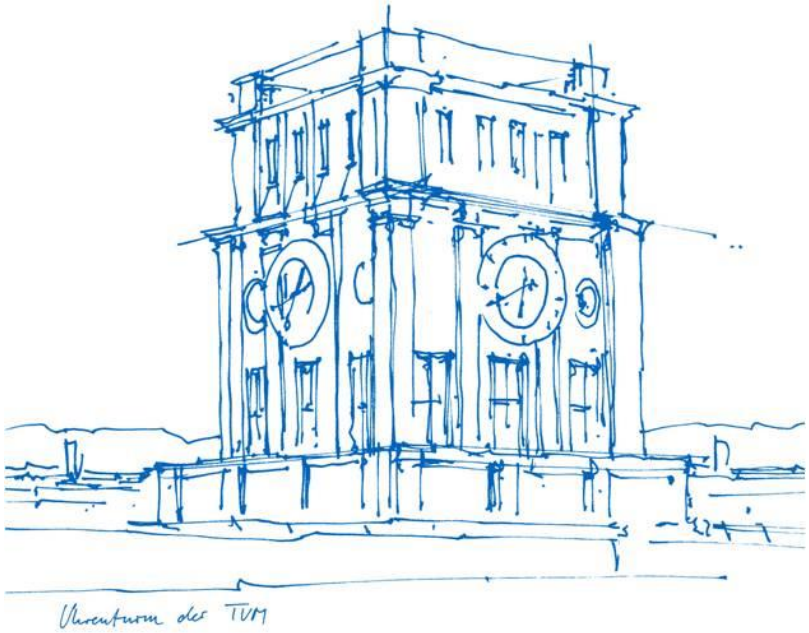
Scientific Seminar Quantum Networks:

Conventional Cryptography

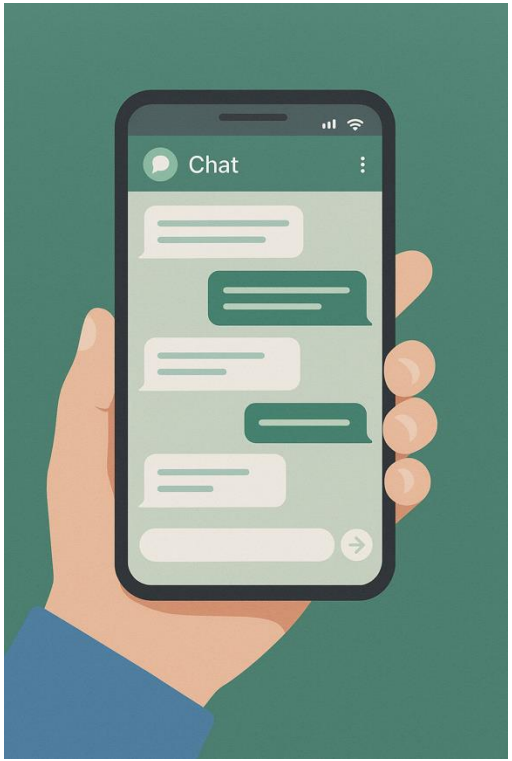
Simon Hang

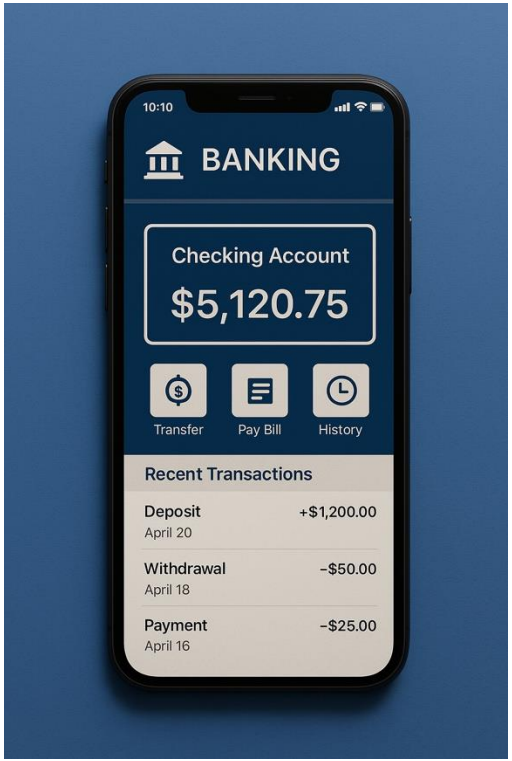
Technical University of Munich

Munich, 10. November 2025



Introduction





All images generated with ChatGPT 5

Outline

- Terminology
- Symmetric-key algorithm: AES
- Asymmetric-key algorithm: RSA
- Comparison of Runtime and Security
- Conclusion
- Outlook

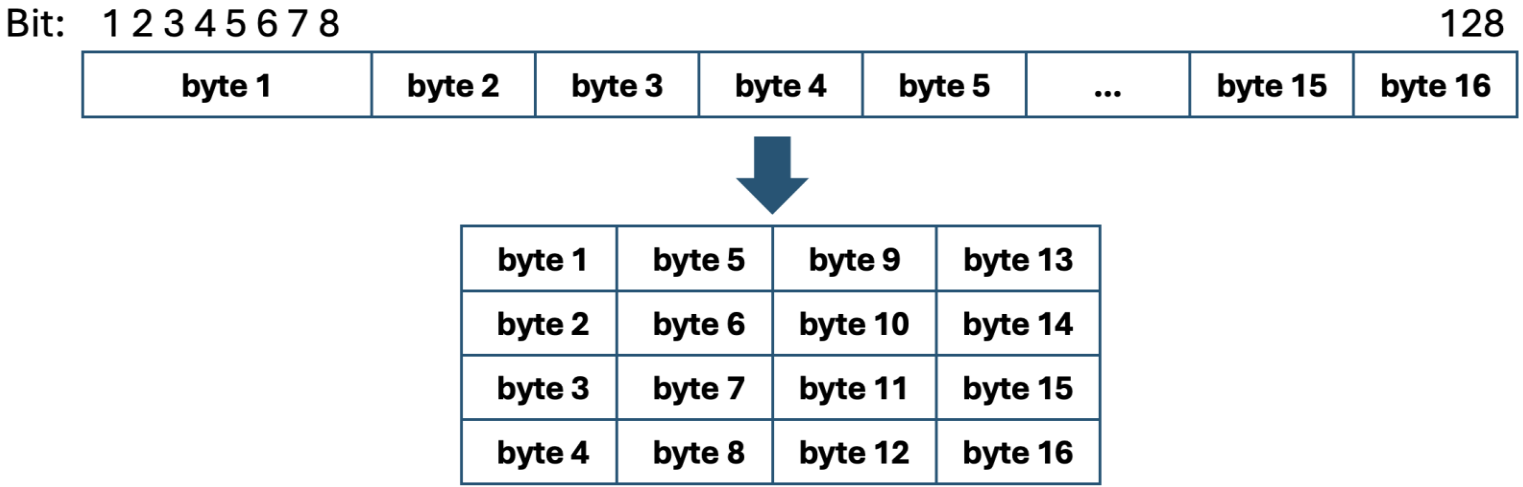
Terminology and Theory

Basic Terminology

- **Plaintext M:** original message
- **Ciphertext C:** transformed and unreadable plaintext
- **Encryption:** function: $C = E_{K_E}(M)$
- **Decryption:** function: $M = D_{K_D}(C)$
- **Key:** parameter of the functions

Symmetric-key Algorithms
Advanced Encryption Standard

- Same key for encryption and decryption
- AES-128: 128-bit key
- Block cypher: block size 128 bits



own illustration based on: National Institute of Standards and Technology, 2023. [Online]. Available: https://doi.org/10.6028/NIST.FIPS.197-upd1

Symmetric-key Algorithms

AES: 1) Byte Substitution

		y														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

National Institute of Standards and Technology, 2023. [Online]. Available: https://doi.org/10.6028/NIST.FIPS.197-upd1

Symmetric-key Algorithms

AES: 2) Shift Rows

- Shift row n by n-1 places to the left

byte 1	byte 5	byte 9	byte 13	1
byte 2	byte 6	byte 10	byte 14	2
byte 3	byte 7	byte 11	byte 15	3
byte 4	byte 8	byte 12	byte 16	4

byte 1	byte 5	byte 9	byte 13	1
byte 6	byte 10	byte 14	byte 2	2
byte 11	byte 15	byte 3	byte 7	3
byte 16	byte 4	byte 8	byte 12	4

own illustration based on: National Institute of Standards and Technology, 2023. [Online]. Available: https://doi.org/10.6028/NIST.FIPS.197-upd1

Symmetric-key Algorithms

AES: 3) Mix Columns

- Matrix (column-) vector multiplication
- Done for all column vectors

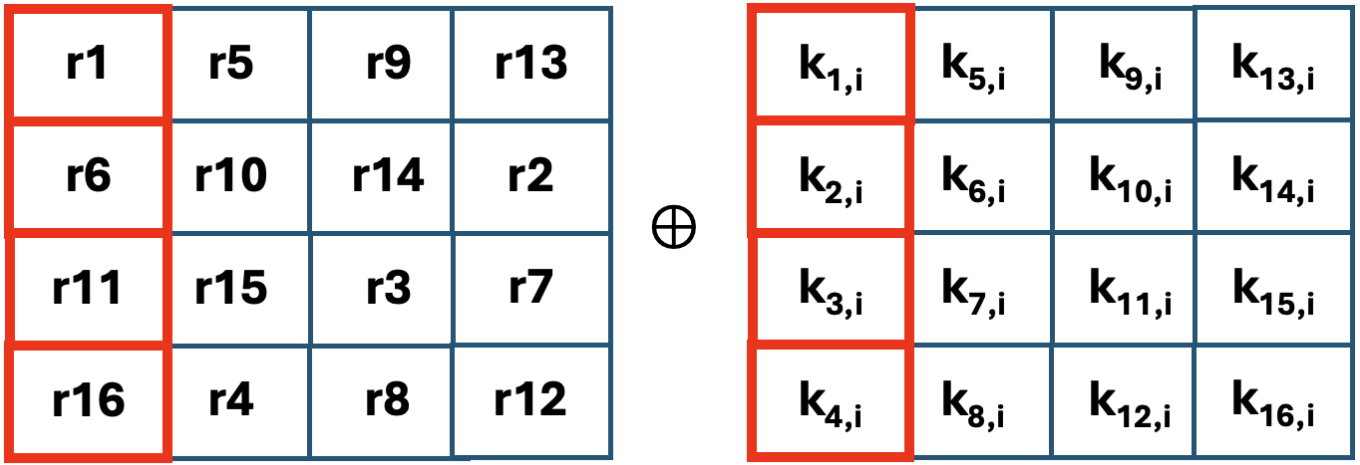
$$\begin{bmatrix} r1 \\ r6 \\ r11 \\ r16 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} byte\ 1 \\ byte\ 6 \\ byte\ 11 \\ byte\ 16 \end{bmatrix}$$

own illustration based on: National Institute of Standards and Technology, 2023. [Online]. Available: https://doi.org/10.6028/NIST.FIPS.197-upd1

Symmetric-key Algorithms

AES: 4) Add Key

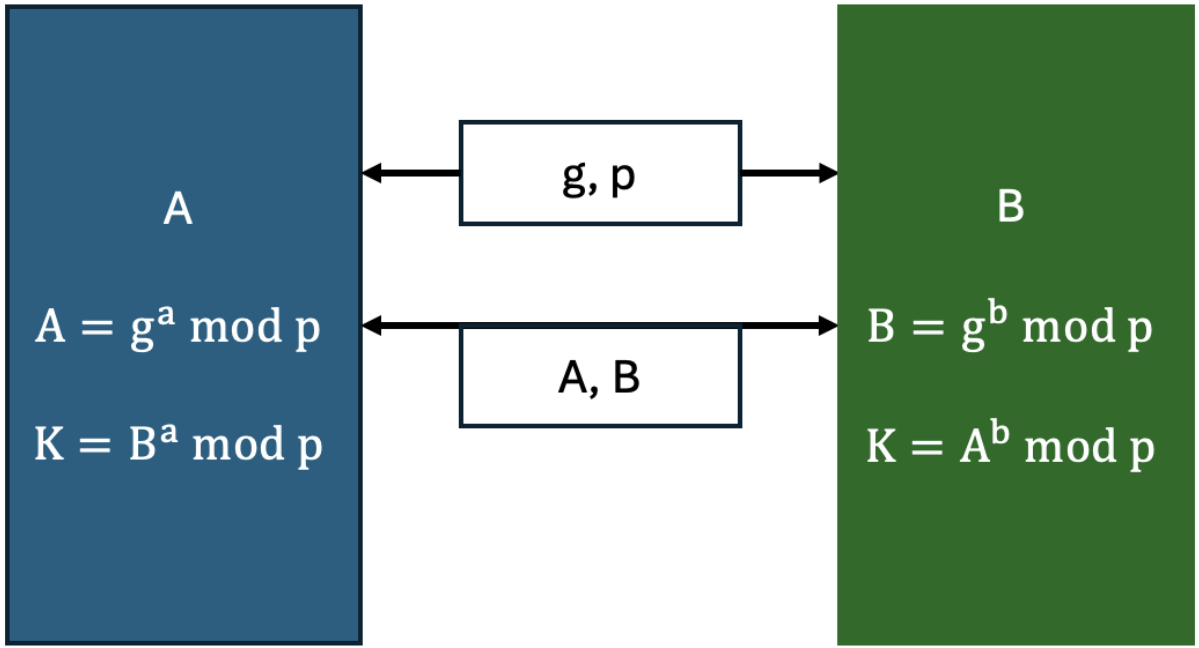
- Add key on the modified plain text
- Done for all columns
- Index **i** is the current round



own illustration based on: National Institute of Standards and Technology, 2023. [Online]. Available: https://doi.org/10.6028/NIST.FIPS.197-upd1

Key Exchange Algorithms

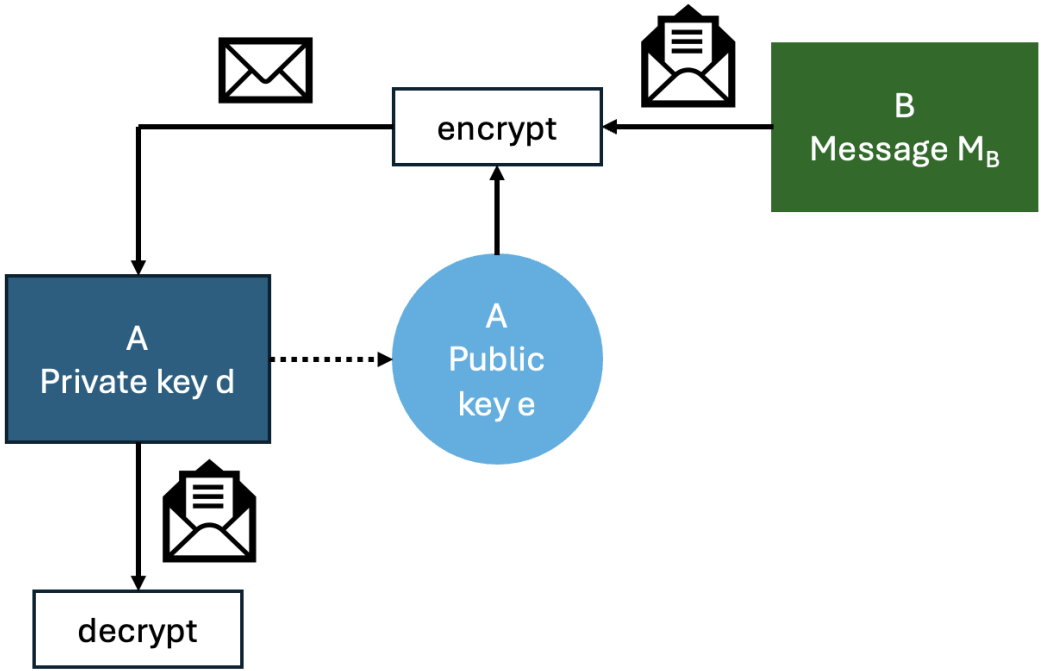
Diffie-Hellman Protocol



own illustration based on: W. Diffie, M. E. Hellman, *IEEE Trans. Inf. Theory*, 1976, *22*(6), 644-654.

Asymmetric-key Algorithms

Rivest-Shamir-Adleman (RSA)



own illustration based on: W. Diffie, M. E. Hellman, *IEEE Trans. Inf. Theory*, 1976, *22*(6), 644-654.

Asymmetric-key Algorithms

RSA: Key Generation 1) - 3)

Algorithm:

1) Choose two random prime numbers p and q

2) Calculate $n = p \cdot q$; n is modulo and is public

3) Calculate $\Phi(n) = (p-1)(q-1)$, all coprime numbers to n between 1 and n.

Example:

1) $p = 3, q = 11$

2) $n = 3 \cdot 11 = 33$

3) $\Phi(n) = (3-1) \cdot (11-1) = 20$

based on: K. Somsuk, *Heliyon*, 2025, *11*(4), e42481.

Asymmetric-key Algorithms

RSA: Key Generation 4) - 5)

Algorithm:

4) Choose public key e, such that:

$$1 < e < \Phi(n)$$

$$\gcd\big(e, \Phi(n)\big) = 1$$

5) Calculate private key d:

$$d \cdot e \bmod \Phi(n) = 1$$

Example:

4) For $e = 3,7,9,11,13,17,19$ it holds:

$$1 < e < 20$$

and $\gcd(e, 20) = 1$

$\rightarrow e = 3$

5) $d \cdot 3 \bmod 20 = 1$

$\rightarrow d = 7$

$\tilde{d}$	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
$i \cdot 3$	3	6	9	12	15	18	21	24
mod 20	3	6	9	12	15	18	1	4

based on: K. Somsuk, *Heliyon*, 2025, *11*(4), e42481.

Asymmetric-key Algorithms

RSA: Encryption and Decryption

Algorithm:

- $C = E_{K_E}(M) = M^e \bmod n$
- $M = D_{K_D}(C) = C^d \bmod n$

Example:

- Send plaintext: $M = \mathbf{5}$, $e = 3$, $d = 7$
- $C = E_{K_E}(3) = 5^3 \bmod 33 = 26$
- $M = D_{K_E}(C) = 26^7 \bmod 33 = \mathbf{5}$

Asymmetric-key Algorithms

RSA: Encryption and Decryption

Algorithm:

- $C = E_{K_E}(M) = M^{\mathbf{e}} \bmod \mathbf{n}$
- $M = D_{K_D}(C) = C^{d} \bmod \mathbf{n}$

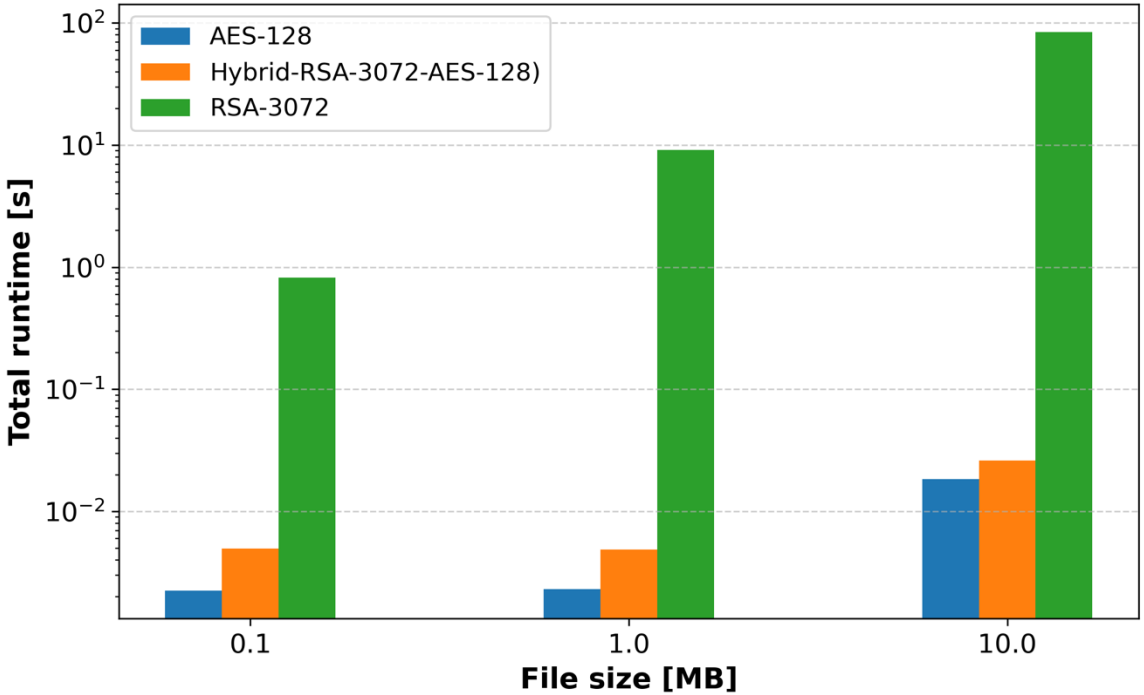
- **Modulo $\mathbf{n}$ and public key $\mathbf{e}$ are public**

Runtime Performance

AES vs RSA

Specifications:

- Key size AES: 128 bit
- Key size RSA: 3072 bit
- Apple MacBook Air (M2 processor, 16 GB of RAM, macOS Ventura 13.5)
- Python 3.9
- cryptography package (v.46.0.3)



Security of the Algorithms

Classical Considerations: AES

- **Security:** Time to recover key
- **AES-128:**
  - Size of key-space: 2^{128}
  - Substitute bytes, shift-rows, mix columns add security
  - “billions of years” to break with brute force

Security of the Algorithms
Classical Considerations: RSA

- **Security:** Time to factor number
- **RSA-2048:**
  - Private key is of order 2048 bits
  - No algorithm with polynomial complexity known for factorisation
  - “billions of years” to break with brute force

Security of the Algorithms
Emerging Quantum Technology

- **AES:**
  - Problem: quadratic speedup due to Grover's algorithm in key search
  - Solution: double key size (i.e. 128-bit → 256-bit)

- **RSA:**
  - Problem: Shor's Algorithm: polynomial complexity for factorisation
  - Solution: new post-quantum cryptography algorithms
  - **Approximation (2025): break RSA-2048 in under a week with less than one million qubits**

Conclusion

- Discussion of symmetric and asymmetric-key algorithms

- **Symmetric-key/AES:**
  + Performant
  + Secure against classical and (partly) quantum attacks
  - Problem: Need to share private key

- **Asymmetric-key/RSA:**
  + No need to share private key
  + Secure against classical attacks
  - Insecure against quantum attacks
  - Less performant for bulk encryption

Outlook

Conventional Cryptography:

- Analysis of different algorithms (e.g. Blowfish, Elliptic Curves)
- Algorithms to break cypher
- Detecting manipulation of data

Post-Quantum Cryptography:

- Exploration of hash- and lattice-based (and other) methods

References, Slides and Code