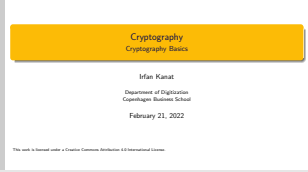
Cryptography

Cryptography Basics

Irfan Kanat

Department of Digitization
Copenhagen Business School

February 21, 2022



In this presentation we focus on cryptography basics up to symmetric key cryptography.

Big Question

- Securing information
- Past efforts
- Symmetric Key Cryptography

Big Question
- Securing information
- Past efforts
- Symmetric Key Cryptography

In this video we will learn how to secure information starting with historical efforts and ending with Symmetric Key Cryptography.

Securing Information

Securing Things

- Restrict Access
- Prevent Alterations

Securing Information is interesting.

Securing Information
Securing Things
- Restrict Access
- Prevent Alterations

Securing Information is interesting.

We all are engaged in securing things. We have doors to our houses with locks on. We have lockers with padlocks. We keep our belongings under our supervision when we are in situations where we can't control the environment.

What we do essentially is restricting access to our objects and preventing alteration of our objects. I would be very cross with you if you altered my lunch by eating it.

Information is interesting, because it is slightly different than physical objects. Unlike my lunch we can both consume the information and neither of us would be worse off. When you take information, you don't necessarily need to destroy the original. (This is the basis of a very weird argument about copyright violations being theft or not.)

Still there is value in keeping access and alteration of information in check. We employ clever technical solutions to limit access to and prevent alteration of information assets. There are whole businesses built around this idea: DRM, Cryptocurrencies, Blockchain technologies, and at the root of it all plain old encryption...

Today we will talk about encryption.

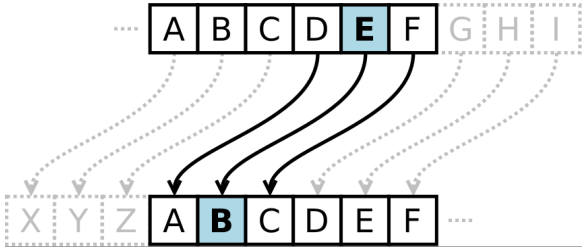
Ye Olde Encryption Schemes

Substitution

Ye Olde Encryption Schemes
Substitution

Ye Olde Encryption Schemes

Substitution



Ye Olde Encryption Schemes
Substitution

Ye Olde Encryption Schemes

Substitution

Transposition

Ye Olde Encryption Schemes
Substitution
Transposition

Ye Olde Encryption Schemes

Substitution

Transposition

6	3	2	4	1	5
L	E	T	S		H
A	V	E		C	O
F	F	E	E		A
T		T	W	O	
O	C	L	O	C	K

LETS HAVE COFFEE AT TWO OCLOCK
TESHLCEV OA EFEAFOT W TCLCOKO

Ye Olde Encryption Schemes
Substitution
Transposition
6 3 2 4 1 5
L E T S H
A V E C O
F F E E A
T T W O
O C L O C K
LETS HAVE COFFEE AT TWO OCLOCK
TESHLCEV OA EFEAFOT W TCLCOKO

Key take away, Caesar wasn't very cryptowise. There is only 26 possible keys afterall.
Simple substitution ala Caesar, and simple transposition of Spartan generals was good a thousand years ago.
The problem is these methods are open to brute force attacks or frequency analysis.
500 years ago, the most advanced crypto technology was to use polyalphabetic crypto. Having multiple substitution patterns and using a different one in round robin fashion...
These days the only place you will find these methods is the puzzle books, and mystery novels.

Cryptography Basic Idea

Scrambling information in a reversible way

Scrambled information looks like gibberish

Cryptography Basic Idea
Scrambling information in a reversible way
Scrambled information looks like gibberish

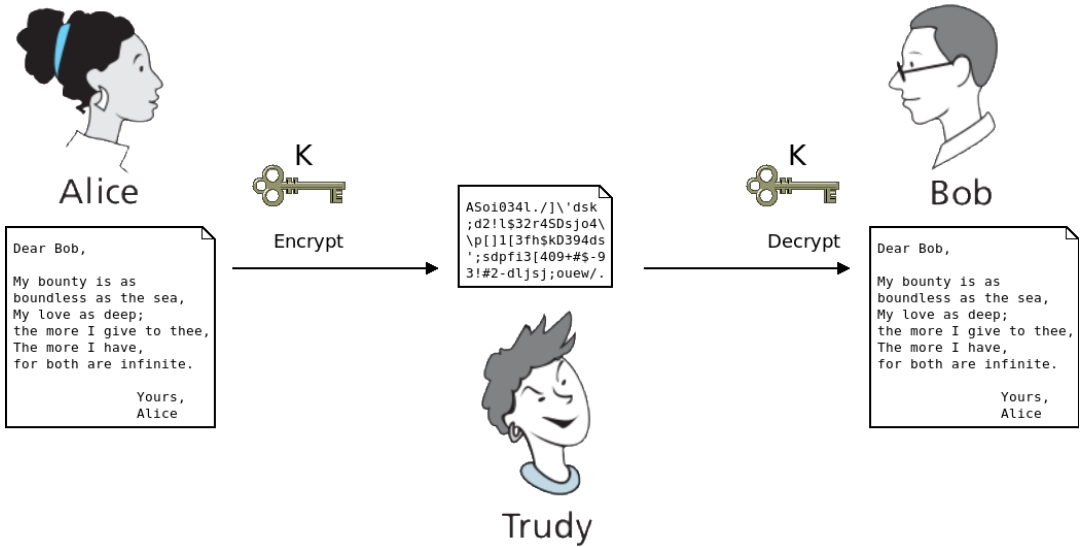
Cryptography Basic Idea

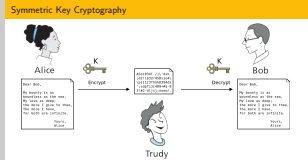
Cryptography Basic Idea

It is easy to imagine messages written on paper, but often it is harder to imagine what is happening to digital data in the computer.

A useful analogy is to imagine data being locked in a box. Locked with a key and unlocked with a copy of the same key.

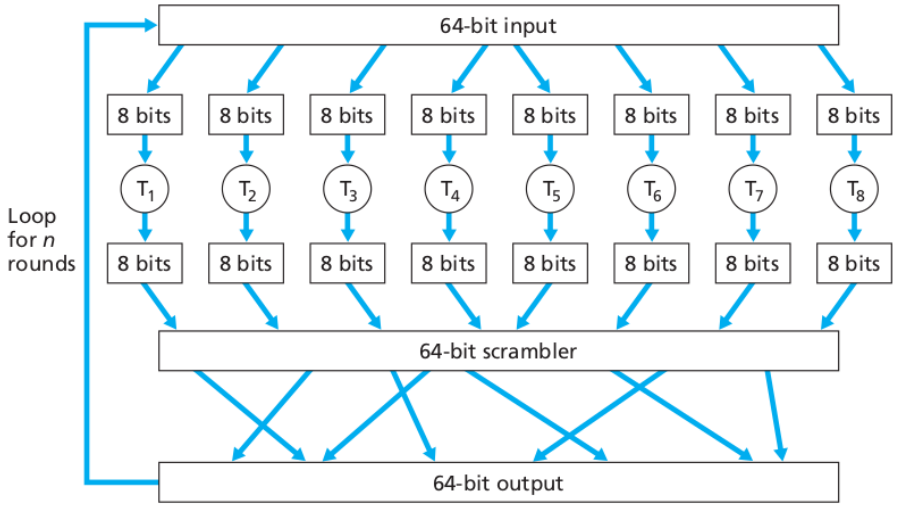
Symmetric Key Cryptography

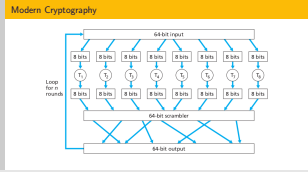




If Alice and Bob have met before and shared a key,
Then they can encrypt and decrypt their messages without Trudy getting any wiser.
A single key both locks and unlocks the box and reveals the tender words of our lovers.

Modern Cryptography





With computers, bruteforcing immense numbers of trials became feasible.
This brought out a need for crypto systems with much larger solution spaces.
Idea is computer can iterate over a crypto algorithm many times more complex than what people can.
Above is a block cipher example like that of DES. Data is broken into blocks (of 8bits) and each block is processed by a different function to produce a different 8 bit block. The resulting blocks are scrambled and process repeated. After several iterations input bits will go through many different functions, resulting in end results that are vastly different from inputs.
The DES algorithm (now defunct) used 56bit keys with 64bit blocks.
AES uses larger block and key sizes (128, 256, 1024).
If you were to brute force DES, it would require you to feed each of the possible keys ($2^{54} = 72057594000000000$) to the decryption algorithm. While this may appear difficult, breaking DES is trivial for modern computers.
YET, the difficulty is exponential. If a computer can break 56bit keys in 1 seconds, it would take the same computer 149 trillion years to break a 128bit key and today we routinely use keys of

What Does Cryptography Look Like Really?

Goal here is to show the difference between cipher and clear text so the students can sort of get what is being done.
You can say that you were touring Kronborg castle up near Helsingor and intercepted the message from the guards
There is an encrypted cipher.txt file in the demo folder of this module.
Show what is in the file:
cat cipher.txt # Or simply open with a text editor
The file is gibberish, doesn't make sense
Decrypt the file
openssl enc -des-ecb -d -in cipher.txt -K 1234 > recovered.txt
Show what was recovered
cat recovered.txt

Symmetric Key Cryptography

Light weight

Straight forward

Data at rest

Symmetric Key Cryptography
Light weight
Straight forward
Data at rest

Symmetric key cryptography is light weight compared to asymmetric key cyrptography.
Can be done faster.
Easy to use without much hassle.
Ideal for data at rest. That is data that is being stored for local use.
Personally identifiable data (PID) of users are often encrypted this way.

Recap

- Securing data
- Past efforts
- Symmetric Key Cryptography

Recap
- Securing data
- Past efforts
- Symmetric Key Cryptography

Internet is a jungle. It can be beautiful but you need to watch out for yourself. Things you do online have consequences IRL.