Cryptography (a short intro)

Dominique Unruh
University of Tartu
κρυπτός  γράφειν

hidden  writing
Secret codes

Encryption
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”
Kerkhoffs 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

• 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
Public-Key Cryptography

"New Directions in Cryptography", 1976

Whitfield Diffie
Martin Hellman
Public Key Cryptography

Public key

Message → Ciphertext → Secret key → Message

Advantage: Public key may be published
Provable Security

1. Postulate complexity assumption
   – Example: Factoring large integers is hard

2. Develop cryptosystem

3. Security proof:
   – If cryptosystem is broken, complexity assumption was wrong
Why Complexity Assumptions

We can’t do better...

(State of the art: we can prove the hardness of almost nothing...)
Example: Proof in the cryptographic model

\[ f : D \rightarrow D \text{ one-way permutation} \]

\[ g(x) := f(f(x)) \]

Is \( g \) one-way permutation?

\[ B(y) := f(A(y)) \]

\[ z = z' \]
\[ x = x' \]
\[ z \leftarrow D \text{ random} \]
\[ y := f(z) \]
\[ z' := B(y) \]
\[ \approx 0 \]

\( g \) is one-way permutation
Beyond the basics
Millionaire’s Problem

None wishes to reveal the size of his fortune

None trusts the other
Secure Auctions

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

Buyers

Sugar beet vendors

Offers

Production quantities
Data-mining

Medical data

Medical data

Medical data

New Knowledge
Zero Knowledge

\[ \forall x, y, z, n > 2: x^n + y^n \neq z^n \]

But I don’t want to tell you the proof!

Zero Knowledge Proof:
- Prover cannot prove wrong statement
- Verifier does not learn anything
Zero Knowledge: How?

Graphs $G$ and $H$ are isomorphic

Permute $G$

Permuted graph $J$

$G$ or $H$

Pick $G$ or $H$

Iso between $J$ and $G$ or $J$ and $H$
Zero Knowledge: How?

\[ G \text{ and } H \text{ not isomorphic} \]

\[ \text{Permute } G \quad \text{Permuted graph } J \]

⇒ Prover will get stuck with probability \( \frac{1}{2} \)

\[ \text{Verifer does not learn anything:} \]

\[ \text{Could produce iso and } J \text{ on his own} \]

\[ \text{Pick } G \text{ or } H \]
Quantum Key Exchange

Alice

Polarisation:

Bob

Measures
Sends directions

Shared key bits
Quantum Key Exchange – Attack

Alice

Bob

Polarisation:

Adversary measures

→ Bit destroyed

→ Alice+Bob: different keys

→ Attack detected
Quantum Position Verification

Speed of light
→ Position verified
Electronic Voting

Charlie for president!
Coercion!

Vote for Alice! And don’t dare throw away the receipt. $?@)$^=+!
Cryptography

More than encryption –
Communication in the presence of the adversary

A fascinating topic, combining relevance and challenging research questions
I thank for your attention