Pros and Cons of Basing Modern Cryptographic Systems on Prime Factoring

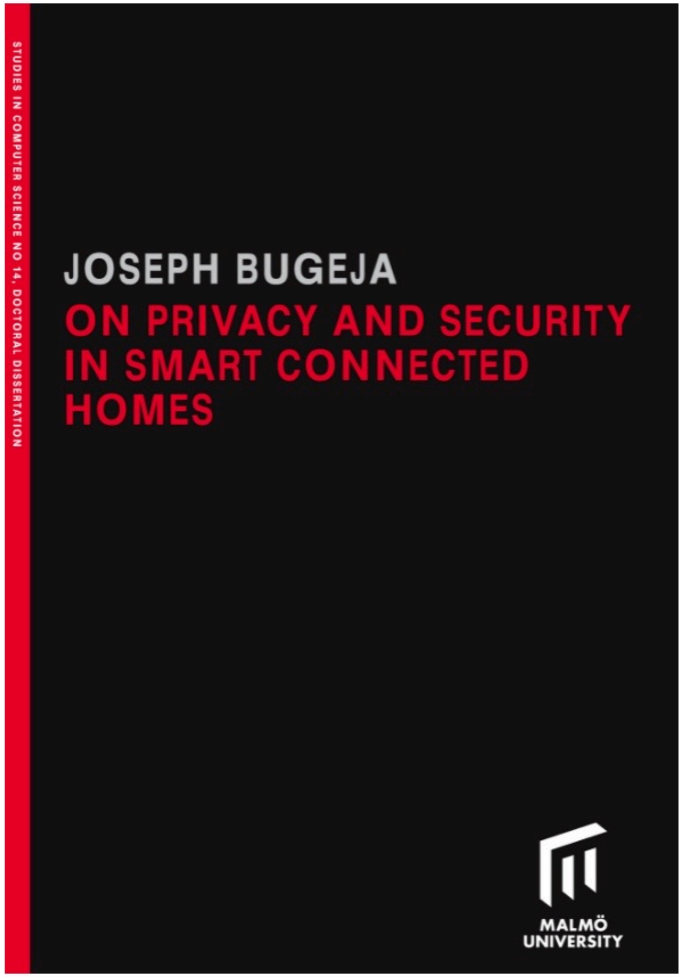
Joseph Bugeja

Learning Outcomes

- Understand the concept of prime factoring
- Explain the fundamental principles underlying the RSA algorithm
- Recognize the advantages and threats to basing cryptographic systems on prime factoring

My Background

- Postdoc and information security lecturer at Malmö University
- Ph.D.(Malmö); M.Sc.(London); B.Sc.(Hons)(Melit.)
- ENISA approved subject matter expert on security and privacy
- 10+ years of software industry experience



STUDIES IN COMPUTER SCIENCE NO 14, DOCTORAL DISSERTATION

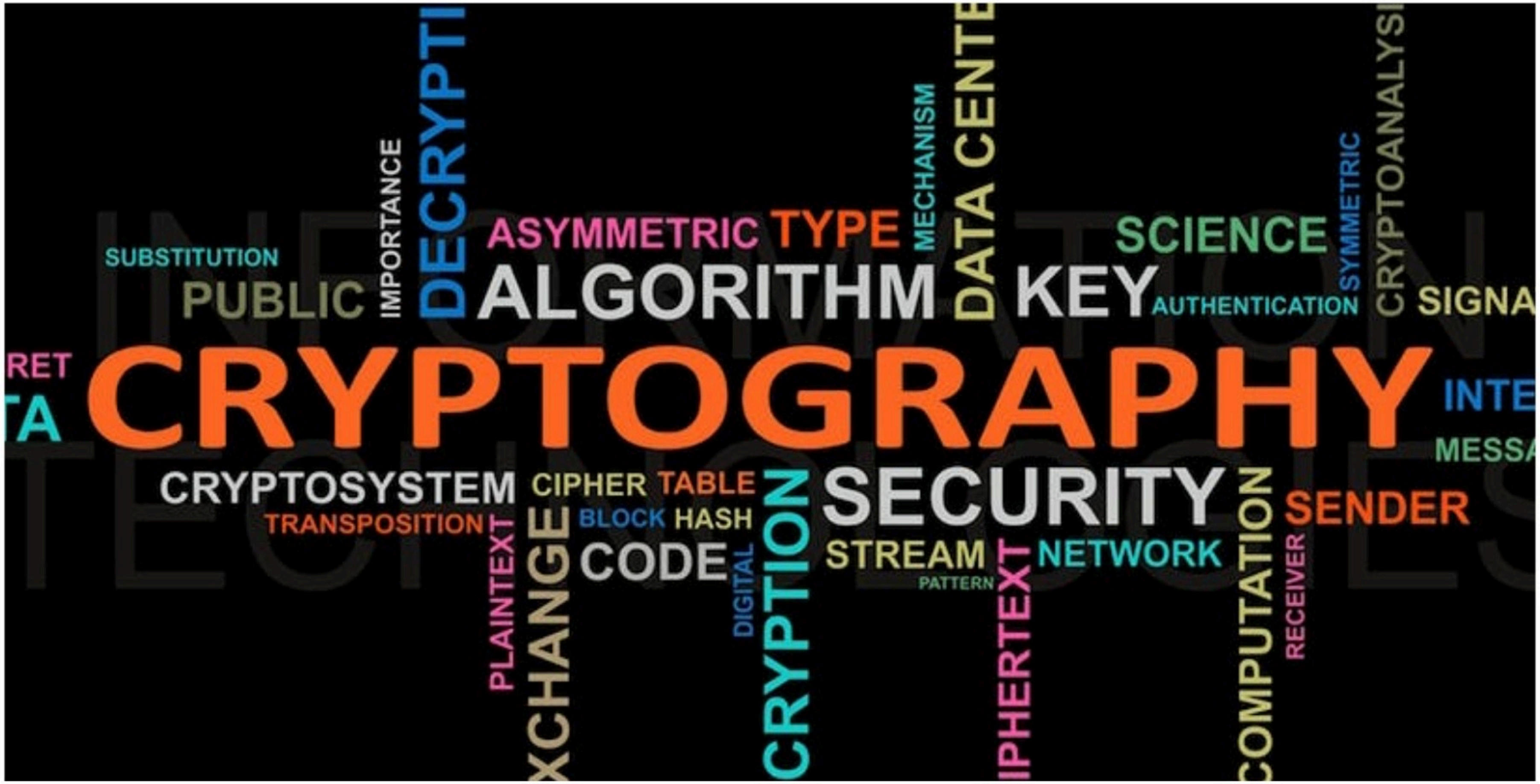
JOSEPH BUGEJA

ON PRIVACY AND SECURITY IN SMART CONNECTED HOMES

MALMÖ UNIVERSITY

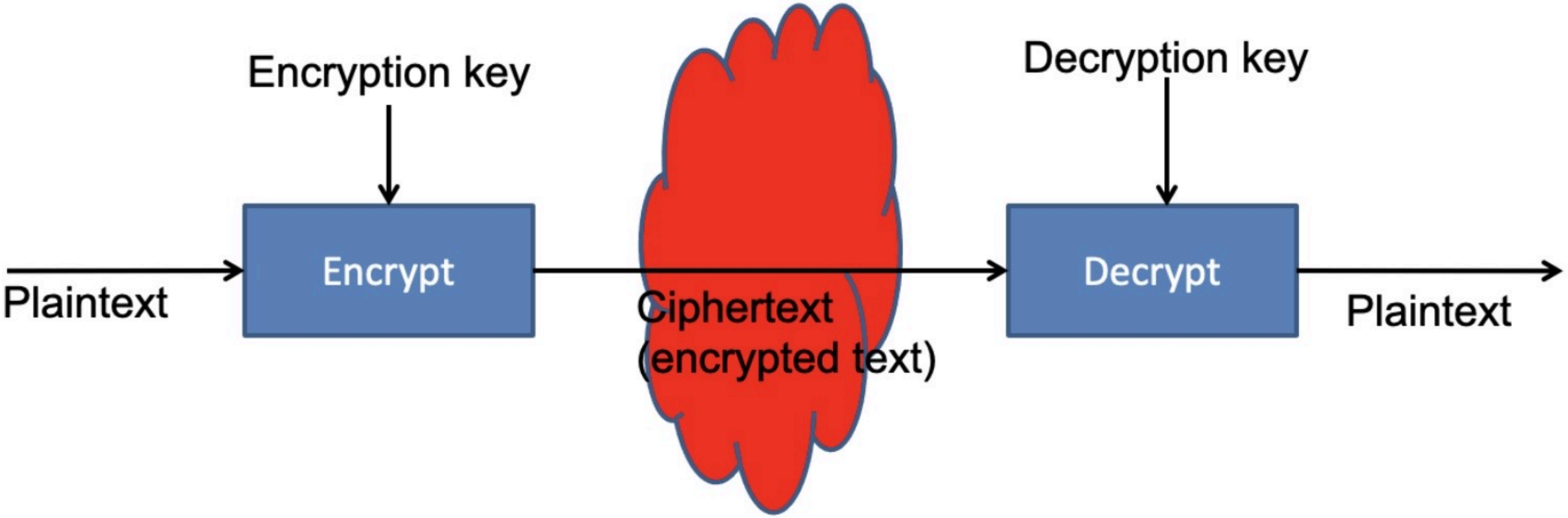
Cryptography

Cryptography is the science and study of secret writing



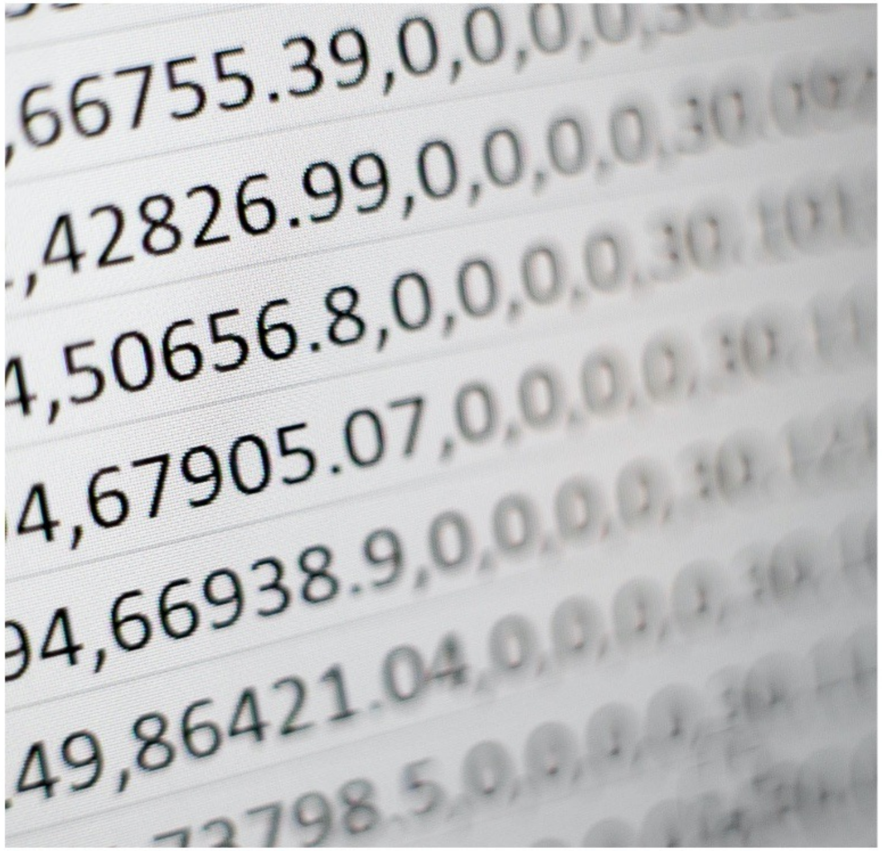
Cryptographic System

A *cryptographic system* refers to a computer system that employs cryptography so that only those for whom the information is intended can read and process it



Difficult Problems

- Discrete Logarithm Problem: Given a prime modulus *p*, a basis *a*, and a value *y*, find *x* such that $y = a^x \mod p$
- *n*th Root Problem: Given integers *m, n* and *a*, find an integer *b* such that $a = b^n \mod m$
- **Factorization: Given an integer *n*, find its prime factors**



Primes

- An integer $n > 1$ is prime if 1 and n are its only divisors
- Examples of primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, ...
- Euclid: There are infinitely many primes
- The largest known prime number (as of November 2022) is $2^{82,589,933} - 1$

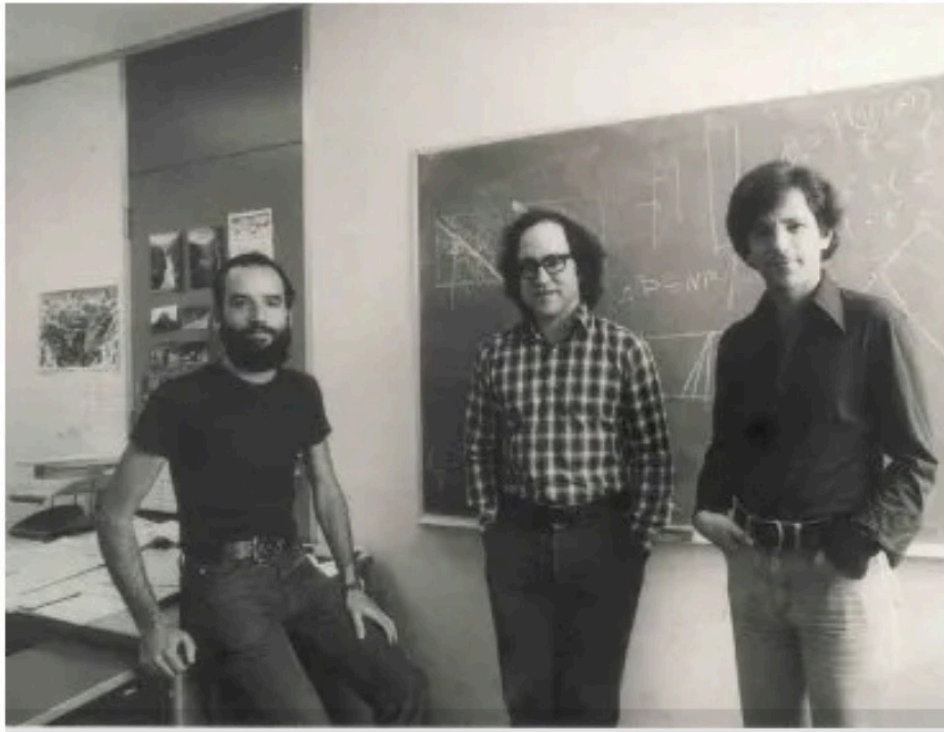
[1] "GIMPS Project Discovers Largest Known Prime Number: $2^{82,589,933}$-1". *Mersenne Research, Inc*. Retrieved 10 November 2022.

Pros to Basing Cryptographic Systems on Prime Factoring

- Multiplying two prime numbers is efficient
- Relatively easy to check if a number is a prime
- There is no known algorithm for standard computers for taking a large number and finding its prime factors in polynomial time

The RSA Algorithm

- Invented by Rivest, Shamir, and Adleman in 1978
- The RSA public key encryption algorithm was the first practical implementation of the public key encryption discovered
- It remains the most used public key encryption today
- RSA can be used for encryption/decryption, digital signature, and key exchange
- Used by TLS, PEM, PGP, Entrust, ...
- RSA achieves its security from the difficulty of factoring large numbers



An early picture of Adi Shamir, Ron Rivest, and Leonard Adleman

The RSA Algorithm

Alice

- Select two large (secret) random primes:

  P & Q
- Publish the product:

  $N = PQ$
- Select integer E
- Use knowledge of P & Q to compute Y

Bob

- To send message Y to Alice, compute

  $Z = Y^E \bmod N$
- Send Z and X to Alice

Public information: N, E

In practice, E is almost always fixed $(X = 65537) = 2^{16} + 1$

RSA Parameters in Practice

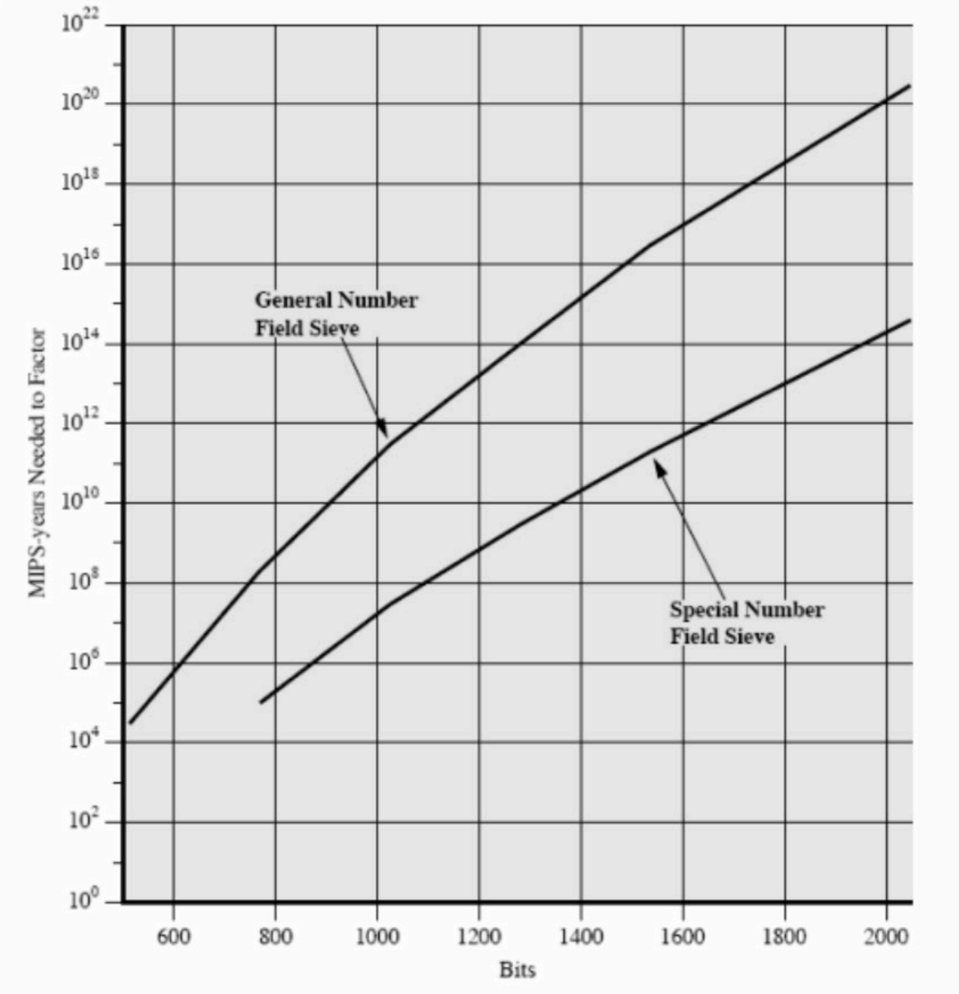
In practice, the RSA modulus *n* should be at least 1024 bit long, which results in a bit length for *p* and *q* of 512. Here is an example of RSA parameters for this bit length:

$$\begin{aligned}
p = {} & E0DFD2C2A288ACEBC705EFAB30E4447541A8C5A47A37185C5A9 \\
& CB98389CE4DE19199AA3069B404FD98C801568CB9170EB712BF \\
& 10B4955CE9C9DC8CE6855C6123_h \\
q = {} & EBE0FCF21866FD9A9F0D72F7994875A8D92E67AEE4B515136B2 \\
& A778A8048B149828AEA30BD0BA34B977982A3D42168F594CA99 \\
& F3981DDABFAB2369F229640115_h \\
n = {} & CF33188211FDF6052BDBB1A37235E0ABB5978A45C71FD381A91 \\
& AD12FC76DA0544C47568AC83D855D47CA8D8A779579AB72E635 \\
& D0B0AAAC22D28341E998E90F82122A2C06090F43A37E0203C2B \\
& 72E401FD06890EC8EAD4F07E686E906F01B2468AE7B30CBD670 \\
& 255C1FEDE1A2762CF4392C0759499CC0ABECFF008728D9A11ADF_h
\end{aligned}$$

Threats to Basing Cryptographic Systems on Prime Factoring

- The continuing increase in computing power
- Continuing refinement of factoring algorithms
- Timing attacks
- Implementation vulnerabilities

Many of the bigger numbers have still not been factored and are expected to remain unfactored for quite some time, however advances in quantum computers make this prediction uncertain due to Shor's algorithm



Going Beyond Prime Factorization Problems

Read more: https://www.enisa.europa.eu/news/enisa-news/post-quantum-cryptography-anticipating-threats-and-preparing-the-future. Published: Oct 2022.

Exercises

1. Write a simple algorithm to check if a number is a prime number.
2. For RSA with a 1024-bit modulus n, the primes p and q each should have a length of about 512 bits, i.e., $p,q \approx 2^{512}$. What is the probability that a random odd number p^* is a prime?
3. Identify an alternative algorithm to RSA for data encryption that is considered quantum-safe.

Final Remarks

- Factorization is a crucial problem
- An algorithm that efficiently factors an arbitrary integer would render RSA-based public-key cryptography insecure
- Progress in factorization algorithms and factorization hardware is hard to predict
- Consider alternative algorithms

References and Useful Links

Main textbook:

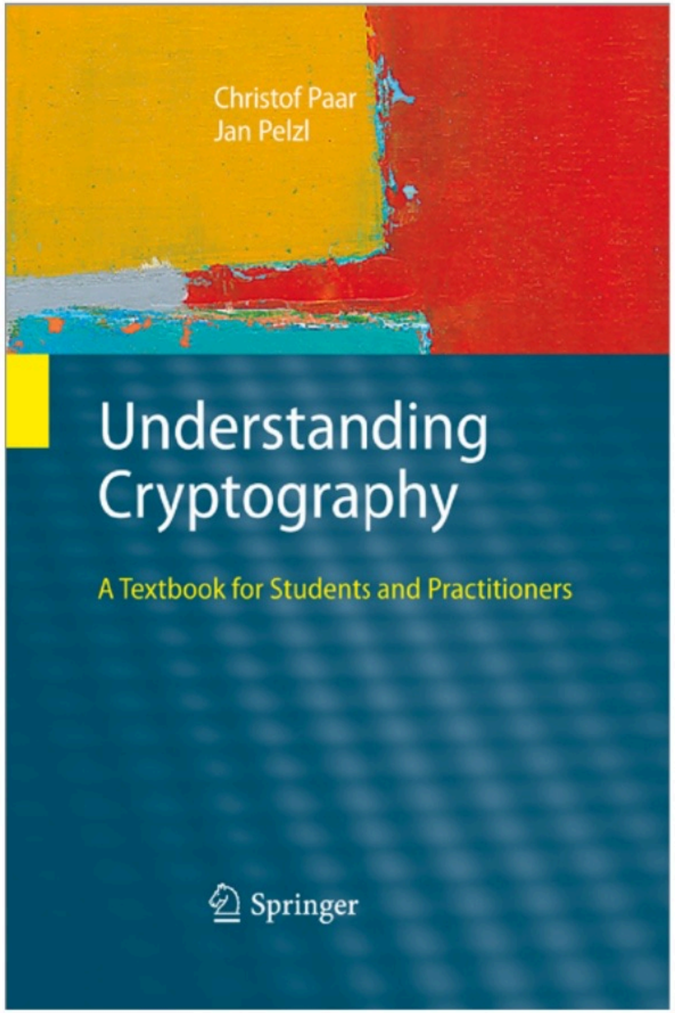
- Paar, Christof, and Jan Pelzl. *Understanding cryptography: a textbook for students and practitioners*. Springer; 1st ed., 2010.

Supplementary textbook:

- Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. CRC Press; 1st ed., 1996.

Research articles:

- Mavroeidis, Vasileios, et al. "The impact of quantum computing on present cryptography." *arXiv preprint arXiv:1804.00200* (2018).


Christof Paar
Jan Pelzl
Understanding Cryptography
A Textbook for Students and Practitioners
Springer

Thank you for listening!

Thoughts? **Questions?**