

Cryptography (a short intro)

Dominique Unruh

University of Tartu

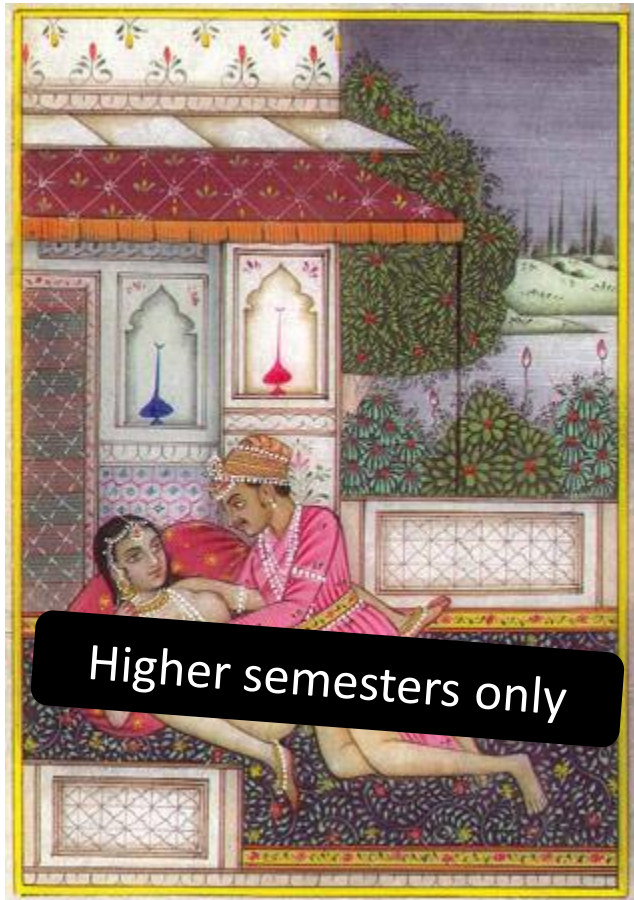
What is Cryptography?

Communication in the presence of an adversary

- More than just encryption
- Protection of data integrity
- Communication *with* the adversary

Cryptography in History

Kama Sutra recommends...



The following are the arts to be studied, together with the Kama Sutra:

[...]

The art of understanding writing in cypher, and the writing of words in a peculiar way.

(Translation by Richard Burton)

Caesar Cipher

- Shift each letter by three places

CAESAR



FDHVDU

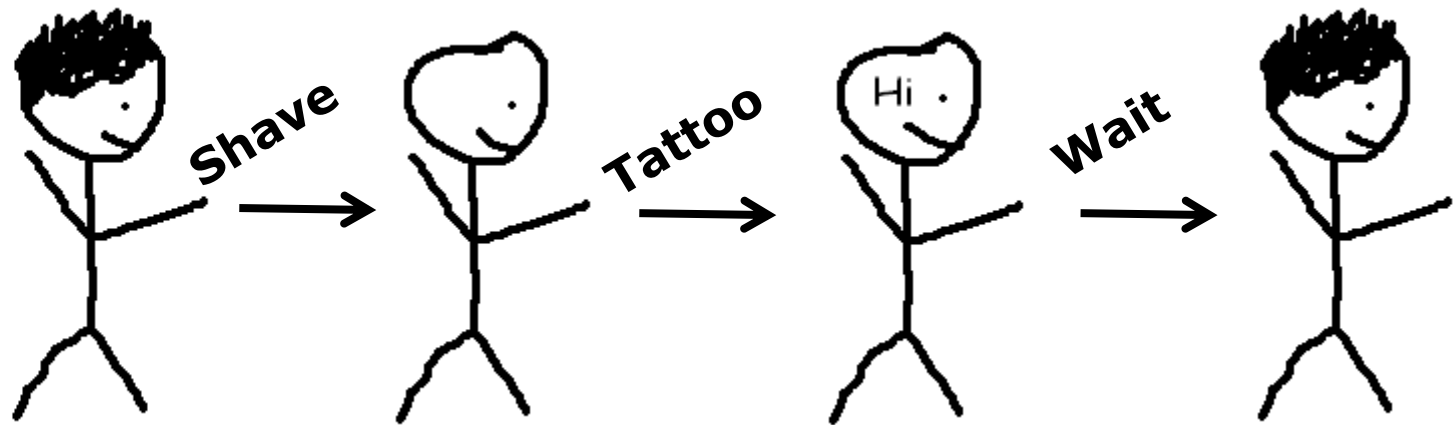
- Supposedly used by Julius Caesar

Scytale

Sparta... 2500 years ago...



Herodotus and the Slave Cipher



(5. century BC)

Invisible Ink

- Lemon juice as invisible ink



- After heating, ink becomes brown

The Kerckhoffs principle

Auguste Kerckhoffs

- “La cryptographie militaire”,
Journal des sciences militaires,
1883
- “The system must not require
secrecy, and it can fall into
enemy’s hands without causing
trouble”



Kerckhoffs Principle - Consequences

- Separation of cryptosystem and key
- System must stay secure even if only key is secret
- Design-principle for modern cryptography

The enemy knows the system.

Claude Shannon

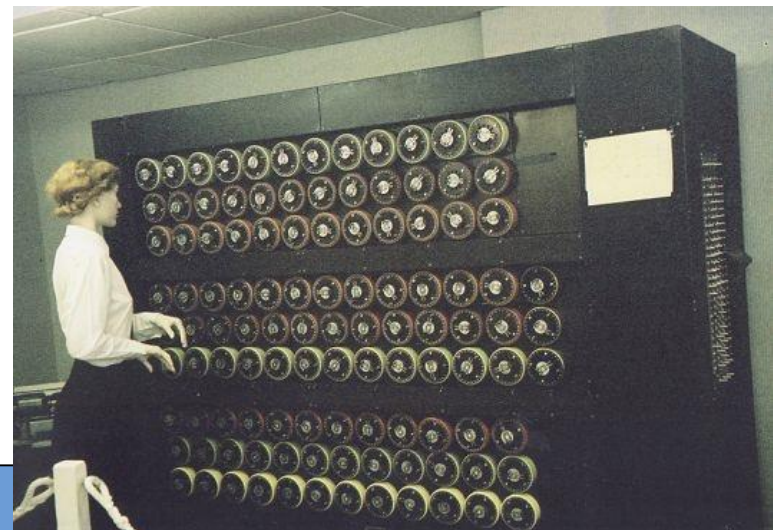
Enigma

- German cipher machine from World War II
- 3-4 wheels (rotors) with electrical wires
- Rotor position determines the wire connections
- Key press →
Lamp lights up, rotor rotates



Enigma

- Rotor position = key
- Even after the British got an Enigma, immense work needed for breaking it
- Alan Turing's team had >10000 helpers
- A success for the Kerkhoffs principle



Modern Cryptography

Information theory



Claude Shannon

- Shannon, “A mathematical theory of communication”, 1948
- Information as a mathematical object
- Security can be defined, analyzed, and proven!

One-time-pad

Message: 001110100100111100010
+
Key: 101011100101001011100
=
Ciphertext: 100101000001110111110

**Shannon: One-time-pad is
provably secure!**

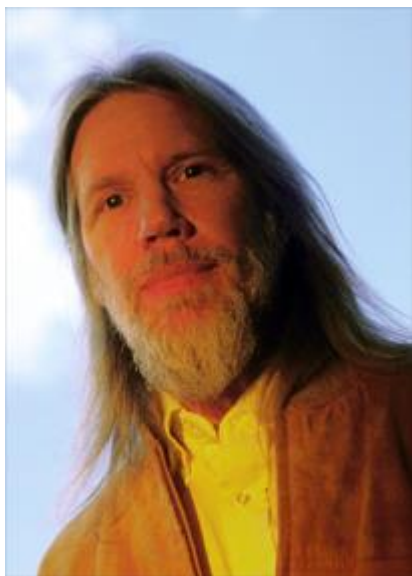
One-time-pad in Practice

Not practical:

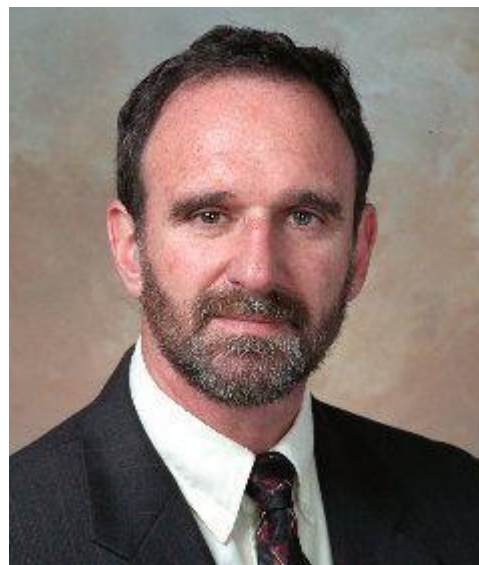
- Long key
- May only be used once
- Useful auxiliary tool



Public-Key Cryptography



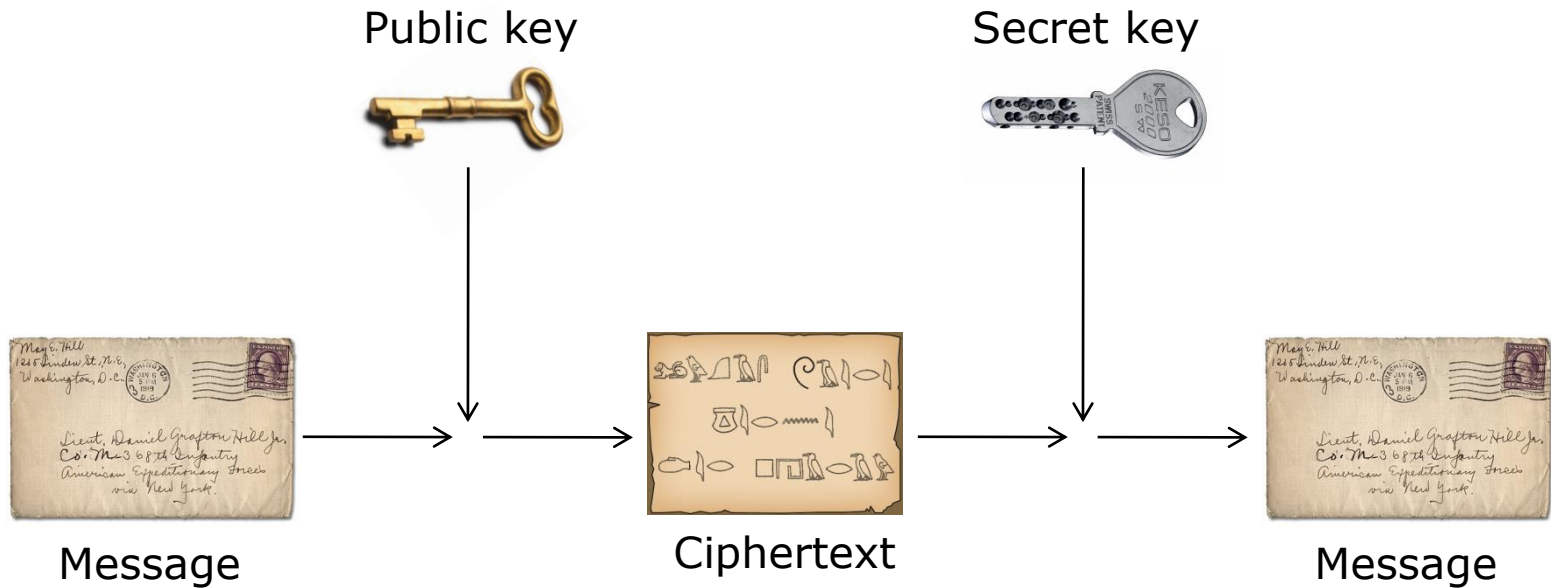
Whitfield Diffie



Martin Hellman

“New Directions in Cryptography”, 1976

Public Key Cryptography



**Advantage: Public key
may be published**

**More than
just encryption**

Millionaire's Problem

I am the richest duck!



None wishes to reveal the size of his fortune

Who is richer?

I am the richest duck!



None trusts the other

Secure Auctions

Buyers



Sugar beet vendors



Offers



Production quantities



No-one wishes to reveal his prices
What shall the market price be?

Data-mining

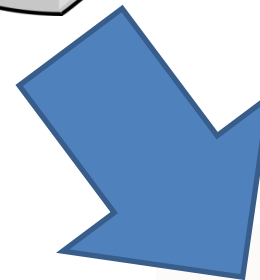
Medical data



Medical data

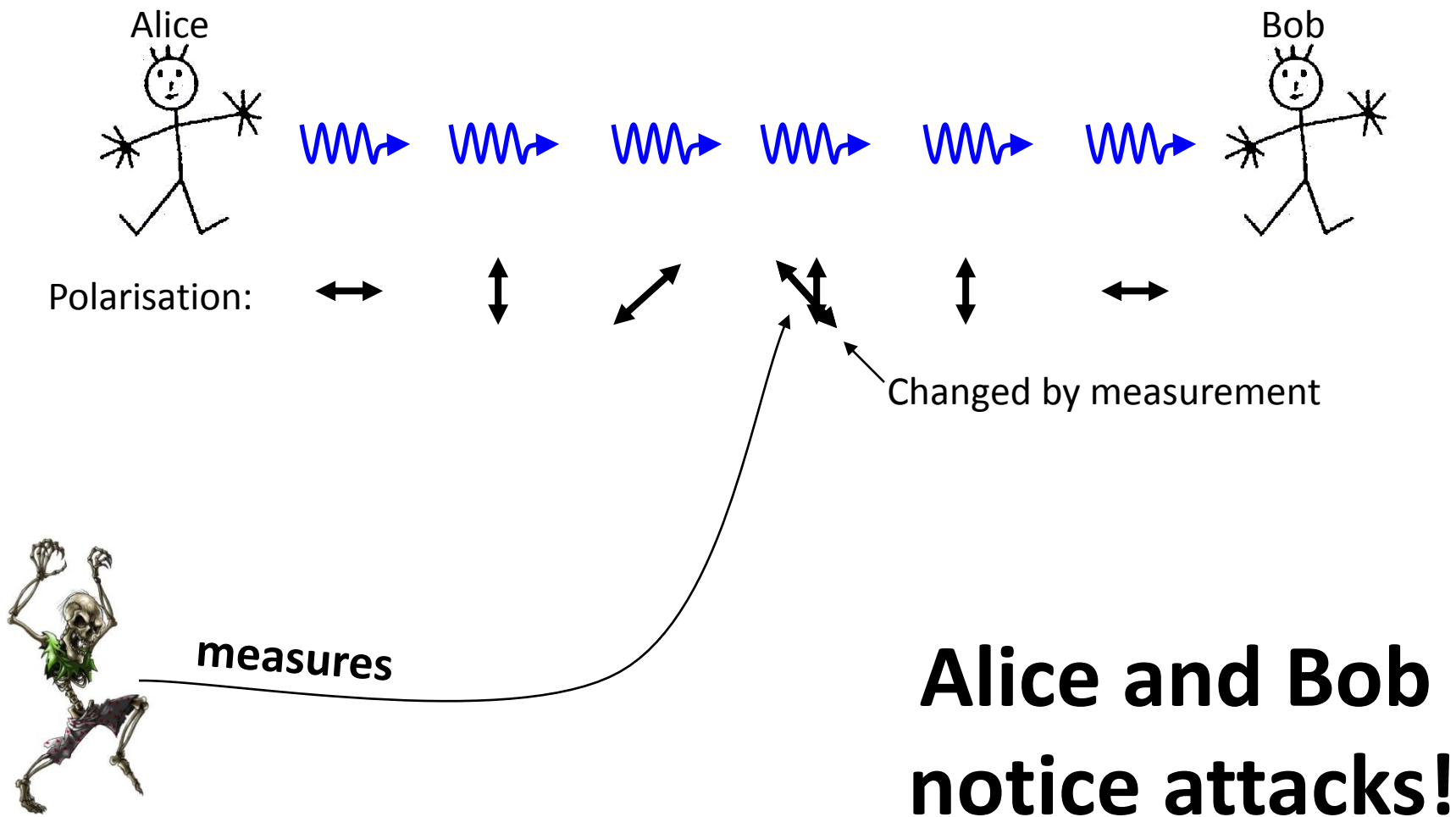


Medical data



New Knowledge

Quantum Key Exchange



Cryptography

**More than encryption –
Communication in the presence of the adversary**

A fascinating topic, combining relevance and
challenging research questions

How to study crypto

- Security lectures at bachelor's level (e.g., applied crypto)
- Crypto more on master's level (or end of bachelor)
- Get a background in math in time

Q?