

ENGLISCH

LEISTUNGSKURS

NEVER GUDE

Carl-Friedrich-Gauß Gymnasium Hockenheim
[GitHub](#)

j.gude/posteo.de



This work is licensed under [CC BY-NC-SA 4.0](#)

Inhaltsverzeichnis

1	ABITURPRÜFUNG	1
1	Rechnerstrukturen	1
1.1	Logikgatter	1
1.2	Boolsche Algebra	2
2	Netzwerke	2
2.1	Schichtenmodell	2
3	Kryptologie	2
3.1	Kerckhoffsches Prinzip	2
3.2	Ziele der Verschlüsselung	2
3.3	(A)symmetrische Verschlüsselung	3

ABITURPRÜFUNG

SECTION 1

Rechnerstrukturen

SUBSECTION 1.1

Logikgatter





IEC Symbol	Mathematisches Symbol	Sym-bol	Bedeutung
	\neg		NOT/Negation
	\wedge		AND/Konjunktion
	\vee		OR/Disjunktion
	\oplus		XOR/Kontravalenz

Tabelle 1. Logikgatter mit deren mathematischen Symbolen

Abbildung 1. Halbaddierer

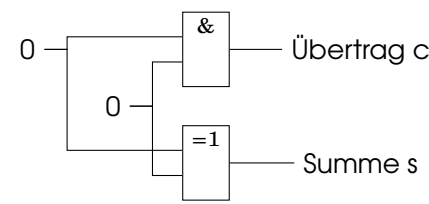


Abbildung 2. Volladdierer

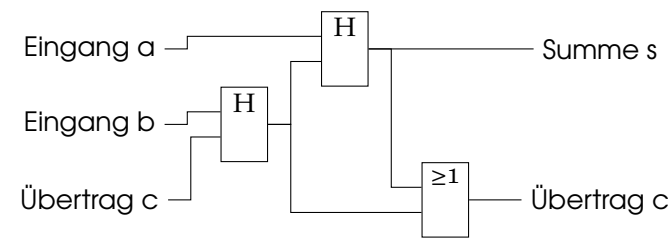
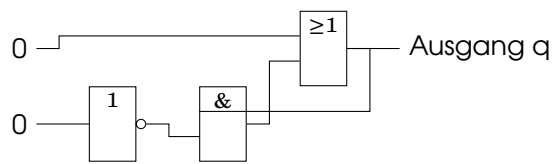


Abbildung 3. RS-Flip-Flop



SUBSECTION 1.2

Boolsche Algebra**KV-Diagramme**

SECTION 2

Netzwerke

SUBSECTION 2.1

Schichtenmodell

Anwendungen Bereitstellung von Funktionen für Anwendungsprogramme

FTP (Ports 20/21) : File Transfer Protocol

HTTP (80): Hyper Text Transfer Protocol

SMTP (25): Simple Mail Transfer Protocol

Bereitstellung von Funktionen zur Organisation des Netzwerkes selbst

DHCP (67,68): Dynamic Host Configuration Protocol

Transport Bereitstellung des universellen Transportdienstes mit explizit geschalteten Verbindungen mit Auf- und Abbaumodalitäten und Datenflusskontrolle.

Internet Festlegen des Wegs vom Sender zum Empfänger durch das Netz über IPv4 oder IPv6

Netzzugang Datenübertragung über physikalische Übertragungsmedien durch MAC und Mechanismen zur Fehlererkennung.

SECTION 3

Kryptologie

SUBSECTION 3.1

Kerckhoffsches Prinzip

Im Jahr 1883 formulierte Auguste Kerckhoff ein Grundprinzip der Kryptologie:

In einem guten Kryptosystem muss nur der Schlüssel geheim bleiben

SUBSECTION 3.2

Ziele der Verschlüsselung

Vertraulichkeit Um ein Mitlesen der Nachricht durch Dritte zu verhindern, muss die Vertraulichkeit gewährt sein.

Integrität Um ein Ändern der Nachricht durch Dritte zu verhindern, muss die Integrität gewährt sein.

Authentizität Um ein Ändern des*der Absender*in zu verhindern, muss die Authentizität gewährt sein.

SUBSECTION 3.3

(A)symmetrische Verschlüsselung

Symmetrische Verschlüsselung Die Nachricht wird mit dem gleichen Schlüssel ver- und entschlüsselt. Der Rechenaufwand ist geringer als beim asymmetrischen Pendent. Bsp.: AES

Asymmetrische Verschlüsselung Die Nachricht wird mit einem Schlüssel verschlüsselt und mit einem anderen entschlüsselt. Es wird dabei ein Schlüsselpaar aus öffentlichem und privatem Schlüssel generiert.

Mit dem fremden öffentlichen Schlüssel wird verschlüsselt, wenn Vertraulichkeit gefordert ist. Entschlüsselt wird dann mit dem eigenen privaten Schlüssel.

Mit dem eigenen privaten Schlüssel wird verschlüsselt, wenn Authentizität gefordert ist. Entschlüsselt wird dann mit dem fremden öffentlichen Schlüssel. Dieses Verfahren wird in der Realität häufig praktiziert.

Bsp.: RSA

Hybride Verschlüsselung Der symmetrische Schlüssel wird per asymmetrischer Verschlüsselung an die andere Person gesendet. Danach kann der symmetrische Schlüssel für die weitere Kommunikation verwendet werden.

Transpositionsverfahren Die Buchstaben des Klartextes werden durch die Verschlüsselung anders angeordnet.

Bsp.: Skytale, (Fleißner, Gartenzaun)

Substitutionsverfahren Die Buchstaben des Klartextes werden bei der Verschlüsselung durch andere Buchstaben (oder Zeichen) ersetzt.

Bsp.: Caesar, Substitutionschiffre, Vigenère, One-Time-Pad

Monoalphabetische Substitution Ein Substitutionsverfahren, bei dem nur ein einziges Schlüsselalphabet verwendet wird.

Bsp.: Caesar, RSA (wenn man es fälschlicherweise auf einzelne Buchstaben anwendet)

Polyalphabetische Substitution Ein Substitutionsverfahren, bei dem mehrere Schlüsselalphabete verwendet werden.

Bsp.: Vigenère, One-Time-Pad

One-Time-Pad Absolut sichere Version der Vigenère-Verschlüsselung, bei dem der Schlüssel mindestens so lang sein muss, wie die Nachricht. Außerdem muss der Schlüssel sicher übermittelt werden und nur einmal verwendet werden. Da bei der sicheren Übertragung des Schlüssels auch gleich die Nachricht übermittelt werden könnte, ist das OTP unpraktikabel.

