

Cryptography

Cryptography Basics

Irfan Kanat

Department of Digitization
Copenhagen Business School

February 21, 2022

This work is licensed under a Creative Commons Attribution 4.0 International License.



Irfan Kanat (CBS) Cryptography February 21, 2022 1 / 10

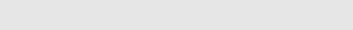
2022-02-21

Cryptography

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

Irfan Kanat
Department of Digitization
Copenhagen Business School
February 21, 2022

This work is licensed under a Creative Commons Attribution 4.0 International License.



Big Question

- Securing information
- Past efforts
- Symmetric Key Cryptography

2022-02-21

Cryptography

Big Question

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

Big Question

- Securing information
- Past efforts
- Symmetric Key Cryptography

Irfan Kanat (CBS)

Cryptography

February 21, 2022

2 / 10

Securing Information

Securing Things

- Restrict Access
- Prevent Alterations

Securing Information is interesting.



Cryptography

2022-02-21

Securing Information

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.

Securing Information

- Restrict Access
- Prevent Alterations

Securing Information is interesting.



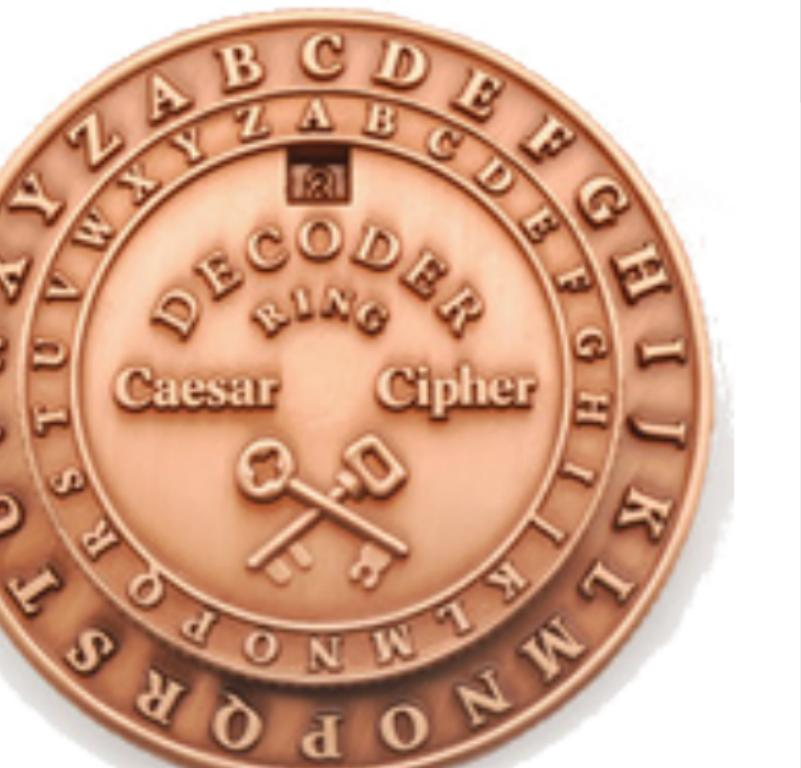
Irfan Kanat (CBS)

Cryptography

February 21, 2022

3/10

Ye Olde Encryption Schemes



The image shows a circular brass-style decoder ring for the Caesar Cipher. It features concentric rings of letters. The innermost ring has the word "Caesar" at the bottom and "Cipher" at the top. Above these, it says "DECODER" and "RING". A small square in the center contains the number "III". Below the rings, there are two crossed keys.

Substitution

2022-02-21

Cryptography

Ye Olde Encryption Schemes

Cryptography

Ye Olde Encryption Schemes

Substitution



Ye Olde Encryption Schemes

Cryptography

2022-02-21

Substitution

The diagram illustrates a substitution cipher. At the top, a sequence of letters A, B, C, D, E, F, G, H, I is shown in a row of boxes. The letter E is highlighted with a blue background. Below it, another sequence of letters X, Y, Z is shown in a row of boxes. The letter B is highlighted with a blue background. Arrows point from the letters A, B, C, D, E, F at the top to the corresponding letters X, Y, Z at the bottom. Specifically, A maps to X, B maps to Y, C maps to Z, D maps to X, E maps to Y, F maps to Z, and G, H, I map to themselves. This represents a substitution mapping where each letter in the plaintext is replaced by a different letter in the ciphertext.

Cryptography

Ye Olde Encryption Schemes

Substitution

This diagram shows a substitution mapping between two sets of letters. The top set contains A, B, C, D, E, F, G, H, I, with E highlighted. The bottom set contains X, Y, Z, with B highlighted. Arrows indicate the mapping: A to X, B to Y, C to Z, D to X, E to Y, F to Z, and G, H, I to themselves. This is a classic monoalphabetic substitution cipher where each letter is mapped to a single, fixed letter in the ciphertext.

Irfan Kanat (CBS)

Cryptography

February 21, 2022

4 / 10

Ye Olde Encryption Schemes

Substitution

Transposition



Cryptography

2022-02-21

Cryptography

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

LET'S HAVE COFFEE AT TWO OCLOCK
TESHLCEV OA EFEAFOT W TCLCOKO

Cryptography

2022-02-21

Ye Olde Encryption Schemes

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

Ye Olde Encryption Schemes

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

LET'S HAVE COFFEE AT TWO OCLOCK
TESHLCEV OA EFEAFOT W TCLCOKO

Cryptography Basic Idea

Scrambling information in a reversible way
Scrambled information looks like gibberish

Cryptography

2022-02-21

- └ Cryptography Basic Idea

Cryptography Basic Idea

Scrambling information in a reversible way
Scrambled information looks like gibberish

Cryptography Basic Idea



2022-02-21

Cryptography

Cryptography Basic Idea

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

Alice's message to Bob:

Dear Bob,
My bounty is as boundless as the sea,
My love as deep;
the more I give to thee,
The more I have,
for both are infinite.
Yours,
Alice

Encrypted message (seen by Trudy):

```
ASoi034l./]\`dsk
;d2!l$32r4SDsjo4\
\p[]1[3fh$kD394ds
';sdpfI3[409+#$-9
3!#2-dljsj;ouew/.
```

Decrypted message (seen by Bob):

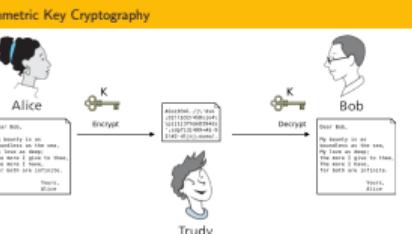
Dear Bob,
My bounty is as boundless as the sea,
My love as deep;
the more I give to thee,
The more I have,
for both are infinite.
Yours,
Alice

Trudy's attempt to decrypt:

Cryptography

2022-02-21

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

Cryptography

2022-02-21

Modern Cryptography

The diagram illustrates a block cipher process. It starts with a **64-bit input** which is divided into eight 8-bit blocks. These blocks are processed through a series of eight functions, T_1 through T_8 , each producing a new 8-bit block. The output of these functions is then fed into a **64-bit scrambler**. The final output is a **64-bit output**. A large bracket on the left indicates a **Loop for n rounds**, where the entire process (functions and scrambler) is repeated for each of the eight rounds.

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.

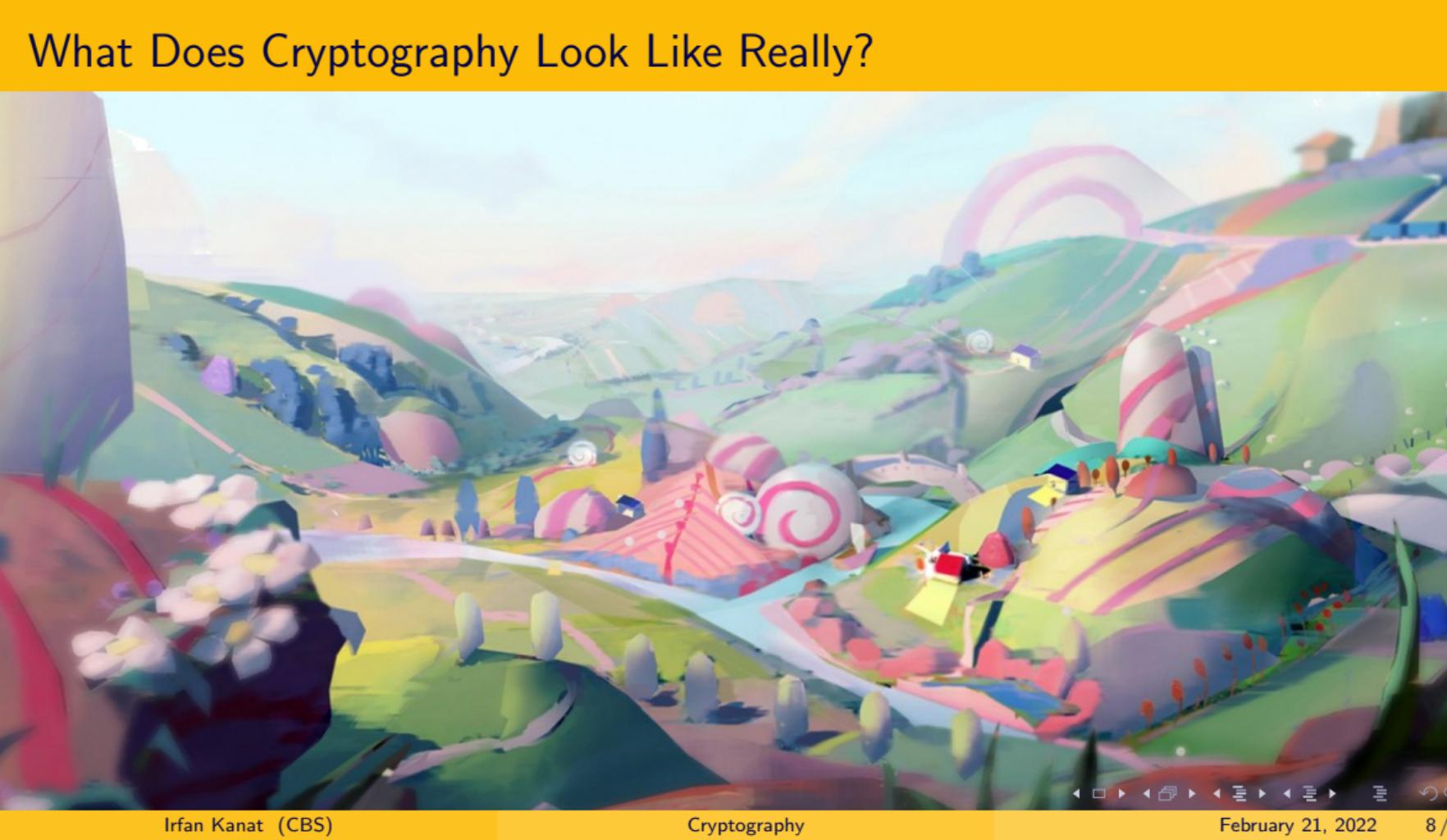
The DES algorithm (now defunct) used 56bit keys with 64bit blocks.

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

7/10



What Does Cryptography Look Like Really?

2022-02-21

Cryptography

└ 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 Helsingør 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`

Irfan Kanat (CBS)

Cryptography

February 21, 2022

8 / 10

What Does Cryptography Look Like Really?

Light weight

Straight forward

Data at rest

2022-02-21

└ Symmetric Key Cryptography

Symmetric key cryptography is light weight compared to asymmetric key cryptography.
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.

Light weight
Straight forward
Data at rest

- Securing data
 - Past efforts
 - Symmetric Key Cryptography

Recap

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