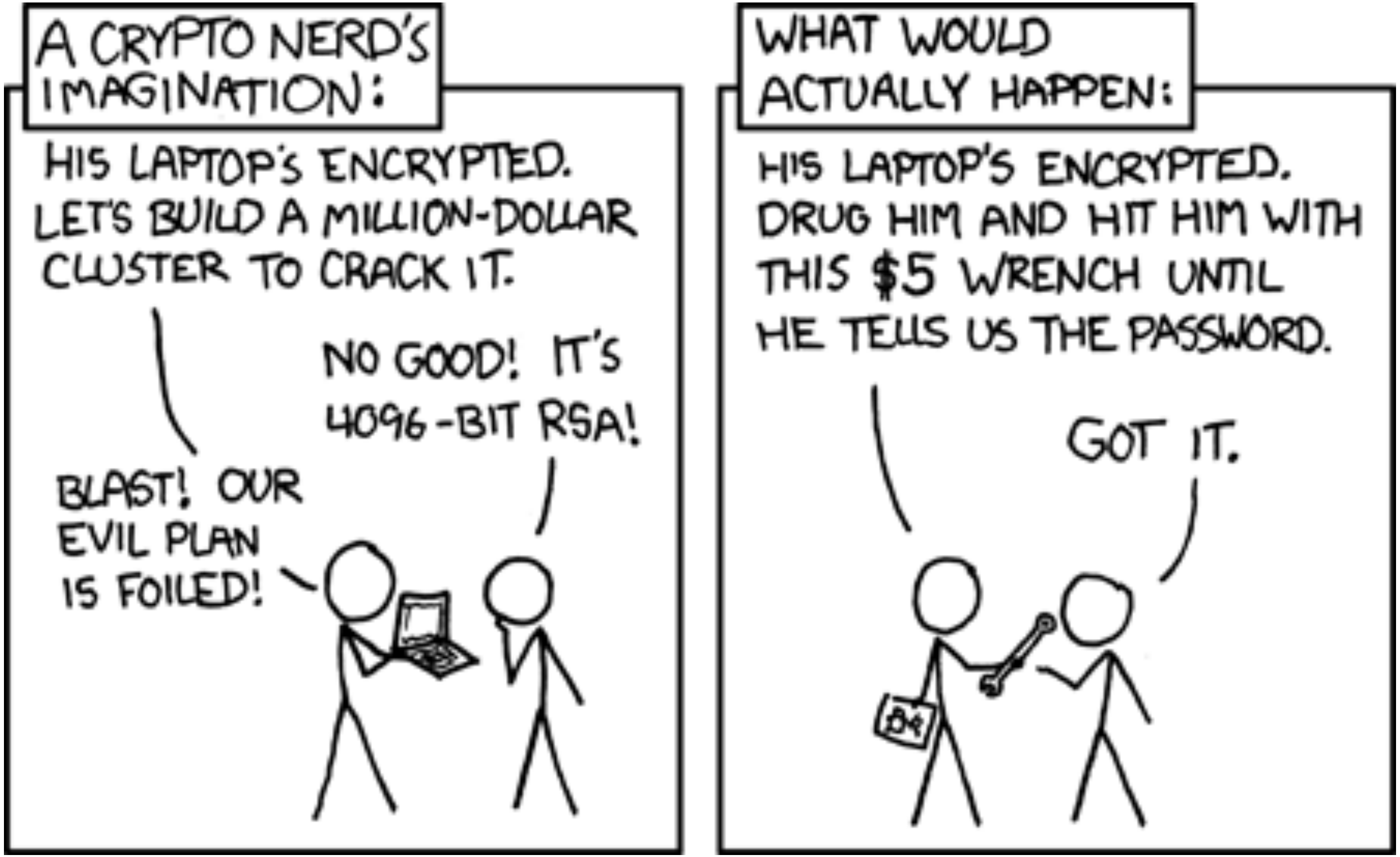
# Essentials of Encryption

Diego Ferigo


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

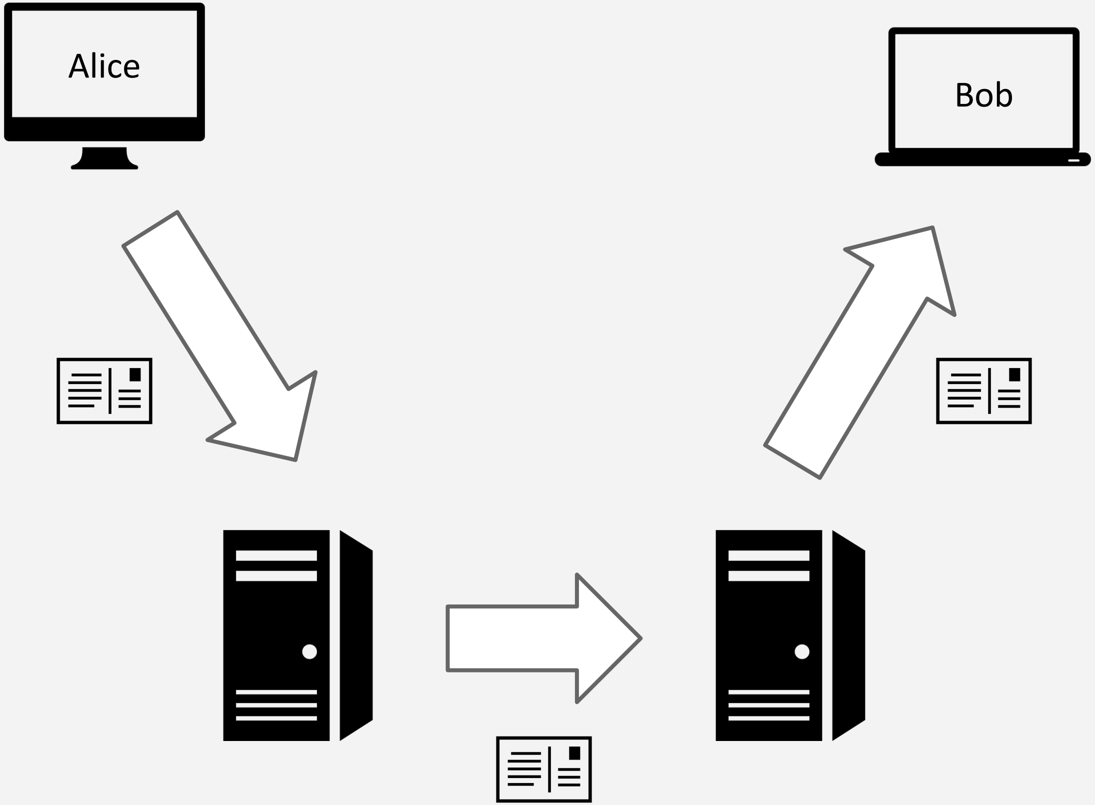
## Points of Failure

Blocchi / Flusso

Basic: login password

Simmetrica

Asimmetrica


Alice
Bob

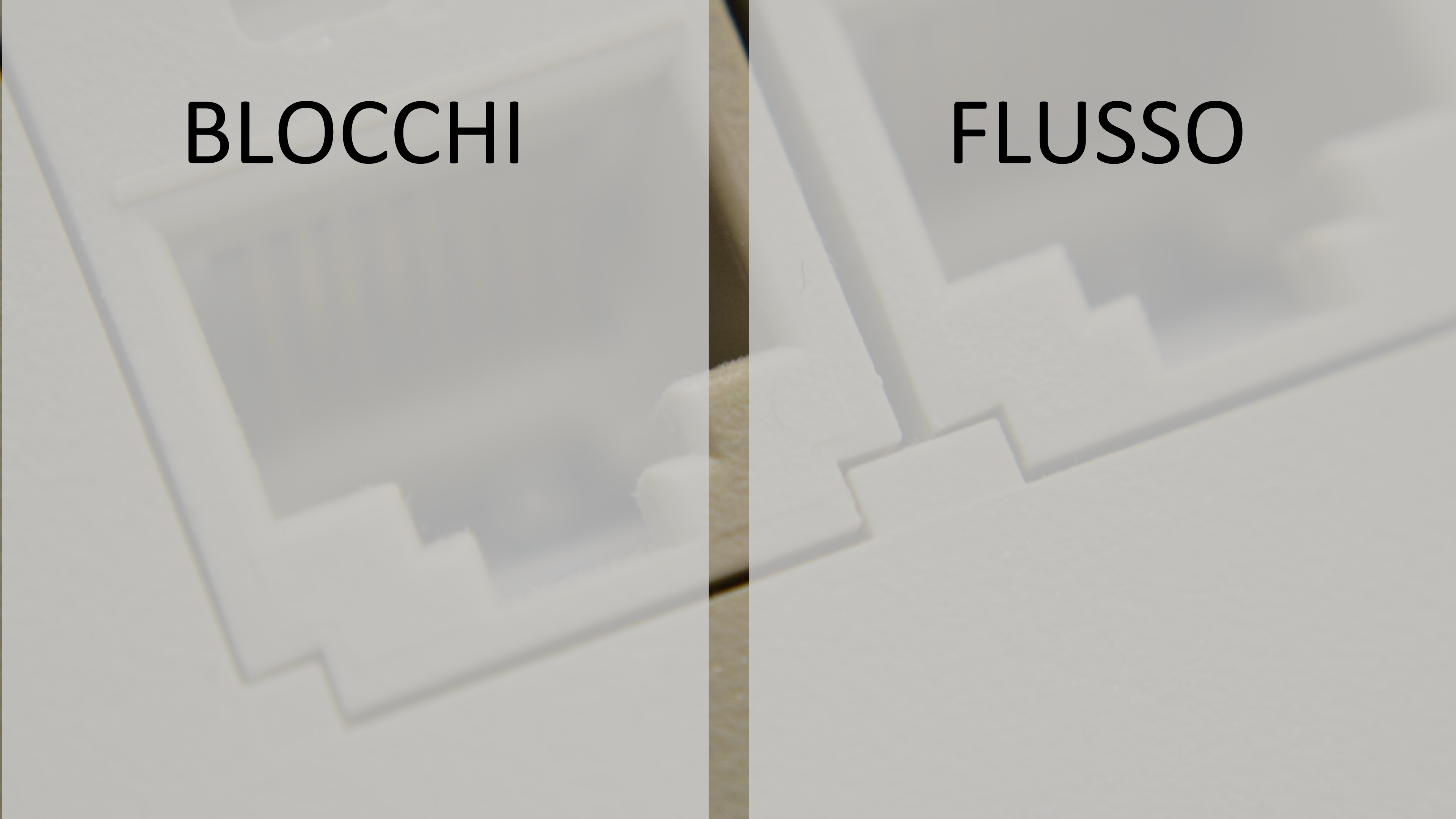
Points of Failure

Blocchi / Flusso

Basic: login password

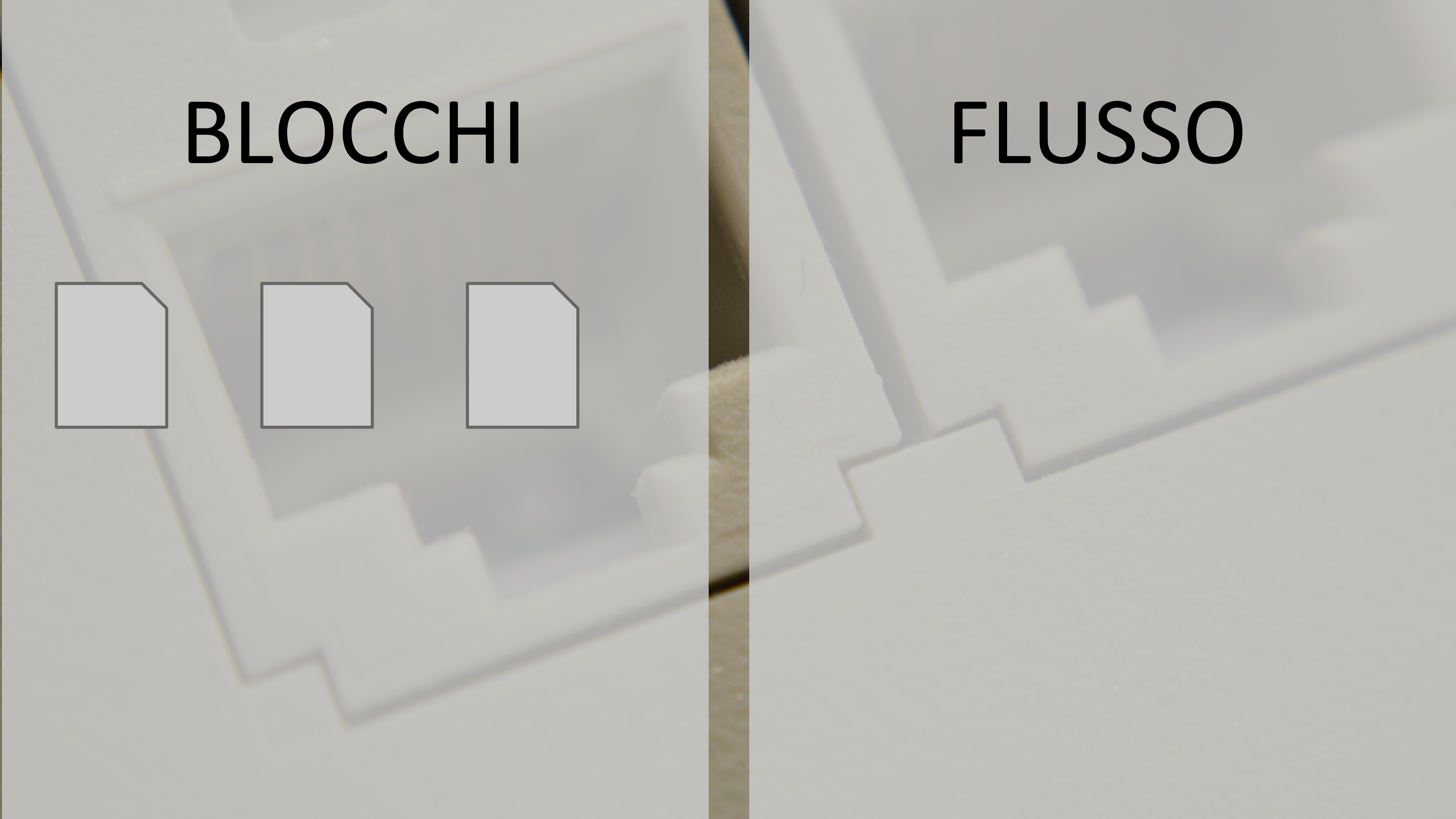
Simmetrica

Asimmetrica



BLOCCHI

FLUSSO



## BLOCCHI

## FLUSSO

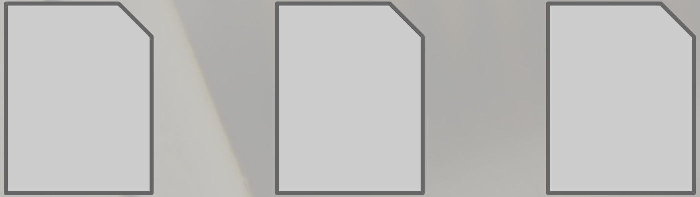
## BLOCCHI

Lunghezza finita

Adatti per FILE

## FLUSSO

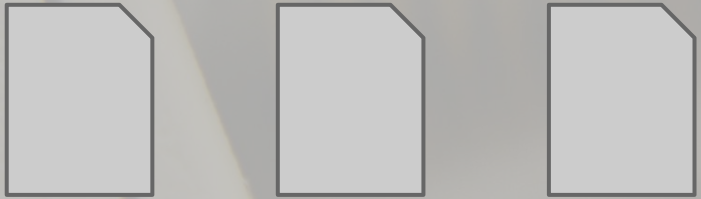
# BLOCCHI



Lunghezza finita
Adatti per FILE

# FLUSSO

# BLOCCHI



Lunghezza finita
Adatti per FILE

# FLUSSO

Lunghezza variabile
Adatti per STREAM

Points of Failure

Blocchi / Flusso

Basic: login password

Simmetrica

Asimmetrica

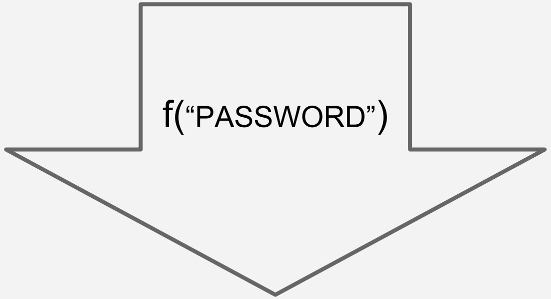
LOGIN

LOGIN

> PASSWORD

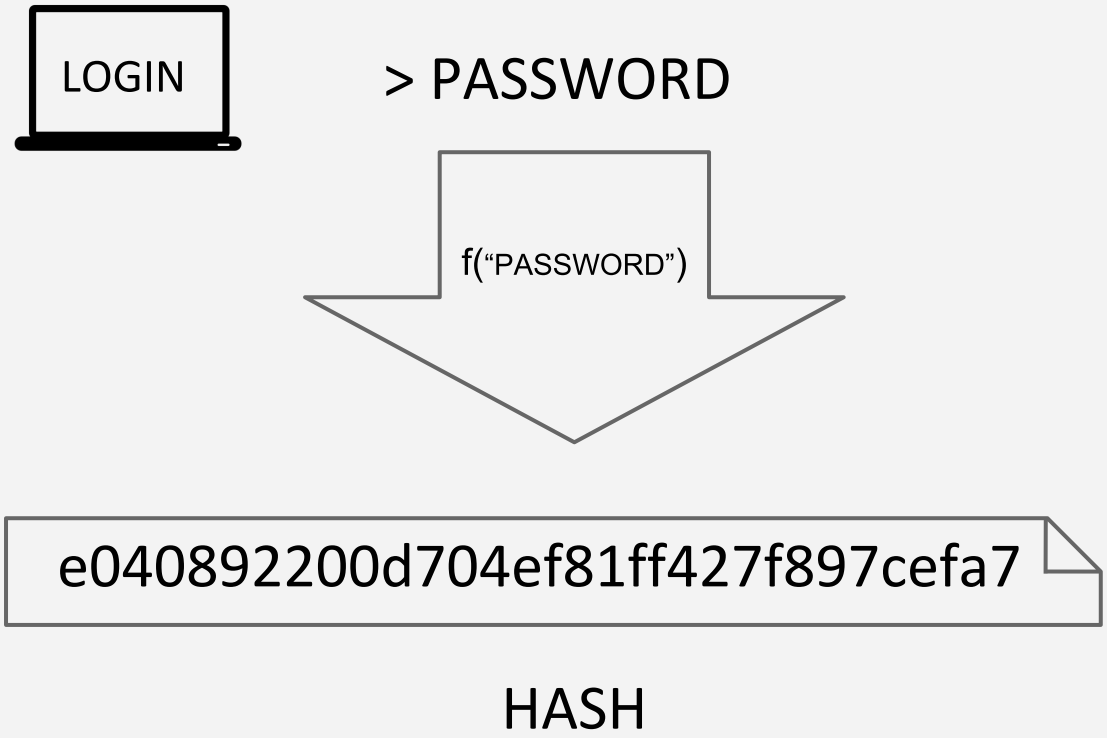
LOGIN

> PASSWORD



f(“PASSWORD”)

e040892200d704ef81ff427f897cefa7



LOGIN

> PASSWORD

f(“PASSWORD”)

e040892200d704ef81ff427f897cefa7

HASH

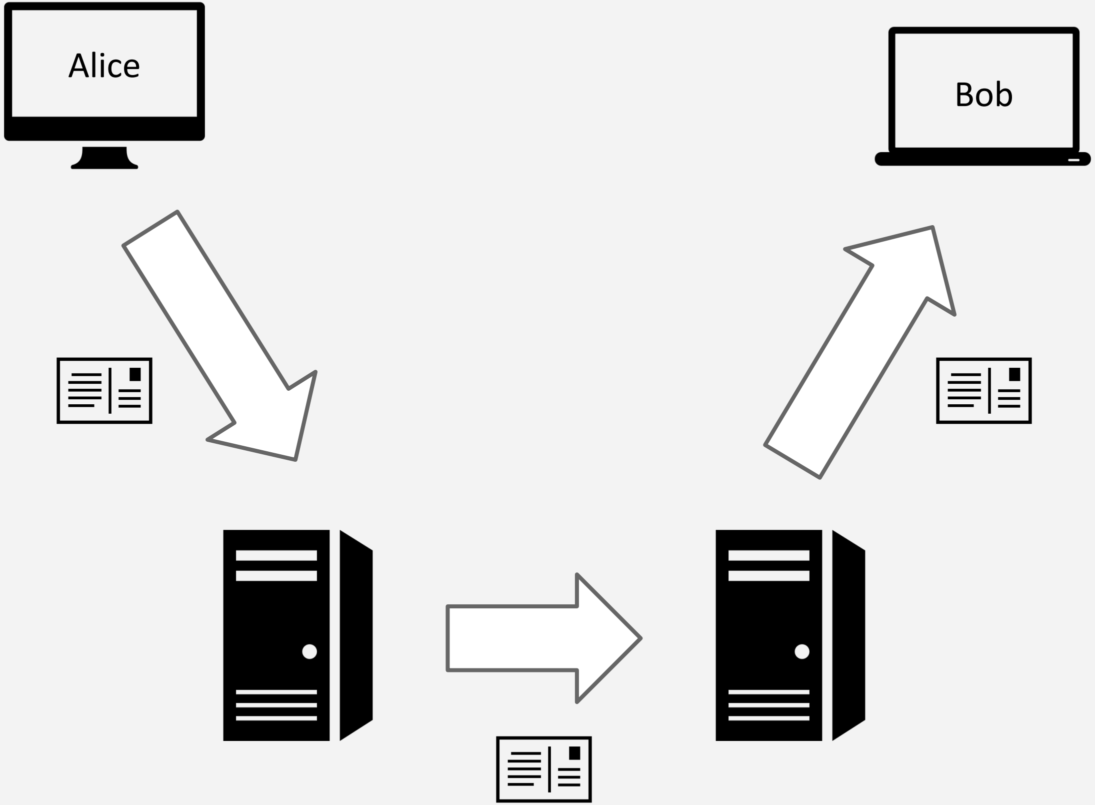
Points of Failure

Blocchi / Flusso

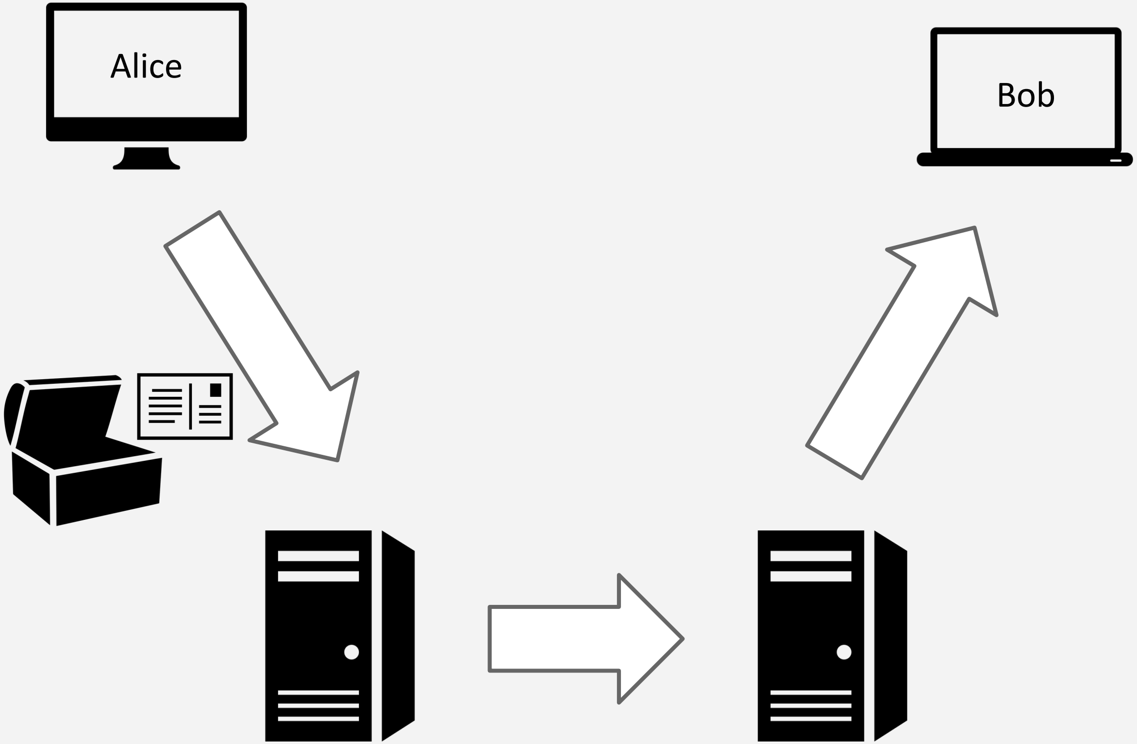
Basic: login password

Simmetrica

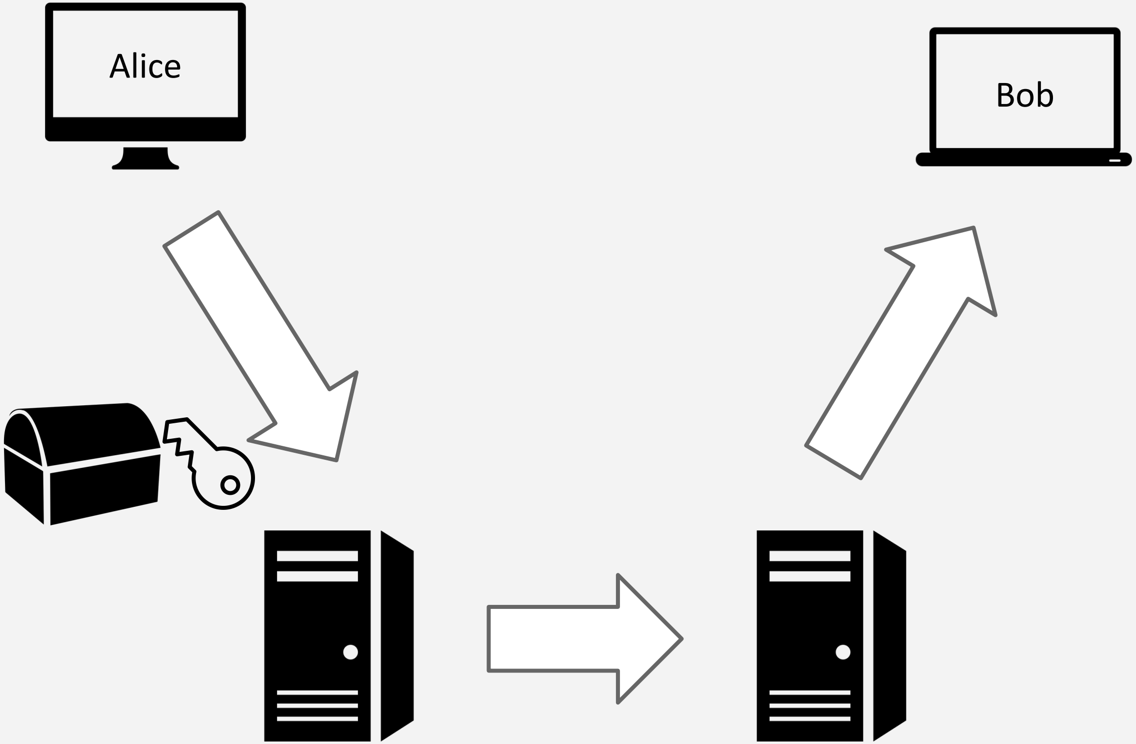
Asimmetrica


Alice
Bob

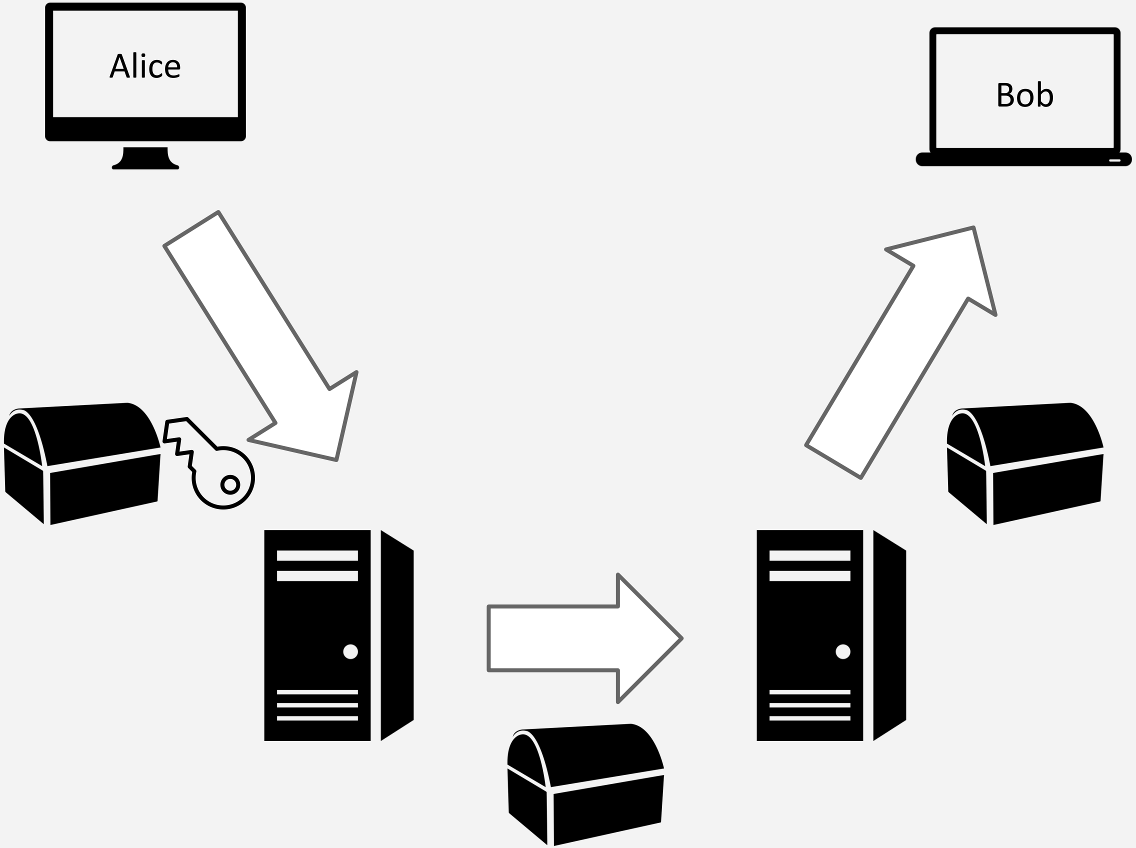
440
SQUIRE
FOUR BRASS LEVERS
FORGED STEEL SHACKLE


Alice
Bob

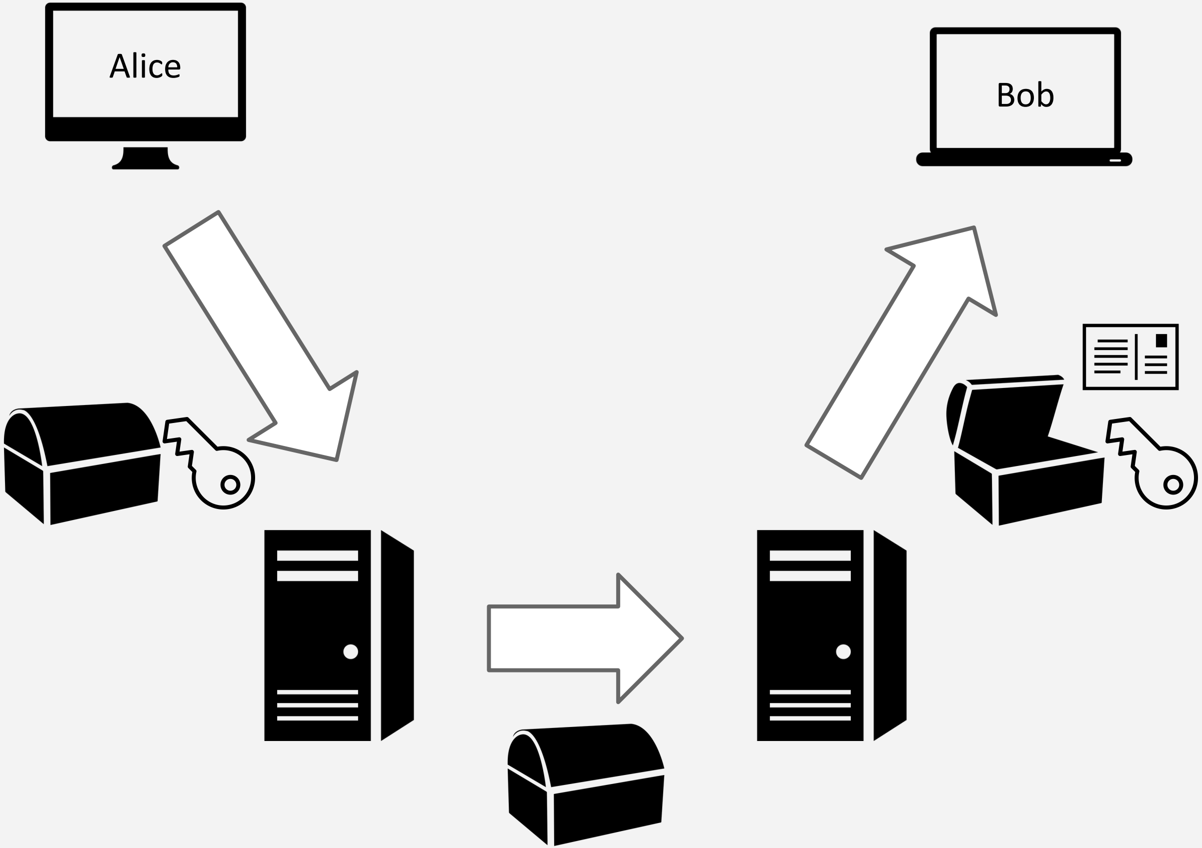
440
SQUIRE
FOUR BRASS LEVERS
FORGED STEEL SHACKLE


Alice
Bob

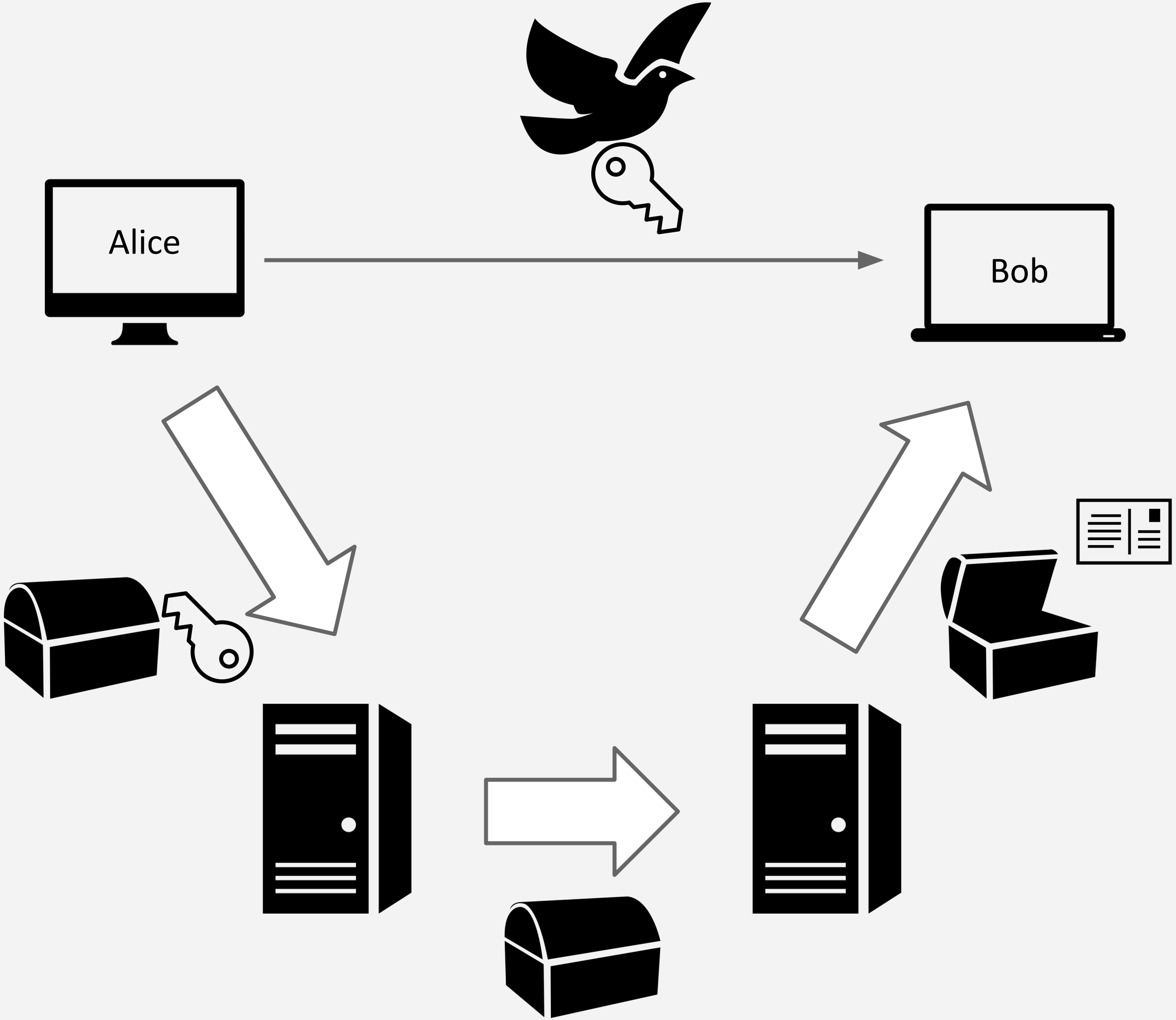
440
SQUIRE
FOUR
BRASS
LEVERS
FORGED
STEEL
SHACKLE


Alice
Bob

440
SQUIRE
FOUR BRASS LEVERS
FORGED STEEL SHACKLE


Alice
Bob

440
SQUIRE


Alice
Bob

440
SQUIRE
FOUR BRASS LEVERS
FORGED STEEL SHACKLE

Points of Failure

Blocchi / Flusso

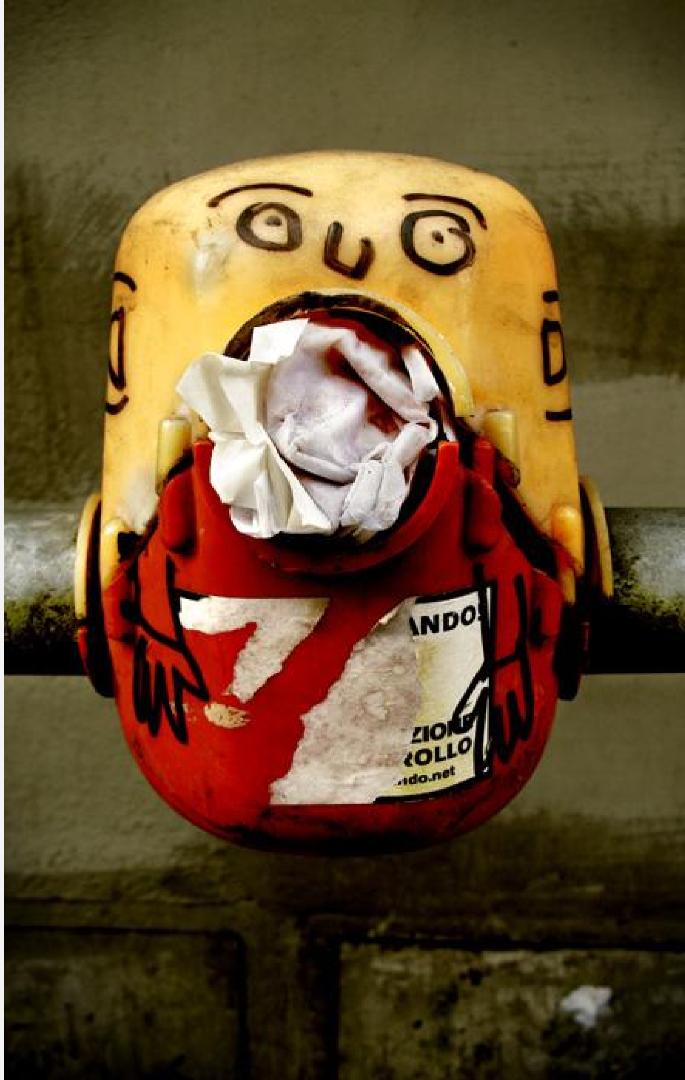
Basic: login password

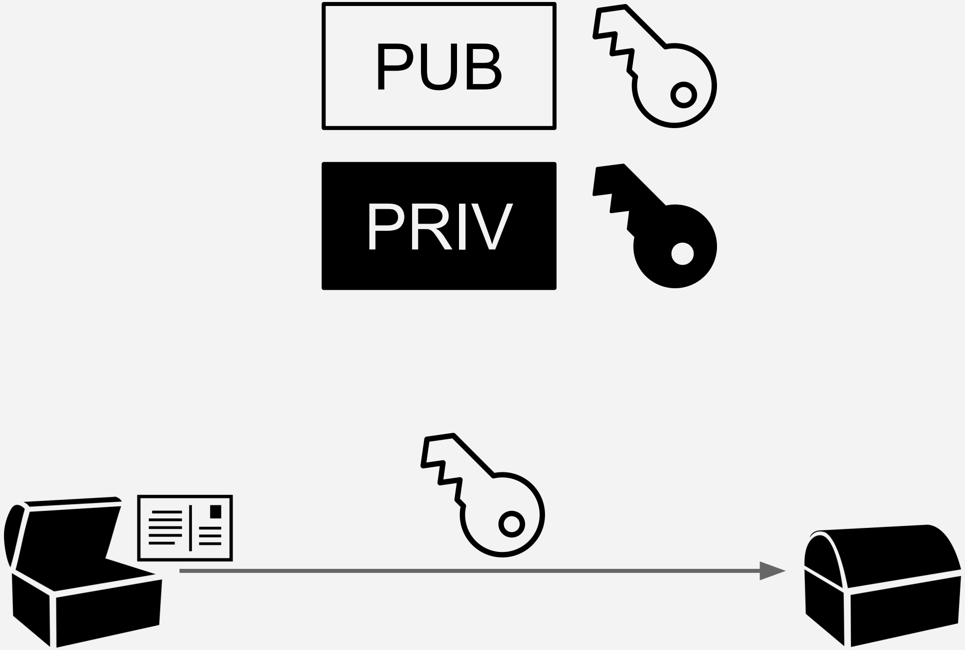
Simmetrica

Asimmetrica

PUB

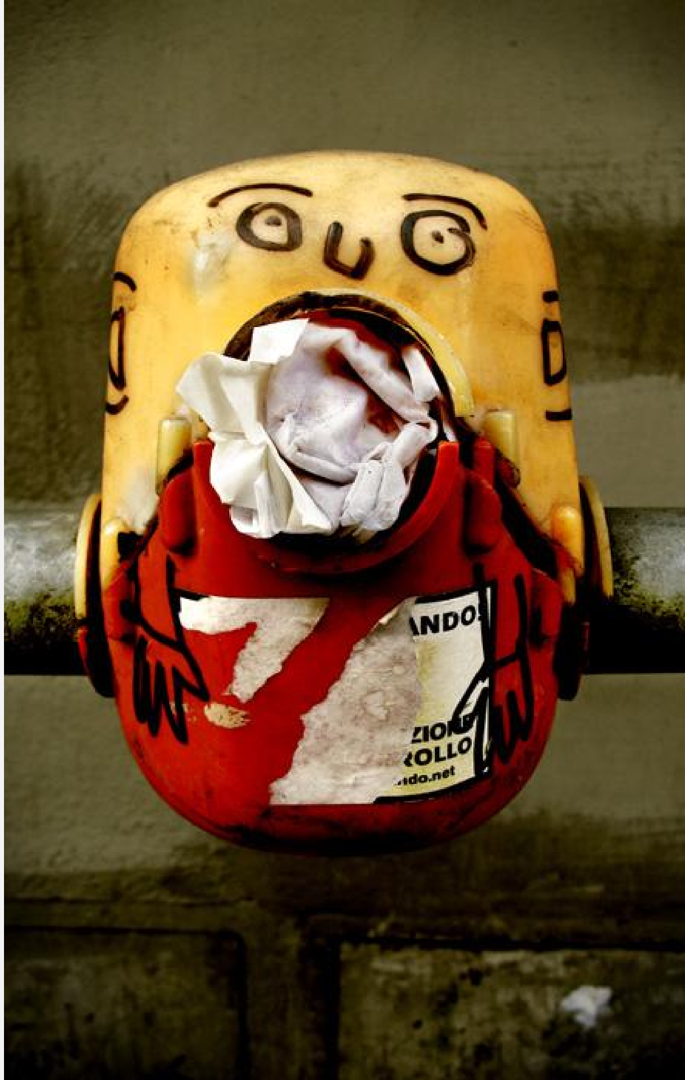
PRIV

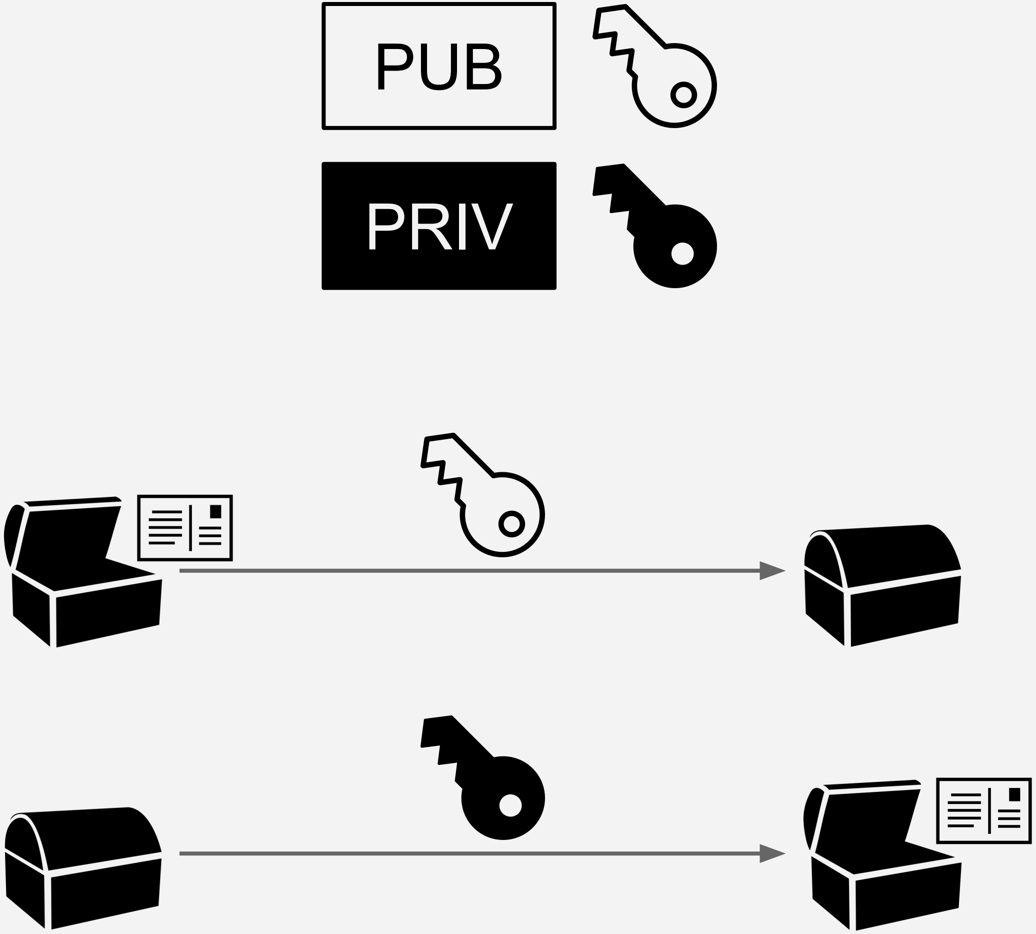




PUB

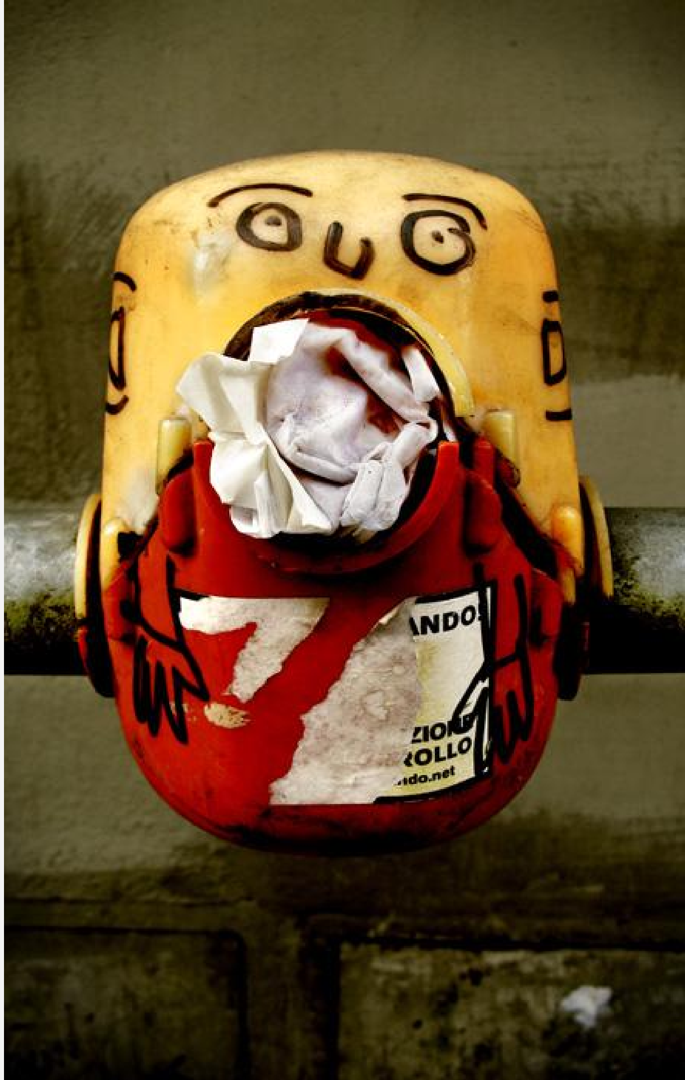
PRIV

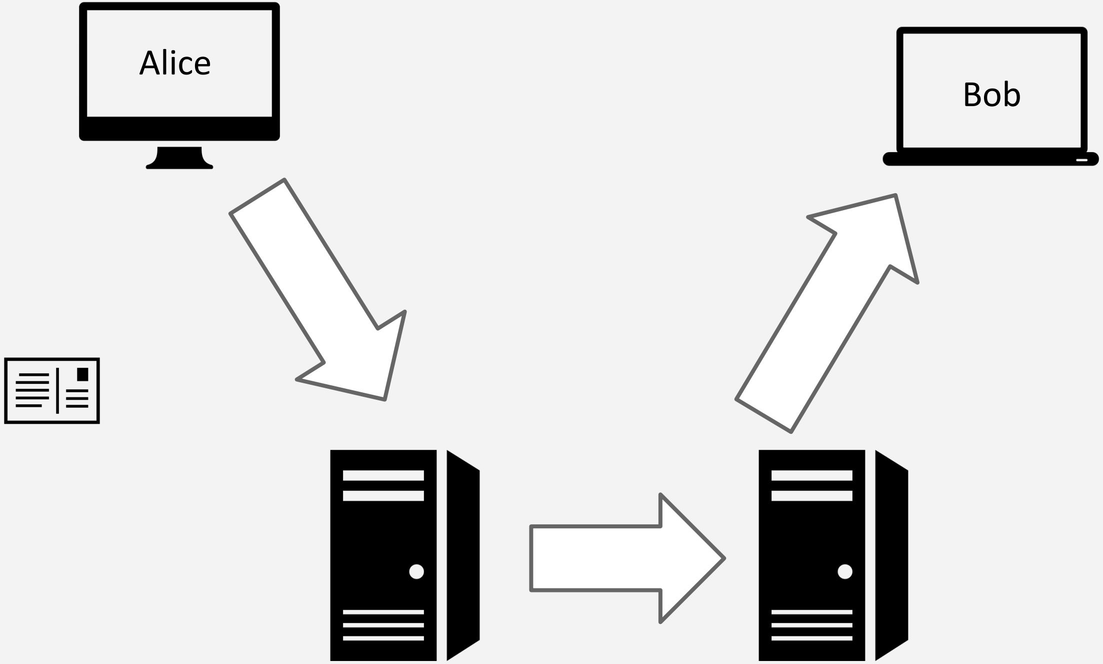




PUB

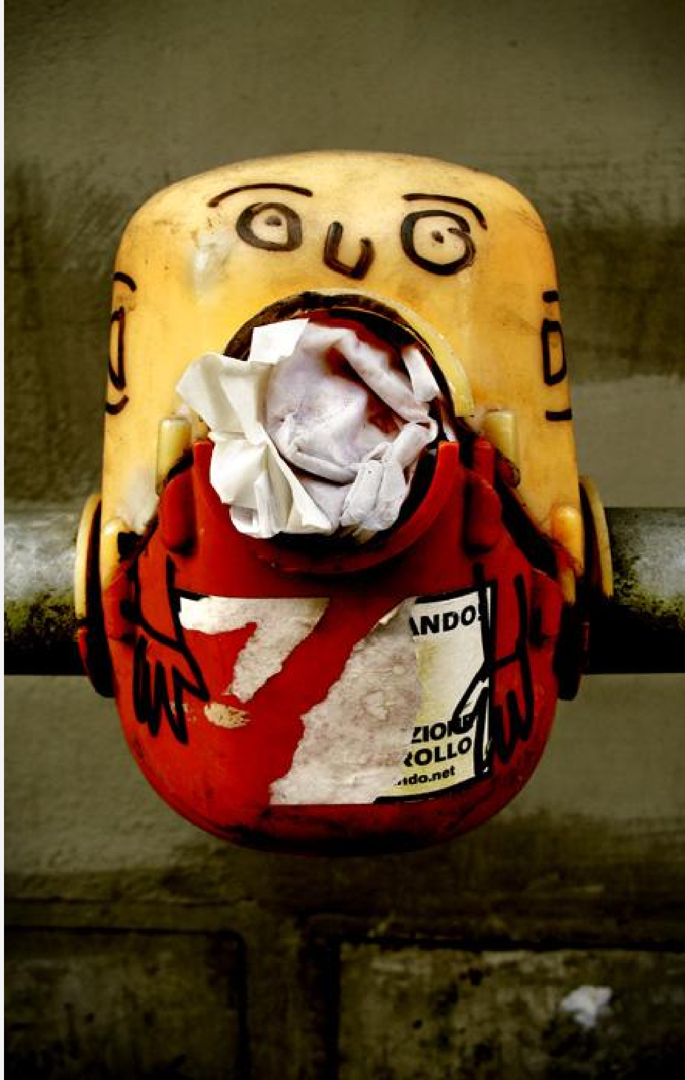
PRIV

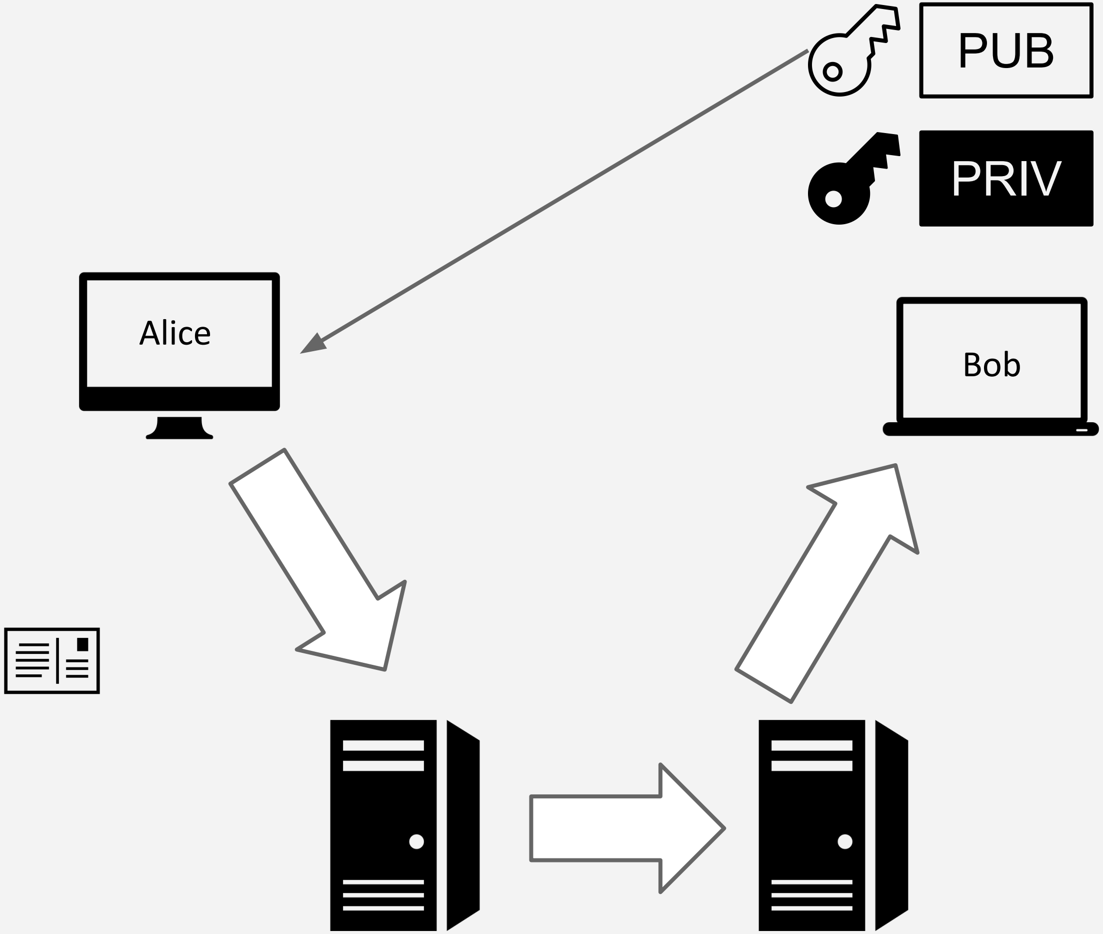


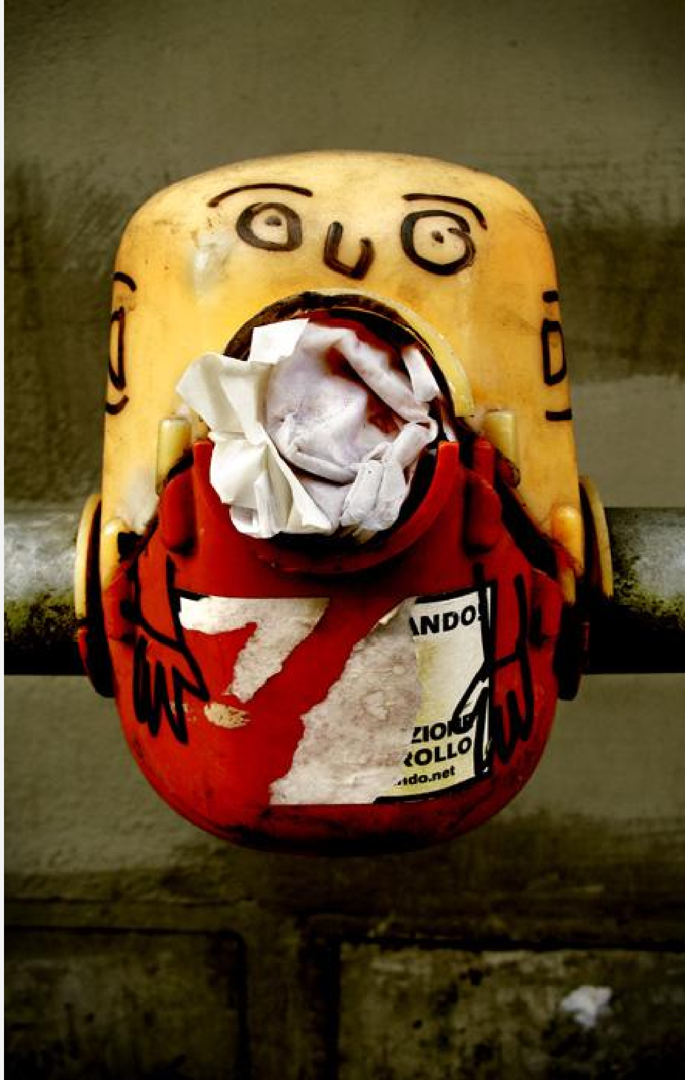


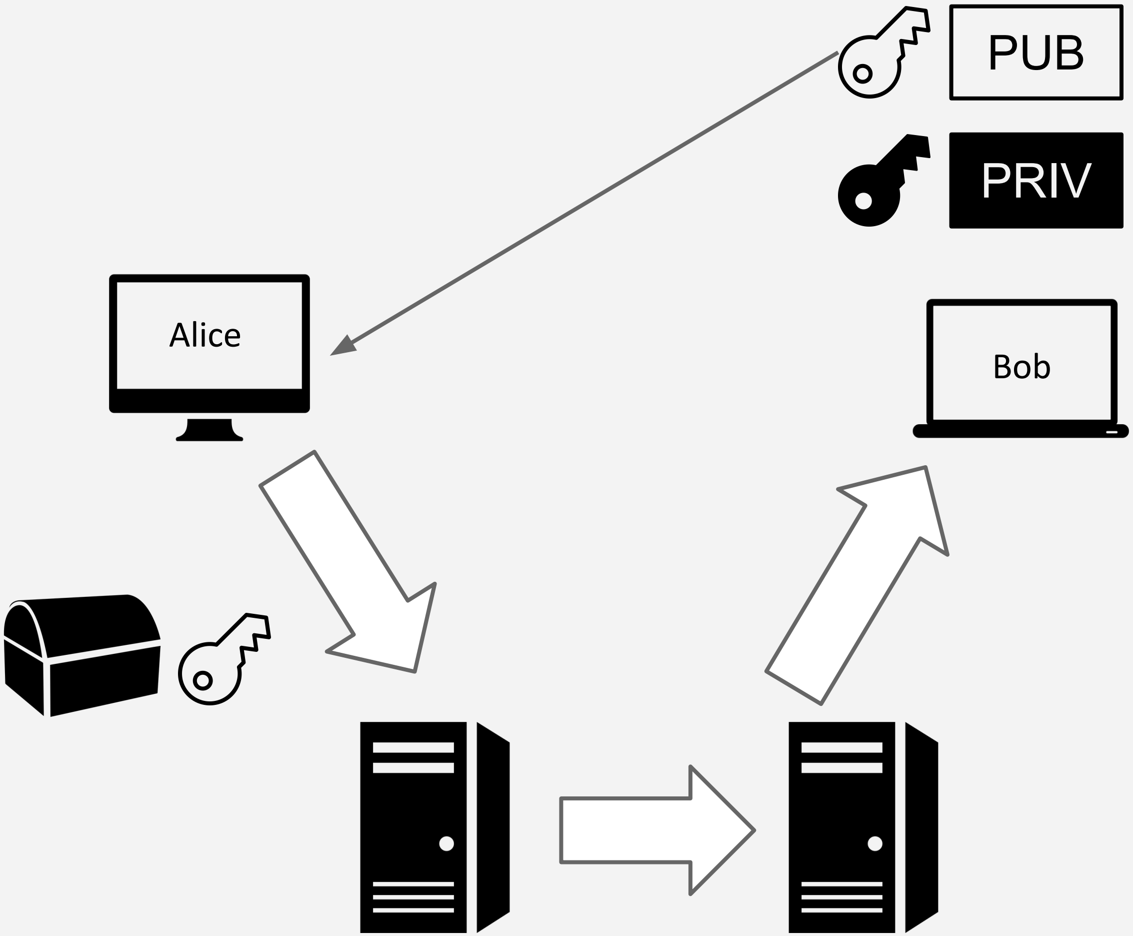
Alice

Bob

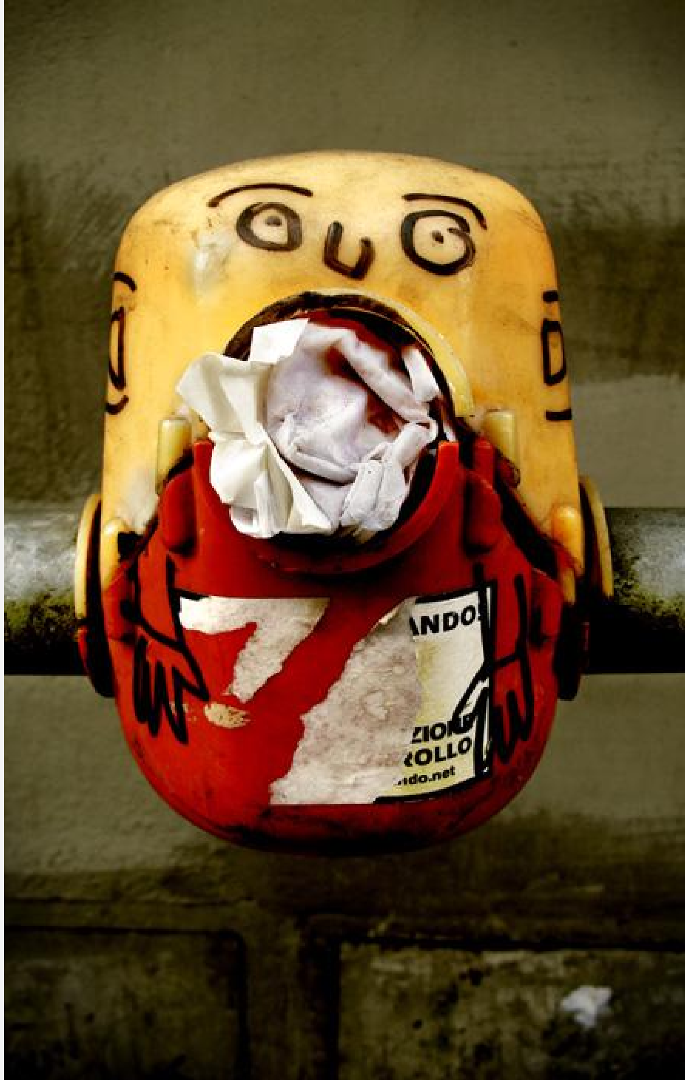



PUB
PRIV
Alice
Bob

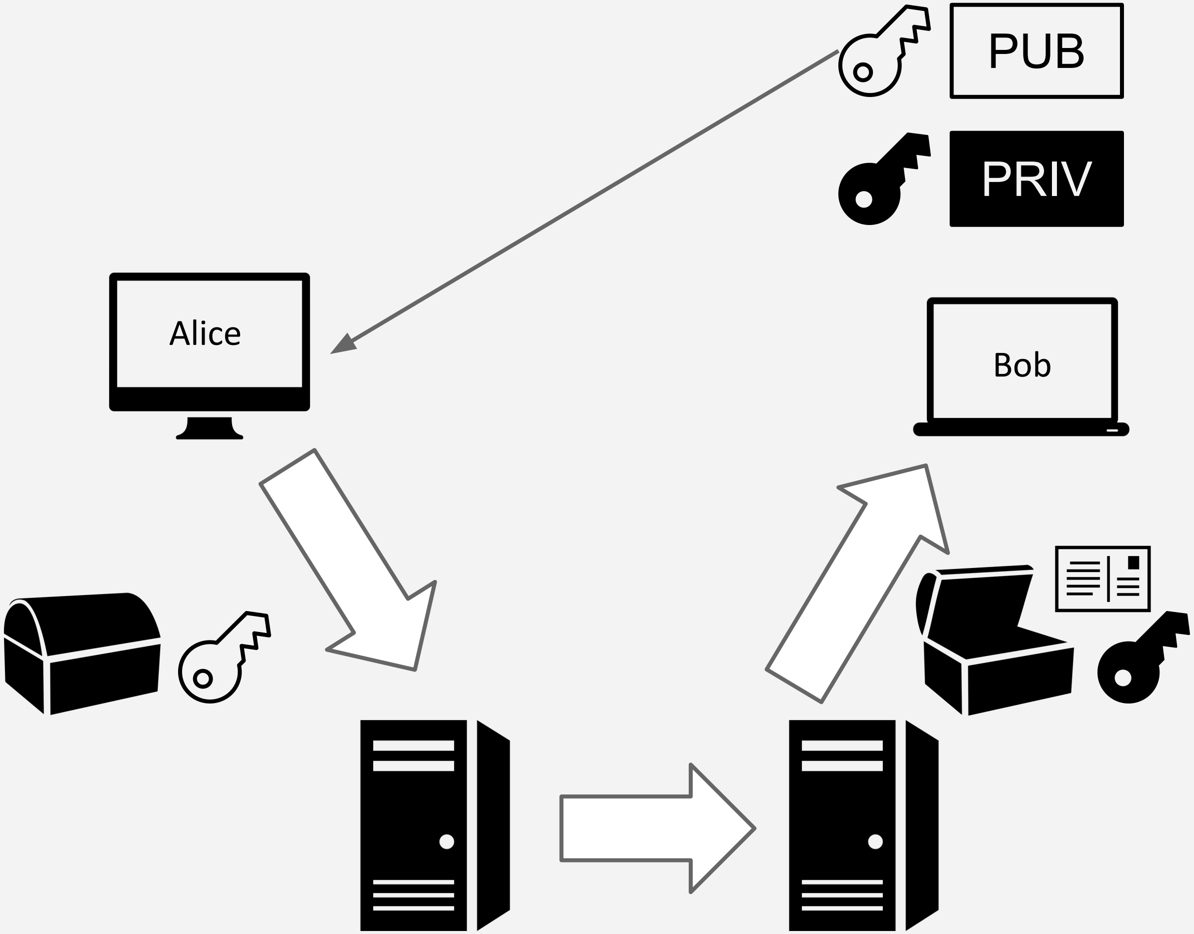

ANDO
ZIONI
ROLLO
ndo.net

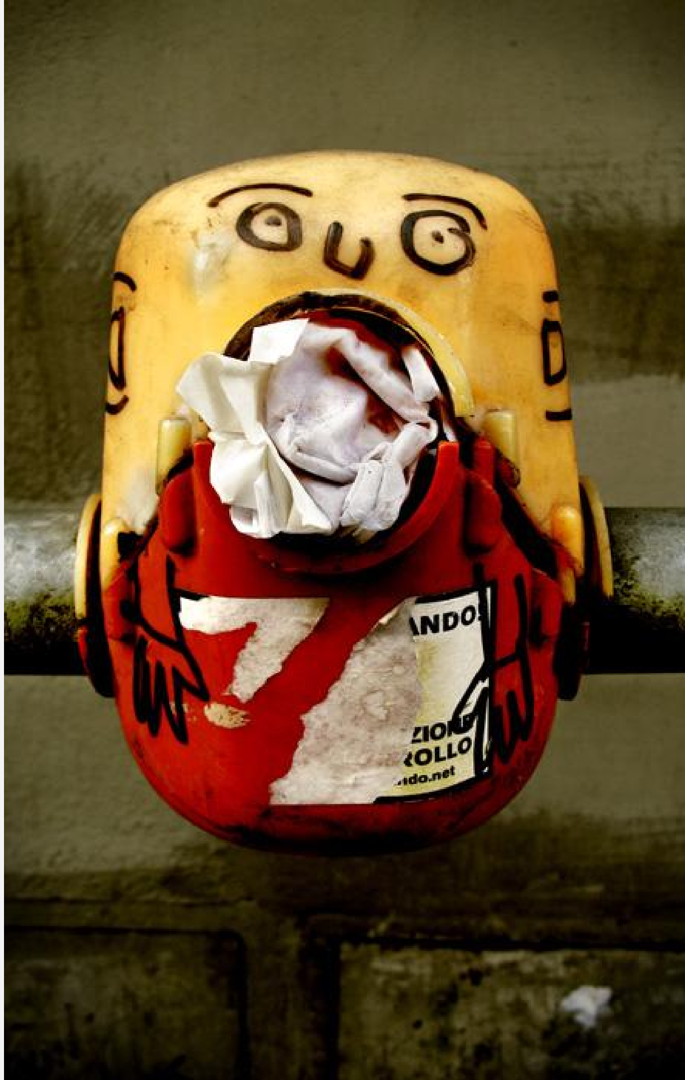


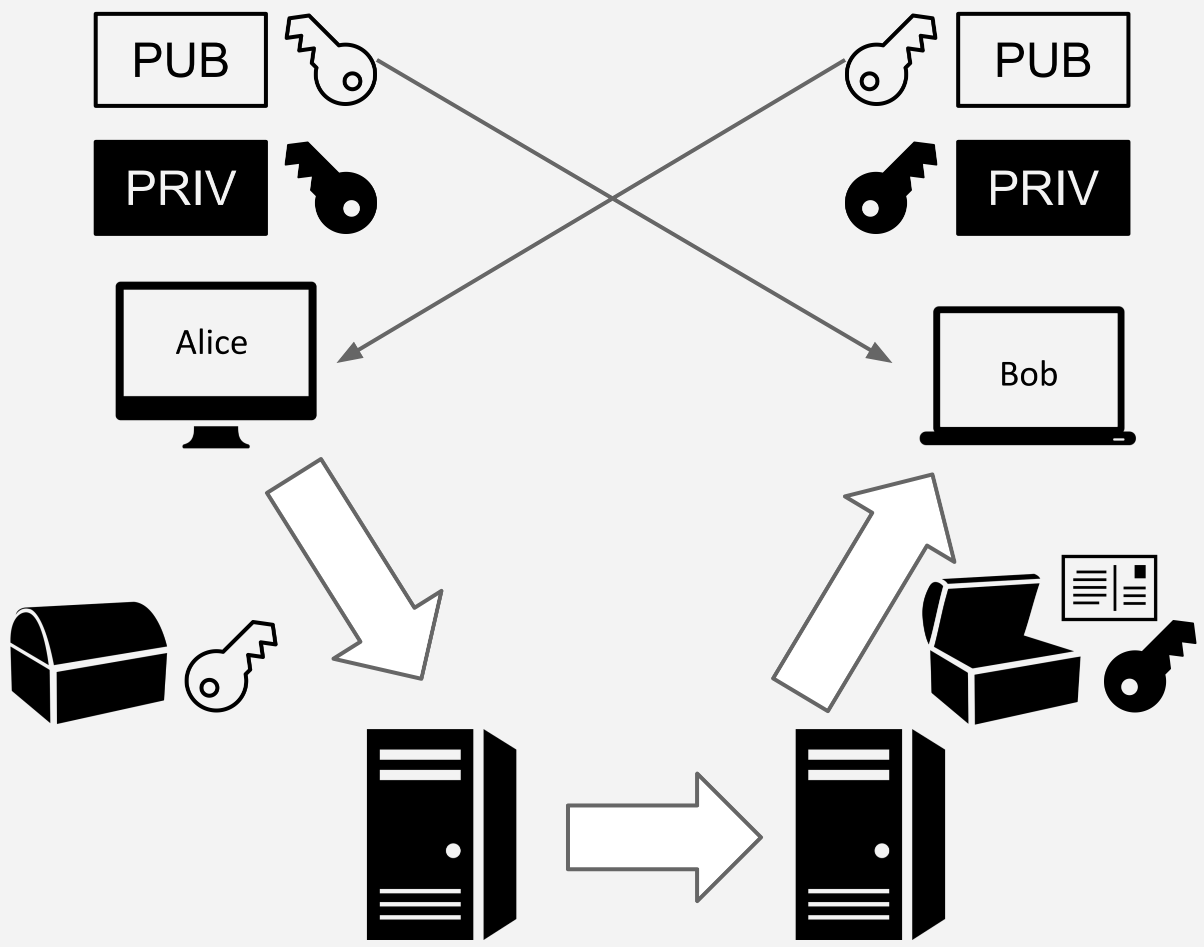
PUB
PRIV
Alice
Bob

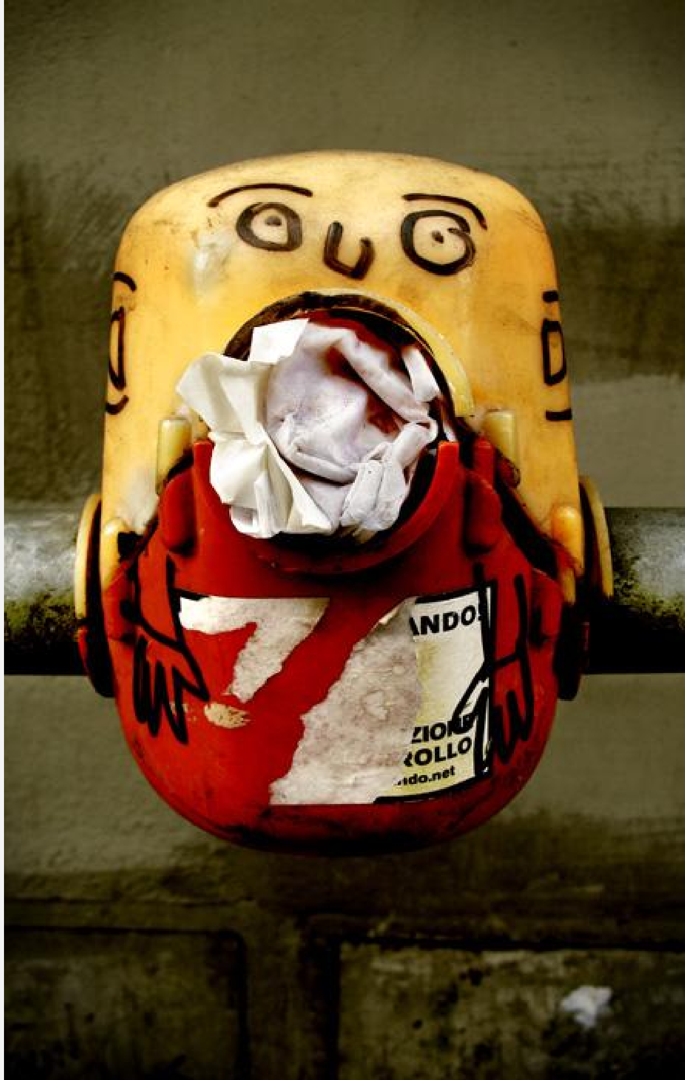


ANDO
ZIONI
ROLLO
ndo.net

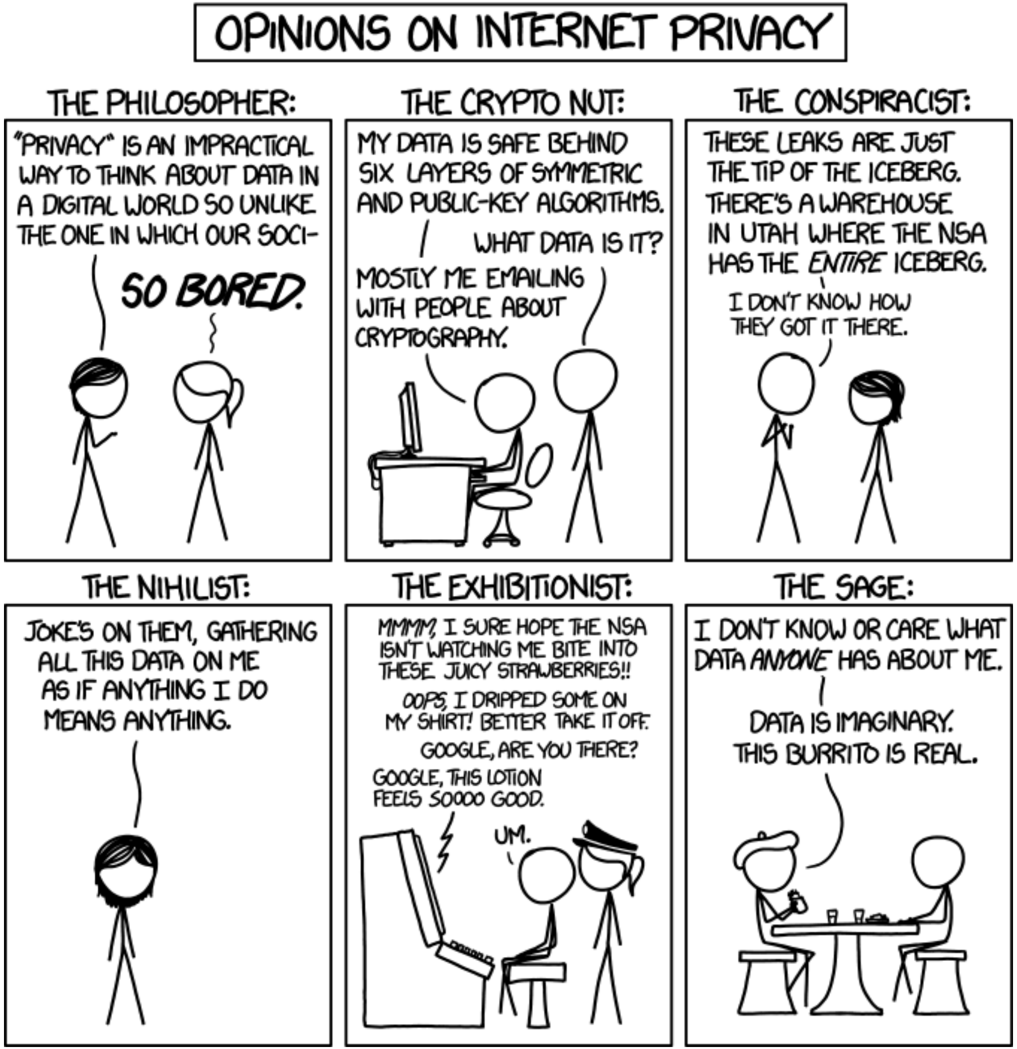

PUB
PRIV
Alice
Bob


ANDO
ZIONI
ROLLO
ndo.net


PUB
PRIV
Alice
PUB
PRIV
Bob


ANDO
ZIONI
ROLLO
ndo.net

# Domande?


OPINIONS ON INTERNET PRIVACY
THE PHILOSOPHER:
"PRIVACY" IS AN IMPRACTICAL WAY TO THINK ABOUT DATA IN A DIGITAL WORLD SO UNLIKE THE ONE IN WHICH OUR SOCI-
SO BORED.
THE CRYPTO NUT:
MY DATA IS SAFE BEHIND SIX LAYERS OF SYMMETRIC AND PUBLIC-KEY ALGORITHMS.
WHAT DATA IS IT?
MOSTLY ME EMAILING WITH PEOPLE ABOUT CRYPTOGRAPHY.
THE CONSPIRACIST:
THESE LEAKS ARE JUST THE TIP OF THE ICEBERG. THERE'S A WAREHOUSE IN UTAH WHERE THE NSA HAS THE ENTIRE ICEBERG.
I DON'T KNOW HOW THEY GOT IT THERE.
THE NIHILIST:
JOKE'S ON THEM, GATHERING ALL THIS DATA ON ME AS IF ANYTHING I DO MEANS ANYTHING.
THE EXHIBITIONIST:
MMMM, I SURE HOPE THE NSA ISN'T WATCHING ME BITE INTO THESE JUICY STRAWBERRIES!!
OOPS, I DRIPPED SOME ON MY SHIRT! BETTER TAKE IT OFF.
GOOGLE, ARE YOU THERE?
GOOGLE, THIS LOTION FEELS SOOOO GOOD.
UM.
THE SAGE:
I DON'T KNOW OR CARE WHAT DATA ANYONE HAS ABOUT ME.
DATA IS IMAGINARY. THIS BURRITO IS REAL.