

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.

Big Question

- Securing information
- Past efforts
- Symmetric Key Cryptography

Securing Information

Securing Things

- Restrict Access
- Prevent Alterations

Securing Information is interesting.



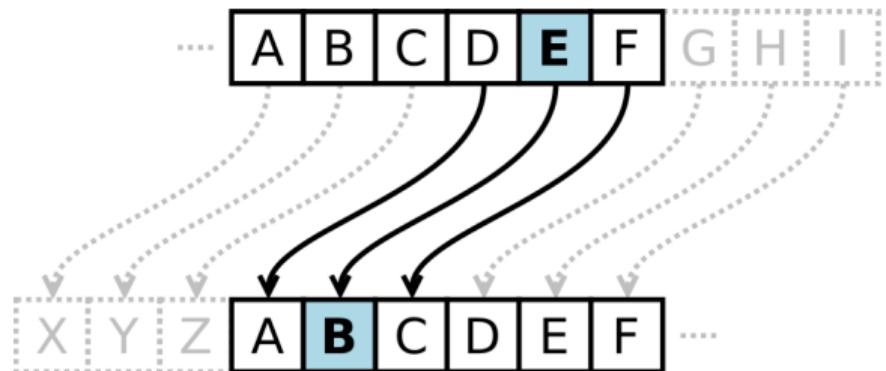
Ye Olde Encryption Schemes

Substitution



Ye Olde Encryption Schemes

Substitution



Ye Olde Encryption Schemes

Substitution

Transposition



Ye Olde Encryption Schemes

Substitution

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

Transposition

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 Basic Idea



Symmetric Key Cryptography



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



Encrypt

ASoi034l./]\`dsk
;d2!l\$32r4SDsjo4\
\p[]1[3fh\$kD394ds
';sdpf13[409+#\$-9
3!#2-dljsj;ouew/.



Decrypt

Dear Bob,

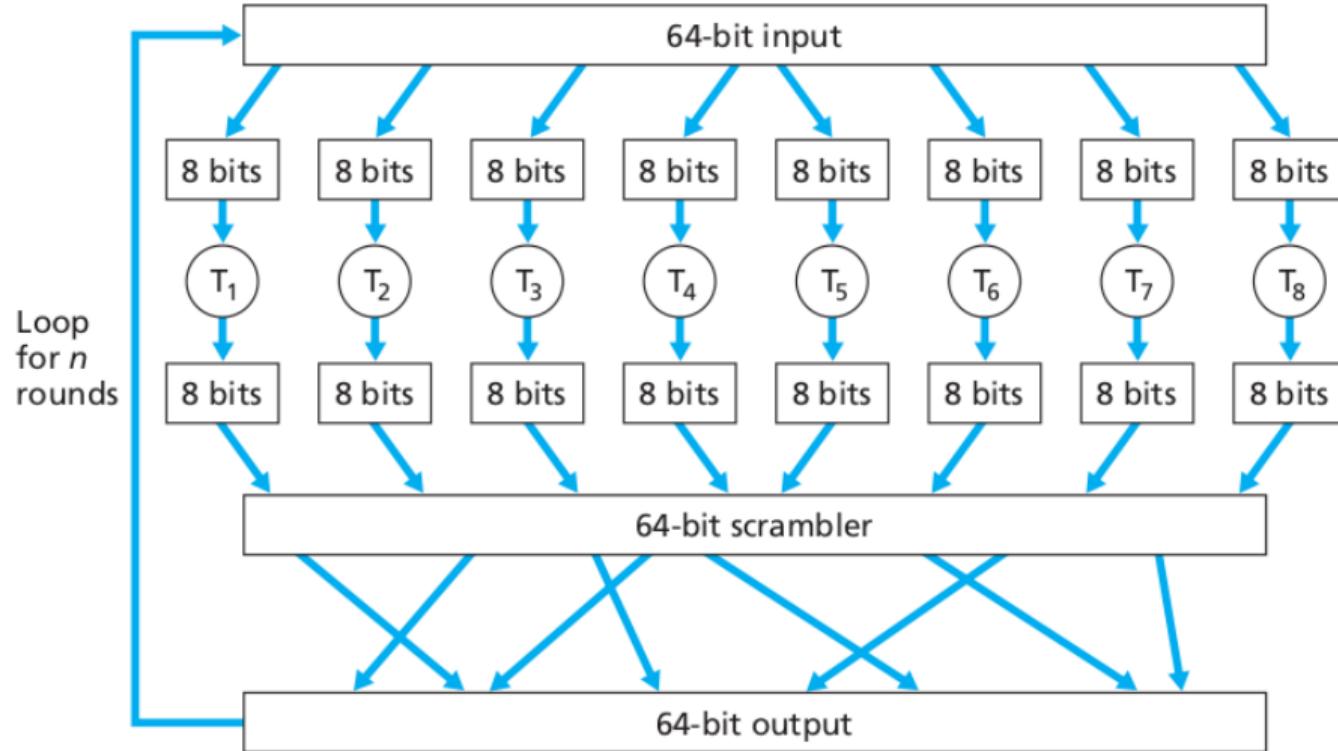
My bounty is as boundless as the sea,
My love as deep;
the more I give to thee,
The more I have,
for both are infinite.

Yours,
Alice



Trudy

Modern Cryptography



What Does Cryptography Look Like Really?



Symmetric Key Cryptography

Light weight

Straight forward

Data at rest

- Securing data
- Past efforts
- Symmetric Key Cryptography