universität innsbruck

The Cradle of Asymmetric Cryptography

Secure Communications Over Insecure Channels

Kristina Magnussen

Motivation

Some Historical Background

Ralph Merkle developed **Merkle's puzzles** in **1974** for a university project. The idea was rejected by his professor. At this time, asymmetric cryptography concepts were not known to the public.

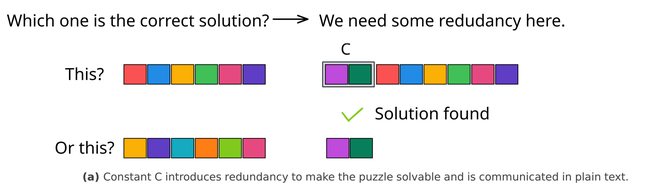
- Symmetric crypto requires key exchange
  → additional *secure channel* needed to transmit key
- This new method allows communication partners to transmit a key over *insecure channels*
- *Assumption:* Attacker can read everything sent on this channel
- *Advantages of this method:*
  - Solution to key distribution problem
  - Easier key exchange in network with multiple communication partners

Puzzle Creation

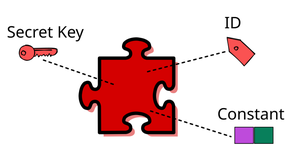
Definition

Puzzle: Cryptogram which can be solved through cryptanalysis
→ Puzzle is meant to be *solved*.

- *Idea:* Hide information (here the secret key) in a puzzle by encrypting it
- Restricting the key space keeps puzzle solvable
  → Increase/decrease puzzle difficulty by adapting key space



(a) Constant C introduces redundancy to make the puzzle solvable and is communicated in plain text.



(b) Information contained in the puzzle.

Key Exchange using Puzzles

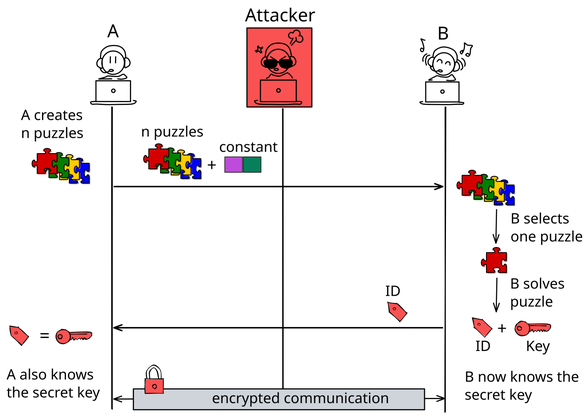
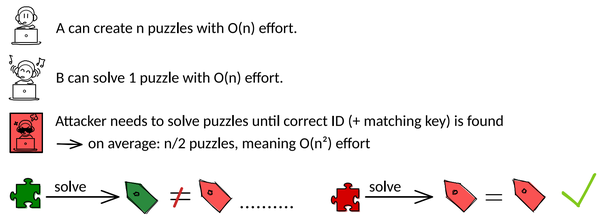


Figure 2: This sequence diagram shows the key exchange between two communication partners A and B using puzzles. The first two messages are unencrypted.

Security of Merkle's Puzzles



What Does This Mean for Security?

Even if a large n is chosen, attacker only has to put in $O(n^2)$ effort, which makes brute-force attacks feasible.

Example

For $n = 10000$, the attacker has to calculate 5000 puzzles on average. If it takes about 1 minute to solve a puzzle, the attacker will have found the key in about 3.5 days.

Disadvantages

- For exchanging a key, communication partners have to transmit a large amount of data
- The larger the n, the larger the amount of effort communication partners have to expend
  → A moderate amount of security requires a very large n.

Merkle's Method Compared to Current Asymmetric Schemes

State of the Art Asymmetric Encryption Schemes

Current asymmetric encryption schemes are based on problems which are considered to be **mathematically hard** to solve.
→ Computing these problems is *infeasible* for large values.

Asymmetric Encryption Schemes are mainly based on:

- *Discrete Logarithm Problem*
- *Integer Factorization Problem*.

Lessons Learned

Influence of Merkle's Puzzles

The rejected idea of a student became one of the first *public-key protocols* known to the public.

- Merkle's idea inspired the *Diffie-Hellmann* key exchange, which is still widely used today.
- The original idea does not offer a sufficient level of security, however, the idea could serve as a base for other protocols.

References:
R. C. Merkle. Secure communications over insecure channels. Communications of the ACM, 21(4):294–299, 1978
C. Paar & J. Pelzl (2010): Understanding Cryptography, Springer
http://www.merkle.com/1974/