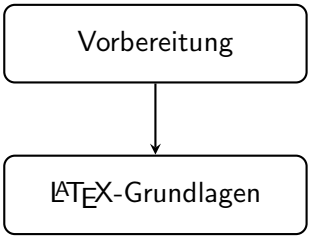
Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

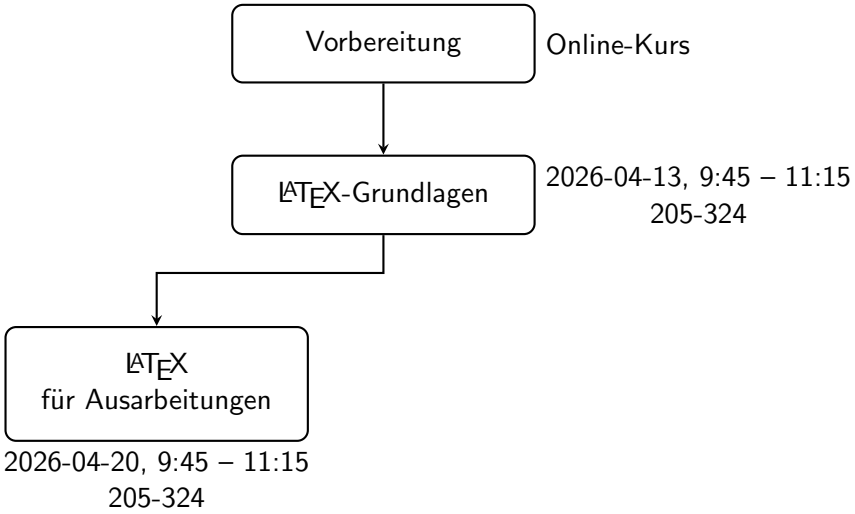
Einführung IT Security

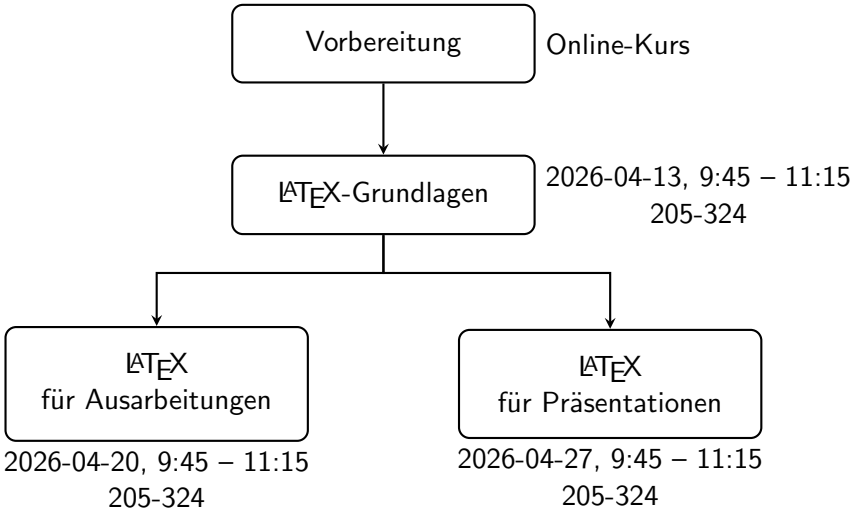
LaTeX

Vorbereitung

Online-Kurs


Vorbereitung
Online-Kurs
LaTeX-Grundlagen
2026-04-13, 9:45 – 11:15
205-324


Vorbereitung
Online-Kurs
LaTeX-Grundlagen
2026-04-13, 9:45 – 11:15
205-324
LaTeX
für Ausarbeitungen
2026-04-20, 9:45 – 11:15
205-324


Vorbereitung
Online-Kurs
LaTeX-Grundlagen
2026-04-13, 9:45 – 11:15
205-324
LaTeX
für Ausarbeitungen
2026-04-20, 9:45 – 11:15
205-324
LaTeX
für Präsentationen
2026-04-27, 9:45 – 11:15
205-324

Beispiel für Chiffrat einer monoalphabetischen Substitutionschiffre:

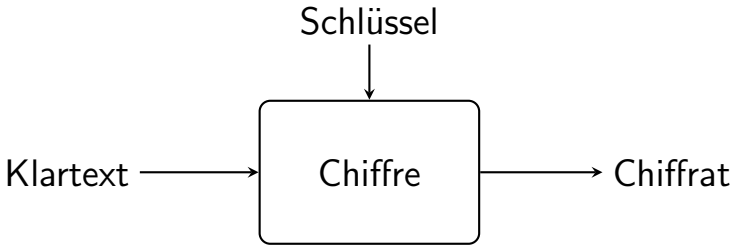
TDB OZBPYDB XDBMBYO RDBX, LSBY TBU ABZBDUIDG TBG LXOBI SYDIAO GDB KIG TPQZ IDQZO ILBZBY. FBTBIMLXXG SDI DQZ KBSBYHBKAO TLRPI, TLGG TBY IDQZO CKBYMBXO.

Kryptoanalyse mit CrypTool Online

Kerckhoffs'sche Prinzip

Schlüssellose Verfahren: Ver- und Entschlüsselung sind festgelegt. Im Falle eines Bruchs, z. B. durch Bekanntwerden der Chiffre, muss die komplette Chiffre getauscht werden.

Kerckhoffs'sche Prinzip



Auguste Kerckhoffs (1835 – 1903)

Kerckhoffs'sche Prinzip:

Die Sicherheit einer Chiffre darf nicht auf Ihrer Geheimhaltung beruhen.

Eugen Drezen, Historio de la Mondo Lingvo

Steganografie und Kerckhoffs'sches Prinzip

Steganografie verstößt gegen das Kerckhoffs'sche Prinzip und spielt in der modernen Kryptografie nur eine untergeordnete Rolle.

Eugen Drezen, Historio de la Mondo Lingvo

Substitutionschiffre

Vigenère-Chiffre

- Giovan Bellaso 1553
- später Blaise de Vigenère zugeschrieben
- polyalphabetische Substitutionschiffre
- erst im 19. Jhd. gebrochen

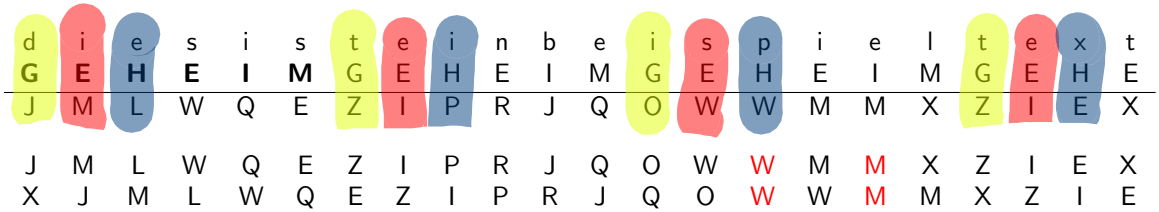
By Thomas de Leu - Woodcut Photograph

Vigenère-Chiffre

- Giovan Bellaso 1553
- später Blaise de Vigenère zugeschrieben
- polyalphabetische Substitutionschiffre
- erst im 19. Jhd. gebrochen

	k	l	a	r	t	e	x	t
+	**G**	**E**	**H**	**E**	**I**	**M**	G	E
	Q	P	H	V	B	Q	D	X

Kryptoanalyse
Autokorrelation



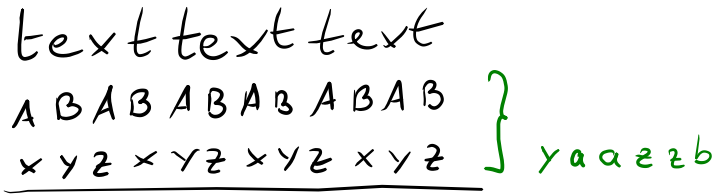
Kasiki

d	i	e	s	i	s	t	e	i	n	b	e	i	s	p	i	e	l	t	e	x	t
G	**E**	**H**	**E**	**I**	**M**	G	E	H	E	I	M	G	E	H	E	I	M	G	E	H	E
J	M	L	W	Q	E	Z	I	P	R	J	Q	O	W	W	M	M	X	Z	I	E	X

J	M	L	W	Q	E	Z	I	P	R	J	Q	O	W	W	M	M	X	Z	I	E	X
X	J	M	L	W	Q	E	Z	I	P	R	J	Q	O	W	W	M	M	X	Z	I	E

Kryptoanalyse
Autokorrelation

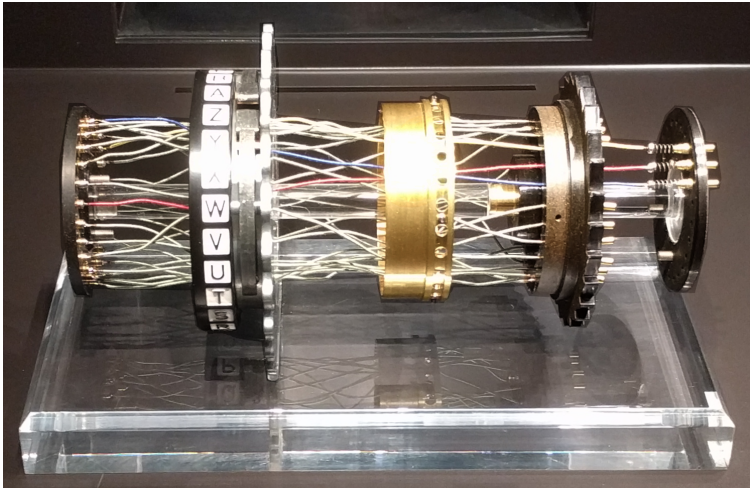
d	i	e	s	i	s	t	e	i	n	b	e	i	s	p	i	e	l	t	e	x	t
G	**E**	**H**	**E**	**I**	**M**	G	E	H	E	I	M	G	E	H	E	I	M	G	E	H	E
J	M	L	W	Q	E	Z	I	P	R	J	Q	O	W	W	M	M	X	Z	I	E	X
J	M	L	W	Q	E	Z	I	P	R	J	Q	O	W	W	M	M	X	Z	I	E	X
X	J	M	L	W	Q	E	Z	I	P	R	J	Q	O	W	W	M	M	X	Z	I	E


text text text
A B A B A B A B A B A B
x y z x y z x y z x y z
y a a z z b

Enigma

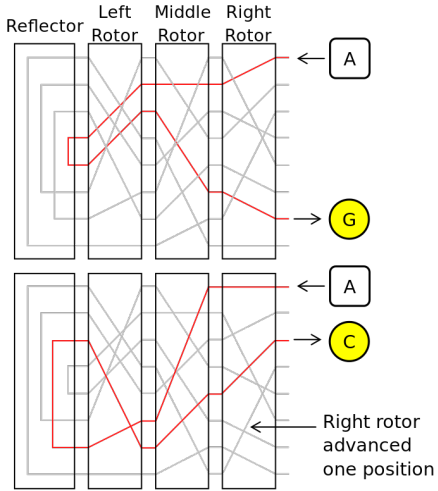
By Greg Goebel - Web page Image

Funktionsweise Enigma



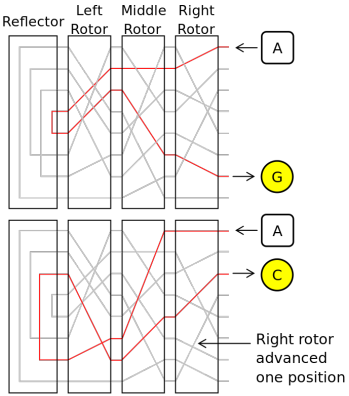
eigenes Foto, Deutsches Museum

Funktionsweise Enigma



Von MesserWoland - Eigenes Werk, basierend auf: File:Enigma-action.png von User:Jeanot; original diagram by Matt Crypto

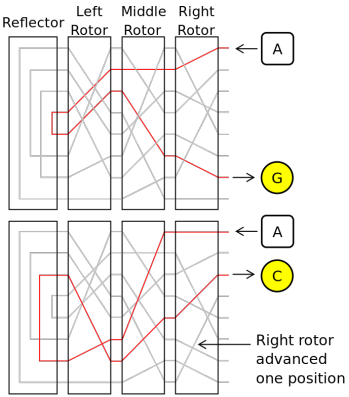
Schwäche der Enigma



Verschlüsselung: fixpunktfreie Permutation

Von MesserWoland - Eigenes Werk, basierend auf: File:Enigma-action.png von User:Jeanot; original diagram by Matt Crypto

Schwäche der Enigma



Verschlüsselung: fixpunktfreie Permutation

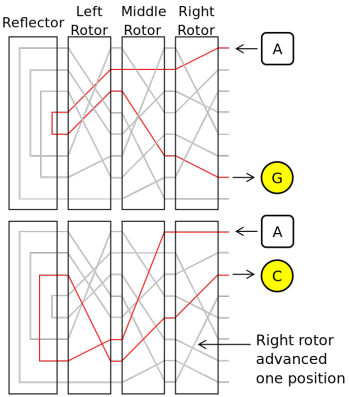
Chiffrat	JFGNB	PSSNK	EFX
Kandidat 1	ANGRI	FFSOF	ORT
Kandidat 2	RUECK	ZUGJE	TZT

Von MesserWoland - Eigenes Werk, basierend auf: File:Enigma-action.png von User:Jeanot; original diagram by Matt Crypto

Erwarten Sie einen Angriff oder einen Rückzug?

Chiffrat	JFGNB	PSSNK	EFX
Kandidat 1	ANGRI	FFSOF	ORT
Kandidat 2	RUECK	ZUGJE	TZT

Schwäche der Enigma



Verschlüsselung: fixpunktfreie Permutation

Chiffrat	JFGNB	PSSNK	EFX
Kandidat 1	ANGRI	FFSOF	ORT
Kandidat 2	RUECK	ZUGJE	TZT

Von MesserWoland - Eigenes Werk, basierend auf: File:Enigma-action.png von User:Jeanot; original diagram by Matt Crypto

Angriffe gegen Chiffren

Mächtigkeit des Angreifers

Ziel des Angreifers

Mächtigkeit des Angreifers

1. Chiffre unbekannt

Ziel des Angreifers

Mächtigkeit des Angreifers

1. Chiffre unbekannt
2. Chiffre bekannt

Ziel des Angreifers

Mächtigkeit des Angreifers

1. Chiffre unbekannt
2. Chiffre bekannt
3. Klartext bekannt
   (*known plaintext*)

Ziel des Angreifers

Mächtigkeit des Angreifers

1. Chiffre unbekannt
2. Chiffre bekannt
3. Klartext bekannt
   (*known plaintext*)
4. gewählter Klartext
   (*chosen plaintext*)

Ziel des Angreifers

Mächtigkeit des Angreifers

1. Chiffre unbekannt
2. Chiffre bekannt
3. Klartext bekannt
   (*known plaintext*)
4. gewählter Klartext
   (*chosen plaintext*)
5. Entschlüsselungsorakel
   (*chosen ciphertext*)

→ oder →

Ziel des Angreifers

Mächtigkeit des Angreifers

1. Chiffre unbekannt
2. Chiffre bekannt
3. Klartext bekannt (*known plaintext*)
4. gewählter Klartext (*chosen plaintext*)
5. Entschlüsselungsorakel (*chosen ciphertext*)

Ziel des Angreifers

1. ohne Schlüssel entschlüsseln (*totaler Bruch*)

Mächtigkeit des Angreifers

1. Chiffre unbekannt
2. Chiffre bekannt
3. Klartext bekannt (*known plaintext*)
4. gewählter Klartext (*chosen plaintext*)
5. Entschlüsselungsorakel (*chosen ciphertext*)

Ziel des Angreifers

1. ohne Schlüssel entschlüsseln (*totaler Bruch*)
2. einen Schlüssel herausfinden

Mächtigkeit des Angreifers

1. Chiffre unbekannt
2. Chiffre bekannt
3. Klartext bekannt (*known plaintext*)
4. gewählter Klartext (*chosen plaintext*)
5. Entschlüsselungsorakel (*chosen ciphertext*)

Ziel des Angreifers

1. ohne Schlüssel entschlüsseln (*totaler Bruch*)
2. einen Schlüssel herausfinden
3. ein Chiffrat entschlüsseln

Mächtigkeit des Angreifers

1. Chiffre unbekannt
2. Chiffre bekannt
3. Klartext bekannt (*known plaintext*)
4. gewählter Klartext (*chosen plaintext*)
5. Entschlüsselungsorakel (*chosen ciphertext*)

Ziel des Angreifers

1. ohne Schlüssel entschlüsseln (*totaler Bruch*)
2. einen Schlüssel herausfinden
3. ein Chiffrat entschlüsseln
4. zwei bekannte Klartexte unterscheiden

Enigma

Angriffe gegen Chiffren

Mächtigkeit des Angreifers

1. Chiffre unbekannt
2. Chiffre bekannt
3. Klartext bekannt (*known plaintext*)
4. gewählter Klartext (*chosen plaintext*)
5. Entschlüsselungsorakel (*chosen ciphertext*)

Ziel des Angreifers

1. ohne Schlüssel entschlüsseln (*totaler Bruch*)
2. einen Schlüssel herausfinden
3. ein Chiffrat entschlüsseln
4. zwei bekannte Klartexte unterscheiden
5. zwei gewählte Klartexte unterscheiden

Paradigmenwechsel der Kryptologie

Die Enigma markierte das Ende der klassischen Kryptologie und den Beginn der modernen Kryptologie.

1910er & 1920er (elektro-)mechanische Chiffriermaschinen

1920er & 1930er Kommerzialisierung & zivile Nutzung

1930er & 1940er Kryptoanalyse: Linguisten $\rightarrow$ Mathematiker