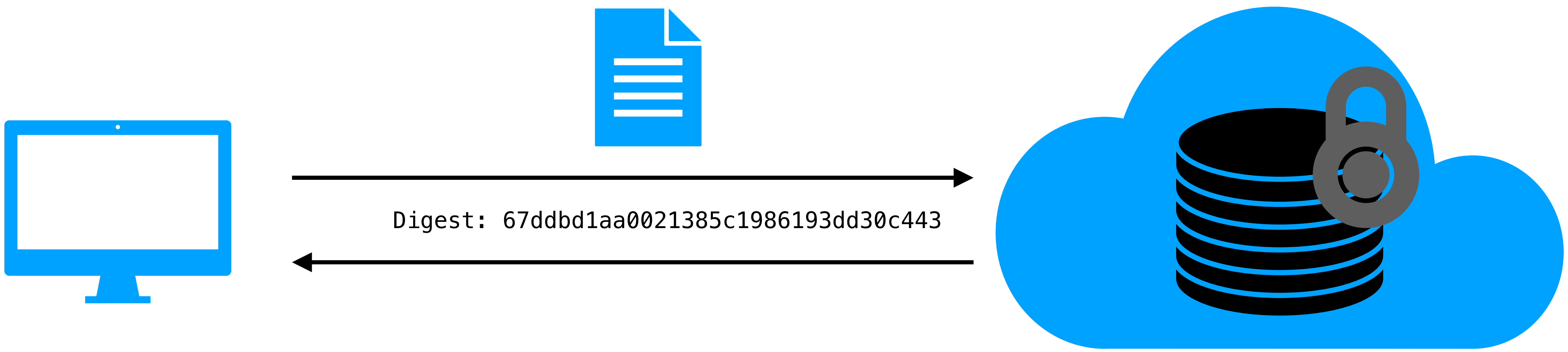
E and D Very simple functions
Simple substitution, permutation

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

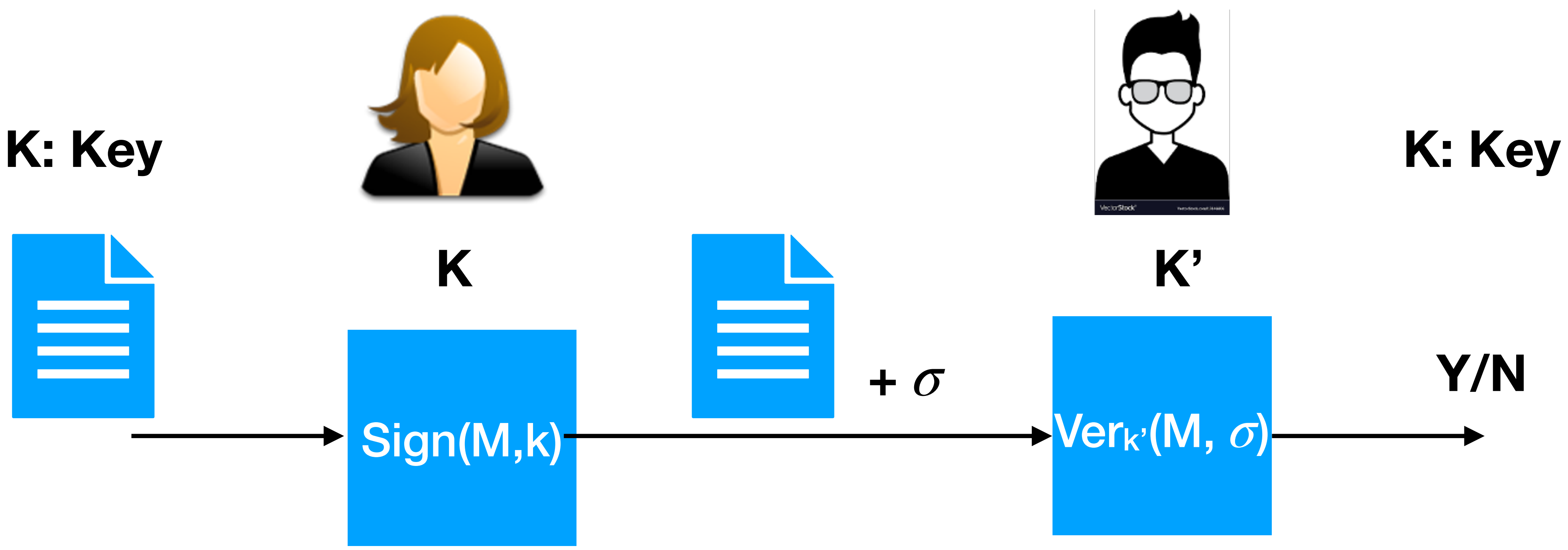


Hash Functions : H

$$H : \{0,1\}^* \to \{0,1\}^l$$

Week 3

Digital Signatures

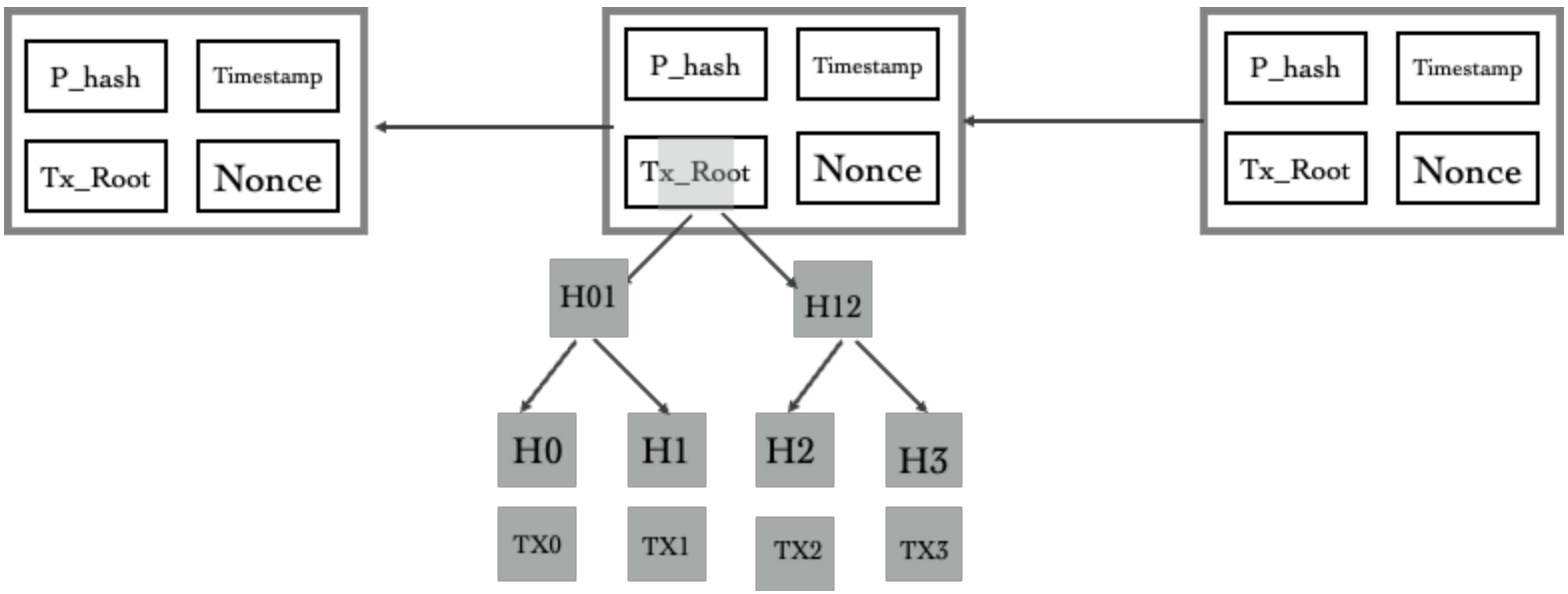


Week 7

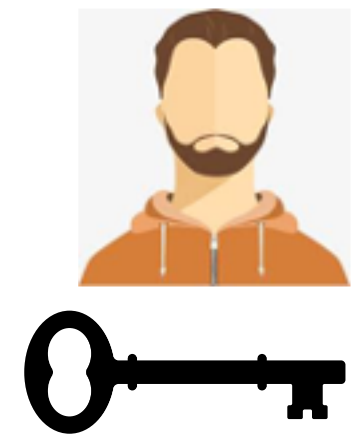
Post Quantum Cryptography

- PKC prone to attacks by Quantum Computers
- How to design new algorithms that are resilient to quantum threats?
- Week 10

Blockchains



Secret Sharing & Cloud Cryptography



At least 2 out of 3 keys are required to open the vault

Threshold Cryptography: Threshold Signatures
Multi-sig wallets etc

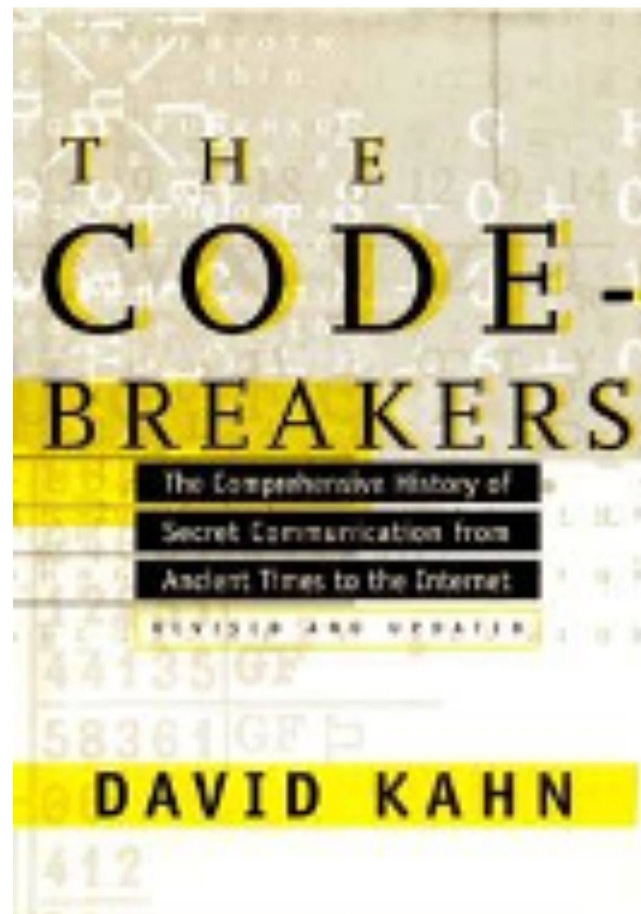
Week 9

Applications

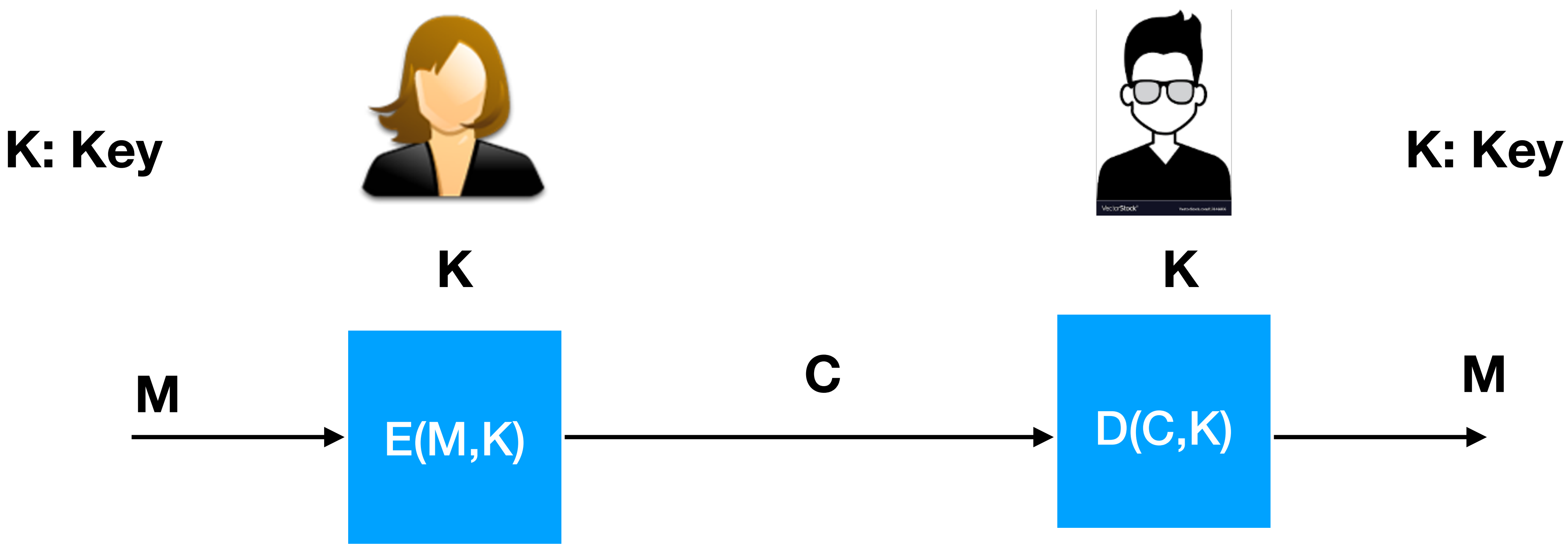
- Secret Sharing
- Secure Communication
- Secure Computation
- Blockchains
- Verifiable credentials
- E-voting

Classical Ciphers

The Codebreakers



Classical Ciphers

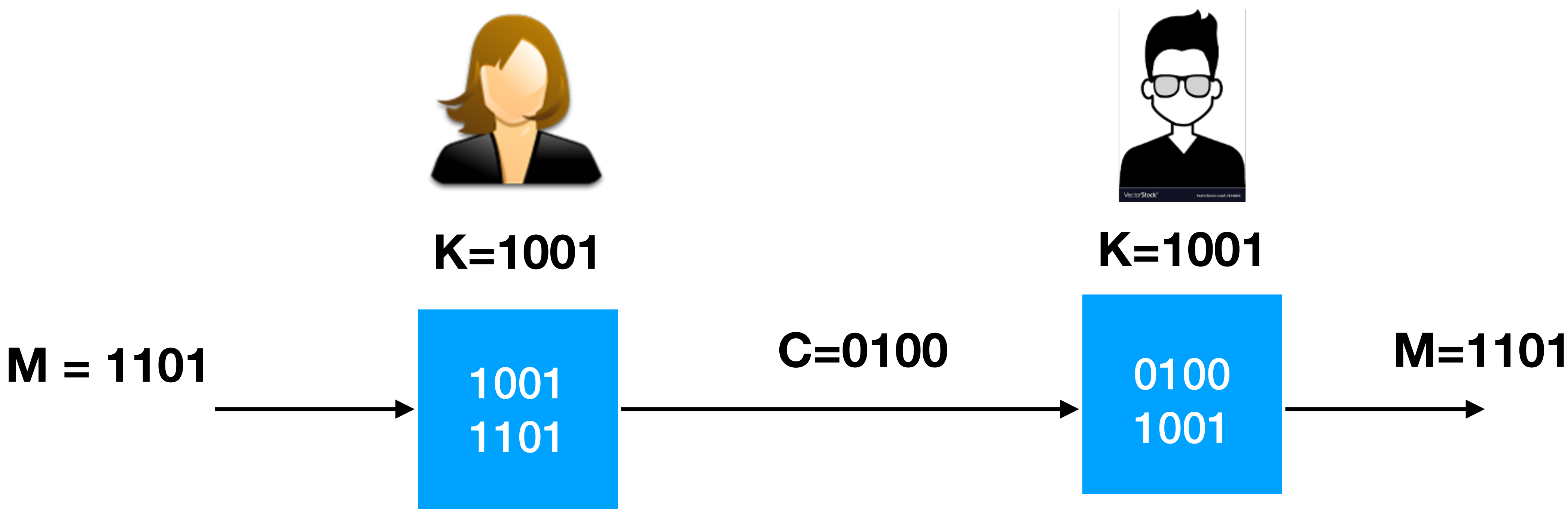


E: Encryption Algorithm

D: Decryption Algorithm

E and D Very simple functions
Simple substitution, permutation

Simple Encryption: XOR



E: Encryption Algorithm : $M \oplus K$

D: Decryption Algorithm: $C \oplus K$

E and D Very simple functions
Simple substitution, permutation

Modular Arithmetic

- $E(M, K) = (M + K) \bmod n$
- $D(C,K) = (C - K) \bmod n$
- $M = 5$, $K = 10$, $n = 13$, $C = 2$
- $D(2, 10) = -8 \bmod 13 = 5$

Message Space

Previous Example

- Message Space: Set of all possible messages **$\{0,1\}^*$**
- Key Space: Set of all possible keys **$\{0,1\}^*$**
- Ciphertext Space: Set of all possible cipher texts **$\{0,1\}^*$**

Simple Ciphers: Shift Ciphers

- Message space $\mathscr{M}$, Key Space $\mathscr{K}$: Set of 26 English Alphabets. correspondence between alphabetic characters and residues modulo 26 as follows: $A \leftrightarrow 0, B \leftrightarrow 1, \cdots Z \leftrightarrow 25$
- $\mathscr{M} = \mathscr{C} = \mathscr{K} = \mathbb{Z}_{26}$
- K = 4 (say)
- C= E (M, K) = (M + K) mod 26
- D (C, K) = (C - K) mod 26
- CRYPTO -> ?

Caesar Cipher, K=3

Simple Ciphers: Substitution Ciphers

- Message space, Key Space: Set of 26 English Alphabets

K is the permutation π

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**...**
B	C	J	F	I	G	A	D	E	H	...

π^{-1}

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**...**
G	A	B	H	I	D	F	J	E	C	...

E: π **D: π^{-1}**

- M = “HEAD”
- C = ? **DIBF**

E(H,π) =π(H)=D

D(I,π) =π^{-1}(I)= E

Size of the key space = ?

Cryptanalyzing Substitution Cipher

- Most common letters in English
- E, T, A, I, N…
- From the given text find the frequency of each alphabet
- Map with English Alphabet
- Try this
- ZRTFT IH PQFTHZ IQ ZRT XBGBOZIO HTQBZT. HTWTFBG ZRLPHBQV HLGBF HYHZTSH RBWT VTOGBFTV ZRTIF IQZTQZILQH ZL GTBWT ZRT FTEPKGIO. ZRIH HTEBFBZIHZ SLWTSTQZ, PQVTF ZRT GTBVTFHRIE LD ZRT SYHZTFILPH OLPQZ VLLAP, RBH SBVT IZ VIDDIOPGZ DLF ZRT GISIZTV QPSKTF LD CTVI AQIXRZH ZL SBIQZBIQ ETBOT BQV LFVTF IQ ZRT XBGBJY. HTQBZLF BSIVBGB, ZRT DLFSTF NPTTQ LD QBKLL, IH FTZPFQIQX ZL ZRT XBGBOZIO HTQBZT ZL WLZT LQ ZRT OFIZIOBG IHHPT LD OFTBZIQX BQ BFSY LD ZRT FTEPKGIO ZL BHHIHZ ZRT LWTFMRTGSTV CTVI

Cryptanalyzing Substitution Cipher

- Or consider pairs of letters (diagrams)
- Or triples of letters….

Vigenere Cipher

K = (2, 8, 15, 7, 4, 17)

T H I S C R Y P T O S Y S T E M I S N O T S E C U R E

C I P H E R C I P H E R C I P H E R C I P H E R C I P H

V P X Z G I A X I V W P U B T T M J P W I Z I T W Z T

Vigener Cipher

- Define $\mathscr{M} = \mathscr{C} = \mathscr{K} = (\mathbb{Z}_{26})^m$
- Let $(x_1, x_2, \cdots, x_m) \in \mathscr{M}$, $(y_1, y_2, \cdots, y_m) \in \mathscr{C}$
- For a key $K = (K_1, K_2, \cdots, K_m)$
- $E((x_1, x_2, \cdots, x_m), K) = (x_1 + k_1, x_2 + k_2, \cdots, x_m + k_m)$

  $=(y_1, y_2, \cdots, y_m)$
- $D((y_1, y_2, \cdots, y_m), K) = (y_1 - k_1, y_2 - k_2, \cdots, y_m - k_m)$

Affine Ciphers

$\mathscr{P} = \mathscr{C} = \mathscr{K} = \mathbb{Z}_{26}$ and let

$\mathscr{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : gcd(a,26) = 1\}$

For $K = (a, b) \in \mathscr{K}$, define

$y = E(x, K) = (ax + b) \bmod 26$

$D(y, K) = a^{-1}(y - b) \bmod 26$ where, $x, y \in \mathbb{Z}_{26}$

Eg: K = (7,3) , verify that this is correct.

Reading

- Stinson-Paterson, Chapter 2
- Extra Reading : Hill Cipher, Permutation Cipher

Mechanical Ciphers

Enigma Machine
(since 1930)

Thank you